



## **Bolignetforeningens hørings svar til udkast til bekendtgørelse og vejledning om telenet- og teletjenesteudbyderes registrering og opbevaring af oplysninger om teletrafik samt praktiske bistand til politiet i forbindelse med indgreb i meddelelshemmeligheden.**

København d 14 maj 2004

### **Indledning**

Bolignetforeningen er fundamentalt enig om, at det er vigtigt at politi og efterretningstjenester sikres fornuftige efterforskningsværktøjer i kampen mod alvorlig kriminalitet. Imidlertid er det vores vurdering, at den politimæssige betydning af bekendtgørelsen vil blive marginal, samtidigt med at konsekvenserne for bolignetforeninger tegner til at blive meget alvorlige. Det skal dertil siges, at bekendtgørelsen gennemgående er så uklart formuleret, særligt indenfor datadelen, at det i praksis er umuligt at kommentere den uden først, at foretage en subjektiv fortolkning af hvad der menes. Dette er i sig selv et væsentligt problem, idet systemadministratorer ikke med denne bekendtgørelse i hånden vil kunne vide sig sikre på at overholde loven.

Når bekendtgørelsen er blevet så tvetydig, synes det at hænge sammen med, at der kontinuerligt skiftes mellem to overordnede målsætninger for bekendtgørelsen. På den ene side synes bekendtgørelsen at lægge op til, at det primære formål er at sikre at data der opbevares i anden forbindelse nu skal opbevares i 1 år. På den anden side synes bekendtgørelsen at lægge op til at kræve en yderligere registrering af specifikke oplysninger, der typisk ikke registreres i dag. Det nødvendige indhold af bekendtgørelsen vil være kraftigt afhængig af hvilken af disse to målsætninger, der er den gældende, og bekendtgørelsens konsekvenser for bolignetforeninger vil ligeledes være kraftigt afhængige heraf.

Havde man holdt sig til, at data, der i anden forbindelse opbevares, skal opbevares i et år, havde bekendtgørelsen været umiddelbart anvendelig. Bekendtgørelsens mål havde dermed været begrænset til at sikre allerede eksisterende elektroniske beviser, der ofte vil have en kort levetid. Hvilke data, der vil blive registreret, vil afhænge af hvilken type netværk der er tale om, og bekendtgørelsen ville således have været teknologineutral, hvilket vil betyde, at bolignetforeningerne ikke skal ud og investere voldsomme summer i opgradering af deres netværksudstyr, og endvidere betyde, at bekendtgørelsen ikke vil blive forældet af den teknologiske udvikling.

Imidlertid indeholder bekendtgørelsen også afsnit hvor man pålægger bolignetforeningerne at registrere og opbevare oplysninger der ikke normalt registreres som en naturlig del af vores virke. Bekendtgørelsens målsætning synes nu ikke at begrænse sig til sikring af eksisterende beviser, men til egentlig ”produktion” af beviser (data registreres alene med det formål at de skal være tilgængelig for politiet på et senere tidspunkt). Da teleloven, persondataloven og registerloven pålægger os at slette data efter endt brug hvis de ikke er omfattet af denne bekendtgørelse, må bekendtgørelsen med denne målsætning nødvendigvis indeholde meget specifikke definitioner af hvilke data der skal registreres og opbevares og hvilke der ikke skal. Imidlertid glimrer bekendtgørelsen i sin nuværende form ved at være meget lemfældig i sin omgang med begreberne indenfor datatransmission, hvorfor det ikke er muligt ud fra bekendtgørelsen entydigt at fastslå hvilke yderligere oplysninger, der nu skal til at registreres



# Bolignetforeningen

(jvf. dette høringssvars tekniske del). Imidlertid vil en bekendtgørelse der meget specifikt søger at definere hvad der skal registreres meget hurtigt blive overhalet af den teknologiske udvikling. Endvidere vil en sådan bekendtgørelse pålægge bolignetforeninger meget store omkostninger til at opgradere deres systemer, så det bliver teknisk muligt at registrere disse data. Bekendtgørelsen er således alt andet end teknologineutral i denne tolkning. Den efterforskningsmæssige gevinst vil ligge i at politiet på forhånd vil vide hvilke beviser der vil være til rådighed på en given lokalitet. Dog må det forventes at folk med et vist IT kundskab meget nemt vil kunne omgå logningen, f.eks. ved kryptering.

Kombinationen af en uklar overordnet målsætning kombineret med en meget uklar og til tider tvetydig omgang med tekniske termer gør at bekendtgørelsen i sin nuværende form er uanvendelig som hjælp til den IT-ansvarlige i at kunne opfylde lovens bogstav.

Bolignetforeningen ser derfor ikke andre muligheder end at bekendtgørelsen for nuværende begrænses til at pålægge teleudbydere at gemme oplysninger registreret i anden forbindelse i et år, dvs. fjerne § 2 stk. 1 fra bekendtgørelsen.

Såfremt der er et politisk ønske om at udvide registreringspligten med specifikke oplysninger ud over hvad der i forvejen registreres, vil Bolignetforeningen foreslå, at der nedsættes et arbejdsudvalg med repræsentanter fra de relevante aktører, således at det sikres at bekendtgørelsens krav er juridisk entydige og teknisk gennemførlige. Et sådant arbejde vil kunne reducere byrden for de berørte aktører samtidigt med at politiet vil kunne sikres bedre efterforskningsværktøjer end med herværende bekendtgørelse. For nuværende udskrives en stor regning der vil gøre IT dyrere end det er i dag, uden at der synes at være nogen væsentlig samfundsmæssig gevinst ved dette.

Endelig har Bolignetforeningen meget vanskeligt ved at se den efterforskningsmæssige logik bag kravet om døgnbetjent kontaktpunkt. Formålet med et døgnbetjent kontaktpunkt synes at knytte sig til en hurtig sikring af beviser. Med herværende bekendtgørelse pålægges telebranchen og bolignetforeningerne jo netop at opbevare alle registrerede data i et år, hvorfor beviset er sikret uden politiets indgriben. Samtidigt er den økonomiske byrde, bolignetforeninger dermed pålægges, helt ude af proportioner. Et døgnbetjent kontaktpunkt koster typisk omkring 3 mill. kr. om året at opretholde, hvilket er væsentligt større end den samlede årlige omsætning for en række af de bolignetforeninger der pålægges at etablere døgnbetjent kontaktpunkt. Såfremt man fortsat ønsker bolignetforeningernes indsats i udbredelsen af højhastigheds internetforbindelser, er det således helt nødvendigt at dette krav udelades i den endelige bekendtgørelse.

I det følgende skal ovennævnte konklusioner blive uddybet og underbygget. Vores høringssvar er inddelt i en generel del, en teknisk del og et appendiks til den tekniske del.



## Generel del

Bolignetforeningen er overordnet set enig om, at det er vigtigt at politiet sikres gode arbejdsbetingelser i opklaringen af alvorlig kriminalitet.

Samtidigt mener vi dog også, at omkostningerne til tilvejebringelse af opklaringsværktøjer bør stå i et rimeligt forhold til den opklaringsmæssige gevinst ved tilvejebringelsen af nye opklaringsværktøjer. Dette mener vi ikke er tilfældet med herværende bekendtgørelse, da logningens kvalitet er defineret utroligt uklart, og et stort antal aktører er helt undtaget fra logningspligt, samt at kriminelle organisationer må forventes at anvende kryptering af data. Dette vil gøre det særdeles nemt for kriminelle at undgå logning. Samtidigt pålægger logningspligten bolignetforeninger en række voldsomme økonomiske og administrative byrder, der i praksis vil gøre bolignetforeningernes store frivillige arbejde med at udbrede IT kendskabet til den danske befolkning meget vanskeligt fremover.

Bekendtgørelsen omhandler netop oplysninger som udbydere ikke normalt vil opbevare, da de ikke er nødvendige for produktion af tjenesteydelsen. De ønskede oplysninger skal således opsamles og opbevares med det ene formål at sikre, at oplysningerne kan tilvejebringes i det tilfælde politiet eller andre med en dommerkendelse får brug for dem. Logningen foretages således alene af hensyn til politi og efterretningstjenester.

Hidtil har overvågning og efterforskningsarbejde været monopoliseret hos Politi og efterretningstjenester, og Bolignetforeningen stiller sig uforstående overfor, at bolignetforeninger nu skal pålægges at udføre politiopgaver. Bolignetforeningerne kan således ikke forventes at ligge inde med den tekniske, økonomiske og administrative kompetence der skal til at løfte denne politimæssige opgave på forsvarlig vis. Vi finder derfor logningspligten overordentligt problematisk og mener, at såfremt den skal gennemføres som der er lagt op til i bekendtgørelsen, bør der for bolignetforeninger være tale om, at dette gøres af en ekstern partner, betalt af politiet. Dette kunne f.eks. ske ved at logfilerne opbevares hos en central uafhængig myndighed i krypteret form hvor den dato- og personspecifikke krypteringsnøgle opbevares af bolignetforeningerne.

Denne eksterne myndighed bør af hensyn til troværdigheden ikke høre under Justitsministeriet men kunne eksempelvis være Datatilsynet.

Samtidigt må det anses for rimeligt at den dataopbevarende myndighed kan udføre gratis konsulentvirksomhed overfor de logningsforpligtede udbydere og på denne måde sikre at den loggede information er tilstrækkelig og korrekt.

Det er særligt problematisk for bolignetforeninger at skulle opbevare personspecifikke oplysninger om vore naboer - herunder deres sexvaner, religiøse overbevisning, og generelle gøren og laden på internettet - netop fordi disse oplysninger berører mennesker som vi har personlig kontakt med i det daglige. Hertil kommer at bekendtgørelsen er meget uklart afgrænset i forhold til persondata- og registerloven.

For nuværende er området primært reguleret i form af regler for hvor længe man må opbevare forskellige typer af oplysninger. Som bekendtgørelsen er udformet nu, vil det i praksis være umuligt for bolignetforeninger at administrere deres netværk på en måde, der hverken strider mod logningspligt eller persondata-/registerloven.

Endelig mener Bolignetforeningen at bekendtgørelsen pålægger bolignetforeninger og televirksomheder betragtelige ukompenserede meromkostninger til udførelse af en samfundsmæssig opgave (terroristbekæmpelse og efterforskning).



# Bolignetforeningen

Bolignetforeningen har vanskeligt ved at se hvilke efterforskningsmæssige kriterier, der adskiller bolignetforeninger fra f.eks. private virksomheder, universiteter, biblioteker m.v., der i bekendtgørelsen er helt undtaget for logningspligt. Bolignetforeningen mener derfor, at bekendtgørelsen bør omfatte alle der stiller en internetforbindelse til rådighed for andre, idet logningen ellers vil blive meget nem at omgå for kriminelle. Det vil således uundgåeligt virke kraftigt demotiverende på de mange frivillige, når de pålægges voldsomme administrative byrder i forbindelse med logningen, og det samtidigt er selvindlysende, at den efterforskningsmæssige værdi af dette arbejde vil være meget ringe.

Bolignet vil (ligesom universiteter og private virksomheder) typisk være opbygget på en måde, der teknisk set gør det ganske vanskeligt at opfylde bekendtgørelsens krav, idet netværksinfrastrukturen ikke er designet ud fra et behov om at kunne fakturere forbrugsafhængigt. Dette betyder at bekendtgørelsen i en række tilfælde vil kræve at bolignetforeninger udskifter netværkskomponenter for anseelige beløb og betyde en forøgelse af etableringsomkostningerne ved nye bolignet.

Hvis logningspligten skal opnå den maksimale efterforskningsmæssige værdi, mener Bolignetforeningen det er nødvendigt, at der må være lighed for loven - dvs. at alle der stiller en internetforbindelse til rådighed for andre bør være forpligtet til at logge de samme data. Som det ser ud nu er både mindre bolignetforeninger, offentlige institutioner og private virksomheder helt eller delvist undtaget fra logning.

Bolignetforeningen mener afgjort, at dette vil mindske den efterforskningsmæssige værdi af de logningsdata der indsamles hos bolignetforeninger og andre teleudbydere, idet det vil være overordentligt nemt for kriminelle at skaffe sig internetadgang gennem en ikke logningsforpligtet part, f.eks. bibliotek, universitet, internetcafe eller arbejdsplads. Hertil kommer problemer med at afgrænse de forskellige typer aktører, f.eks. ved hjemmearbejdende.

Det er overordentligt svært, at se de efterforskningsmæssige hensyn der berettiger, at bolignetforeninger pålægges logningspligt, når et større antal sammenlignelige aktører slipper. Hertil kommer, at det må forventes at kriminelle allerede anvender kryptering af data, hvilket yderligere må forventes at gøre den efterforskningsmæssige værdi af logningen begrænset.

Kravet om døgnbemandet kontaktpunkt er særdeles problematisk for bolignetforeninger uanset størrelse. Dette krav vil være særdeles omkostningstungt, og i praksis økonomisk umuligt at honorere for en række bolignetforeninger, der med herværende bekendtgørelse vil være omfattet af dette krav. Selv hvis Bolignetforeningens medlemmer i fællesskab gik sammen om at etablere et døgnbemandet kontaktpunkt for medlemsforeningernes til sammen ca. 10.000 slutbrugere ville omkostningerne hertil typisk betyde kontingentstigninger i størrelsesordenen 20-40 %. For en Bolignetforening med 500 brugere vil omkostningen overstige foreningens årlige omsætning. Kravet om døgnbetjent kontaktpunkt vil således umuliggøre etableringen af bolignetforeninger fremover, og være praktisk umuligt at honorere for de fleste af de allerede eksisterende bolignetforeninger.

Endvidere finder Bolignetforeningen kravet om døgnbemandet kontaktpunkt ganske besynderligt, set i forhold til indholdet i herværende bekendtgørelse, idet logningspligten jo netop sikrer at registrerede data vil være tilgængelige for politiet i op til et år efter registreringen. Det vil således ikke være nødvendigt hurtigt at skulle sikre beviser. Behovet for døgnbetjent kontaktpunkt synes ydermere uforståeligt når bekendtgørelsen ikke indeholder krav om tidsfrister for udlevering af data til politiet.



# Bolignetforeningen

Bolignetforeningen foreslår derfor, at kravet om døgnbetjent kontaktpunkt erstattes med tidsfrister for udlevering af oplysninger, eventuelt kombineret med et krav om at Politiets Teletjeneste er bekendt med systemadministrators telefonnummer.

Opretholdes kravet om døgnbemandet kontaktpunkt for bolignetforeninger, vil det reelt betyde dødsstødet for det store frivillige arbejde, der foregår rundt omkring i lokalmiljøerne med at fremme udbredelsen af internet.

Bekendtgørelsen forholder sig ikke til hvilken juridisk person der er ansvarlig for logningens gennemførelse. For en bolignetforening er ansvaret ofte meget uklart defineret. Er det således de lokale kræfter der står for den daglige drift af en bolignetforening, afdelingsbestyrelsen for bolignetforeningen der i sin tid initierede netværkets etablering, og muligvis ejer netværket helt eller delvist, eller er det bolignetforeningens hovedbestyrelse, der står med strafansvaret for logningens gennemførelse?

Uanset hvem, der står med det strafretslige ansvar, så vil strafansvar i denne sammenhæng gøre etablering og drift af bolignetforeninger overordentligt vanskeligt fremover. Der er ingen tvivl om, at de frivillige der i dag udfører et stort og ulønnet arbejde i bolignetforeningerne rundt omkring i landet, vil have ganske vanskeligt ved at påtage sig et strafansvar igennem udførelsen af et stykke frivilligt arbejde. Såfremt ansvaret placeres hos hovedbestyrelsen for boligselskabet, vil dette ganske givet betyde, at der kommer et pålæg ovenfra om at sådanne anlæg ikke kan etableres fremover, idet hovedbestyrelsen næppe vil være interesseret i at pådrage sig et strafansvar, som de i praksis ikke kan styre - i og med at de intet har at gøre med den daglige drift - herunder logning.

Bolignetforeningerne har spillet en ganske væsentlig rolle i etableringen af Danmark som foregangsland på internettet. Etableringen af bolignetværk har således i væsentligt omfang fået de lidt teknologiforskrækkede borgere på internettet, idet de har fået den fornødne hjælp fra naboer og netværksfolk i boligområdet. Bolignetforeningerne er ofte etableret og drevet af frivillige kræfter i lokalmiljøet på ikke kommerciel basis. Bekendtgørelsen vil påføre disse ildsjæle, der i forvejen udfører et stort ulønnet arbejde, endnu en tung teknisk-administrativ byrde. I praksis kan dette give en række bolignetforeninger store problemer, idet ildsjælene simpelthen bukker under for arbejdspresset og kaster håndklædet i ringen. Bolignetforeningen synes selvsagt at det er ærgerligt, hvis det ikke også fremover vil være praktisk muligt at etablere bolignetforeninger.

I de tilfælde hvor en bolignetforening vælger at kontrahere med tredjepart til gennemførelse af logning, hvilket for en del foreningers vedkommende vil være deres eneste reelle mulighed for at leve op til bekendtgørelsen, da de ikke besidder den nødvendige tekniske ekspertise, påtager tredje part sig dermed også strafansvar for logningens gennemførelse?

Det er Bolignetforeningens opfattelse, at der i dag er en generel mangel på viden om hvad bolignetforeningers rettigheder og pligter er overfor politiet. Dette bliver ikke bedre når herværende bekendtgørelse træder i kraft. Specielt mener vi, at det er helt afgørende, at der udarbejdes minimumsretningslinier for hvorledes bekendtgørelsen **samt** relevant lovgivning omkring opbevaring af persondata kan honoreres i praksis. Såfremt bolignetforeningerne skal udføre dette arbejde, er det nødvendigt at det ikke skal gennemføres på baggrund af vores skøn, men kan baseres på vejledninger indeholdende minimumskrav til tekniske specifikationer samt softwaremæssige forhold. Dette er ikke tilfældet med herværende bekendtgørelse.



## Teknisk del

På det tekniske område er bekendtgørelsen efter Bolignetforeningens opfattelse alt for uklar. I sit udgangspunkt synes bekendtgørelsen at lægge op til at hvad der kan registreres skal registreres, og hvad der ikke kan registreres skal ikke registreres. Bekendtgørelsens manglende specifikation af præcis hvad der kræves registreret vil medføre, at det er op til domstolene at afgøre om fx en bolignetforening har gjort sit arbejde ordentligt. Det er ikke et ønskværdigt forhold for hverken domstolene eller bolignetforeningerne. Endvidere finder Bolignetforeningen det yderst uheldigt at pålægge bolignetforeninger og andre et strafansvar, når det reelt er umuligt at finde ud af hvornår man som registreringspligtig har opfyldt sin logningsforpligtelse.

De tekniske uklarheder medfører som beskrevet, at det er uklart præcis hvilke oplysninger der skal registreres, og det er derfor også uklart hvilke omkostninger denne registrering vil påføre fx bolignetforeninger. Indsamling af en række af de i bekendtgørelsen skitserede registreringsoplysninger vil kræve en betydelig investering i udstyr. Endvidere fremgår det ikke af bekendtgørelsen og tilhørende vejledning, at pålideligheden af de registrerede oplysninger af rent tekniske grunde kan være endog yderst tvivlsom. Eksempelvis kan opkaldende IP adresser og e-mail adresser forfalskes og datakommunikation kan krypteres (fx i netbanksystemer og netbetalinger).

I de følgende afsnit beskrives en række af de tekniske uklarheder som Bolignetforeningen mener kræver afklaring. Beskrivelserne er forsøgt holdt i et letforståeligt sprog, og hvor nødvendigt henvises der til appendiks.

Med udgangspunkt i de nedenfor beskrevne forhold mener Bolignetforeningen, at det for al datakommunikation alene er meningsfuldt og hensigtsmæssigt at registrere opkaldende og opkaldte IP adresse, tidspunkt, eventuelt TCP portnummer, og geografisk lokation forstået som den lejlighed i foreningen som kommunikationen hidrører.

### **Registrering af trafik**

Udbyder skal ifølge bekendtgørelsen registrere trafik (§ 2, stk. 1, nr. 5), hvilket i den tilhørende vejledning specificeres som den anvendte trafiktype.

Trafiktype er ikke noget veldefineret begreb indenfor datakommunikation, og derfor er det yderst uheldigt at vejledningen til bekendtgørelsen ikke indeholder et eneste eksempel på hvad der forstås ved trafiktype for datakommunikation.

Headerinformation fra netværksprotokoller (fx Internet Protocol) og transportprotokoller (fx Transmission Control Protocol) er umiddelbart tilgængelige i systemer der viderebefordre datakommunikation, mens information om hvilken applikationsprotokol der anvendes (fx Hypertext Transport Protocol [HTTP] eller Simple Mail Transfer Protocol [SMTP]) ikke er umiddelbart tilgængelige (se appendiks).

Hvis der med trafiktype menes applikationsprotokol vil det pålægge bolignetforeninger betydelige omkostninger til registrering. Endvidere kan applikationsprotokollen være umulig at fastlægge fordi kommunikationen krypteres eller der er tale om en ubeskreven applikationsprotokol. Derfor vil pålideligheden af informationen om den anvendte applikationsprotokol være forbundet med betydelig usikkerhed.



Bolignetforeningen finder det derfor uklart hvad, der i bekendtgørelsen forstås ved trafik/trafiktype i forbindelse med datakommunikation.

Det er Bolignetforeningens opfattelse, at den endelige bekendtgørelse klart bør specificere hvad der menes med registrering af trafik i forbindelse med datakommunikation, ellers vil det være umuligt at afgøre om man som registreringspligtig opfylder kravene til registrering. Endvidere vil omkostningerne til registrering være særdeles afhængige af hvad der menes med trafiktype.

Det er Bolignetforeningens opfattelse at den endelige bekendtgørelse ikke bør kræve specifikation af trafik udover transportprotokol og eventuelt dertil knyttet portnummer. Dette er begrundet med, at identifikation af anvendt applikationsprotokol i visse tilfælde vil være umulig (krypteret kommunikation, fx netbank, eller en ubeskrevet applikationsprotokol), og hvor den er mulig vil være forbundet med betydelige meromkostninger for udbyder, idet disse informationer ikke er umiddelbart tilgængelige i dennes systemer og derfor vil kræve intensiv pakkeanalyse at fremskaffe.

Af bekendtgørelsen fremgår det endvidere, at det skal registreres om kommunikationen blev gennemført, om der blev etableret forbindelse til den opkaldte identitet og, hvis dette ikke er tilfældet, hvorfor kommunikationen ikke blev gennemført. Vedrørende datakommunikation vil det i en lang række tilfælde være umuligt, at indsamle disse oplysninger. Eksempelvis har visse almindeligt anvendte transportprotokoller (fx UDP) ikke nogen defineret sekvens eller forløb, og dermed ingen afslutning. Det giver i så fald ikke mening, at tale om kommunikationens afslutning.

Det vil oftest også være umuligt at afgøre, hvorfor en given netværkspakke ikke nåede den opkaldte identitet (var serveren slukket, forbindelsen afbrudt eller noget helt tredje). Bolignetforeningen mener derfor ikke, at en registrering af om kommunikationen blev gennemført giver mening for datakommunikation, og derfor bør et sådant krav bortfalde.

## **Opkaldende og opkaldte identitet**

For datakommunikation fremgår det af bekendtgørelsen og dertilhørende vejledning, at opkaldende identitet og opkaldte identitet (og ændring af disse) er IP-adresser (se fx vejledningen, side 17, eksemplet om internet ADSL).

En IP adresse identificerer i sig selv alene en computer tilkoblet internettet, og indeholder derfor hverken information om hvem, der anvender denne computer eller hvor, den rent geografisk er lokaliseret (se appendiks).

Det er for Bolignetforeningen uklart hvordan en IP adresse kan anvendes i efterforskningsøjemed, medmindre denne IP adresse specifikt identificerer en slutbruger (fx et medlem af en bolignetforening) eller en præcis geografisk lokation (fx en lejlighed som har forbindelse til foreningens netværk).

Trods dette er slutbrugeridentitet (fx navn og CPR-nummer) ikke nævnt i bekendtgørelsen eller dertilhørende vejledning, og lokaliseringsdata er ikke anført i typeeksemplet på de oplysninger, som udbyder af datakommunikation typisk skal udlevere til myndighederne (vejledningen, side 17, eksemplet om internet ADSL).

I eksisterende bolignetforeninger identificerer en opkaldende IP adresse indenfor foreningen i dag enten



# Bolignetforeningen

- i) en arbitrær computer tilsluttet foreningens netværk,
  - ii) en specifik lejlighed som er tilkoblet foreningens netværk, eller
  - iii) en unik slutbruger (fx hvor login er påkrævet for etablering af forbindelse til internettet).
- I en række bolignetforeninger vil det være forbundet med betydelige udgifter at indkøbe udstyr der kan fastlægge hvilken lejlighed der kommunikerer med en given IP-adresse.

For Bolignetforeningen er det afgørende at den endelige bekendtgørelse klart specificerer hvad, der forstås ved opkaldende identitet og opkaldte identitet i forbindelse med datakommunikation. Såfremt der med opkaldende identitet menes identiteten af en slutbruger, pålægges bolignetforeninger en identifikationsbyrde som er langt tungere end det er tilfældet for fastnettelefoni, hvor lokaliseringsdata for kommunikationsudstyret synes tilstrækkelig (fx en adresse tilknyttet et givent telefonnummer).

Såfremt bolignetforeninger skal identificere slutbrugere, bør det endvidere fremgå af den endelige bekendtgørelse hvilke legitimationskrav bolignetforeninger pålægges i forbindelse med identifikation af medlemmer (fx billedlegitimation i form af pas eller kørekort).

Hvis den opkaldende identitet fastlægges udfra sammenkobling af IP adresse med lokaliseringsdata (den fysiske adresse hvor slutbrugerens kommunikationsudstyr er koblet på udbyderens netværk) bør disse anføres blandt de informationer, som udbyder af datakommunikation typisk skal udlevere til myndighederne (vejledningen, side 17, eksemplet om internet ADSL).

Anvendelse af trådløse netværk umuliggør endvidere en præcis fastlæggelse af geografisk lokation. Kravet om registrering af geografisk lokation (fx lejlighed) kan derfor hindre udbredelsen af trådløse netværk i fx bolignetforeninger.

For Bolignetforeningen er det endvidere uklart, hvilke oplysninger der kræves opsamlet, når en opkaldt IP-adresse udenfor foreningen dækker over hvad der kan opfattes som flere forskellige identiteter. Et ofte forekommende eksempel på dette er såkaldte hosting-firmaer, som tilgængeliggør hjemmesider tilhørende flere forskellige domæner (fx www.dr.dk, www.pol.dk) fra samme IP adresse (dvs. samme computer). I disse tilfælde vil en IP-adresse i sig selv ikke entydigt identificere hvilke af disse domæner som opkaldes. Fastlæggelse af hvilket domæne, der i en sådan situation opkaldes, forudsætter analyse af kommunikationens indhold (se appendiks) og vil påføre bolignetforeninger væsentlige omkostninger til analyseudstyr.

Bolignetforeningen finder det derfor af afgørende betydning, at det i den endelige bekendtgørelse nærmere specificeres hvad der menes med opkaldte identitet.

## **Registrering af e-postadresser**

Ifølge bekendtgørelsen og dertilhørende vejledning skal en udbyder, som overfører elektroniske postbeskeder mellem en bruger og en e-postserver, registrere e-postadresserne på afsender og modtager. Endvidere skal dato, tid, og unik identitet involveret i alle adgange til en e-postadresse tilknyttede e-poster registreres.

Begreberne afsenders og modtagers e-postadresse er uklart beskrevet i bekendtgørelsen. Det er eksempelvis muligt at anføre hvad som helst i e-postens "To"-felt, eftersom det er "RCPT to"-kommandoen i (SMTP-)kommunikationen med e-postserveren, som har betydning for hvem e-posten afleveres til. Med andre ord er det temmelig ligegyldigt at registrere "To"-feltet.



# Bolignetforeningen

Oplysninger om e-postadresser er ikke umiddelbart tilgængelig i systemer, der overfører datakommunikation mellem bruger og e-postserver (se appendiks). Det er heller ikke muligt umiddelbart at afgøre om en given datakommunikation er en e-post (fx kan kommunikationen med en e-postserver foregå på en hvilken som helst port, ikke nødvendigvis TCP port 25, som er standard for SMTP kommunikation). Derfor er det forbundet med betydelige ressourcer at fremskaffe disse oplysninger, idet samtlige IP-pakker, der transporteres i netværket, skal analyseres for tilstedeværelsen af e-post-adresser.

Af sikkerhedsmæssige grunde kan datakommunikation med en e-postserver krypteres (selve indholdet behøver ikke være krypteret, det kan alene være kommunikationen med serveren), og det vil i så fald være umuligt at bestemme e-postadresserne på afsender og modtager.

Endvidere kan e-postadressen på afsenderen let forfalskes.

Der er derfor store omkostninger og tekniske ressourcer forbundet med registrering af e-postadresser, og pålideligheden af de registrerede oplysninger er forbundet med betydelig usikkerhed.

Bolignetforeningen mener ikke, det er meningsfuldt eller hensigtsmæssigt at kræve registrering af specifikke e-postoplysninger, og mener derfor at kravet om registrering af e-postadresser enten bør bortfalde, eller alternativt afgrænses til e-post opbevaret på udbyderens egen e-postserver.

E-postkommunikation bør efter Bolignetforeningens opfattelse alene pålægges samme registreringspligt som gælder for al anden datakommunikation (IP-adresser etc.).

Det forhold, at udbydere af web-posttjenester ikke pålægges at registrere e-postadresser på afsender og modtager, taler også for at dette krav helt bortfalder i den endelige bekendtgørelse.

## **Registrering af chat-tjenester**

Bolignetforeningen forstår bekendtgørelsen således, at udbydere der alene viderebefordrer datakommunikation mellem en chat-klient og en chat-server ikke skal registrere chatroom-identitet, IP-adresse og anvendt chatroom. I modsat fald vil dette være forbundet med betydelige omkostninger til udstyr, idet disse oplysninger ikke umiddelbart er tilgængelige i systemer, der alene viderebefordrer datakommunikation, og derfor skal indhentes via pakkeanalyse (se appendiks). Endvidere kan kommunikationen foregå via proprietære protokoller, hvor det vil være umuligt at analysere indholdet, idet protokollens datastruktur er hemmelig.

Bolignetforeninger stiller ofte en personlig hjemmeside til rådighed for deres medlemmer, og en af de funktioner, som kan tilbydes på en sådan hjemmeside, er en chat-tjeneste. Det fremgår ikke klart af bekendtgørelsen hvem, der i sådanne tilfælde har registreringspligten. Såfremt den personlige hjemmeside opbevares på medlemmets egen computer er bolignetforeningens registreringsmuligheder begrænset som beskrevet ovenfor, idet foreningens systemer alene viderebefordrer datakommunikationen. Det fremgår ikke af bekendtgørelsen om det enkelte medlem i dette tilfælde skal registrere chatroom-identiteter og tilhørende IP-adresser. Det fremgår heller ikke af bekendtgørelsen hvem, der er registreringspligtig såfremt medlemmets personlige hjemmeside (med tilhørende chat-tjeneste) opbevares på foreningens server.



## **Nettermineringspunkter**

Bolignetforeningen forstår bekendtgørelsen således, at datakommunikation mellem to nettermineringspunkter indenfor foreningen (det lokale netværk) er omfattet af registreringspligten.

Dette medfører i så fald, at registreringen ikke alene kan foretages på det centrale udstyr der viderebefordrer kommunikation til/fra internettet, men også skal foretages i de enkelte underkrydsfelter som forbinder foreningens nettermineringspunkter sammen i et netværk. Udstyret i disse underkrydsfelter (hubs, switche og routere) har i dag ingen eller begrænsede logningsfunktioner, og indkøb af nyt udstyr, der kan foretage den krævede registrering, er forbundet med meget betydelige omkostninger.

Såfremt registreringspligten omfatter informationer, der kun kan fremskaffes ved pakkeanalyse (fx e-postadresser eller applikationsprotokoltyper), er det endvidere tvivlsomt om det rent teknisk er muligt at opfylde registreringspligten ved kommunikation mellem nettermineringspunkter indenfor foreningen.

Bolignetforeningen mener derfor, at registreringspligten bør begrænses til at gælde datakommunikation mellem et nettermineringspunkt indenfor foreningen og et nettermineringspunkt udenfor foreningen.

I forbindelse med bekendtgørelsens § 3 stk. 1 og 2 om fritagelse af logningspligt for virksomheder og offentlige institutioner kan som et kuriosum opstilles følgende paradoks: En beboer i en logningspligtig bolignetforening har i forbindelse med sit arbejde i en logningsfritaget virksomhed fået etableret en VPN-tunnel mellem sin bopæl og sin arbejdsplads.

Skal beboerens nettermineringspunkt i hjemmet betragtes som en del af virksomhedens netværk således at bolignetforeningen er fritaget for at logge denne beboers trafik, eller er beboerens nettermineringspunkt en del af bolignetforeningens netværk, selvom dette ikke har umiddelbar ”adgang” til trafikken, således at bolignetforeningen er forpligtet til at analysere og logge den krypterede trafik i tunnelen?



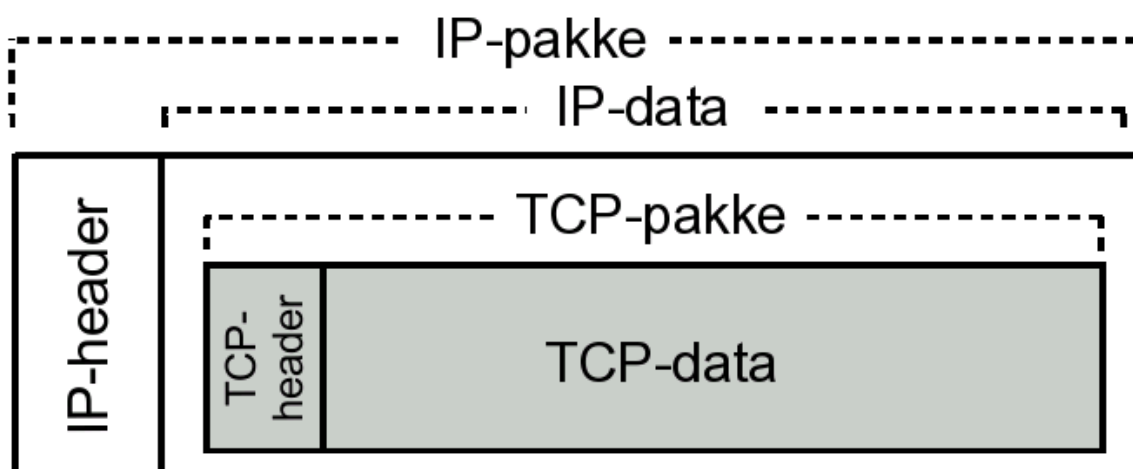
## Appendiks om datakommunikation

### TCP/IP

Datakommunikation mellem computere tilsluttet internettet foregår ofte via netværksprotokollen Internet Protocol (IP). Der transmitteres datapakker (IP-pakker) mellem afsender og modtager, og disse pakker består af en header- og en datastruktur (se figur). IP-headeren ("brevhovedet") indeholder blandt andet afsenderens og modtagerens IP-adresser. IP-pakkens datastruktur er ofte en transportprotokolpakke (fx en Transmission Control Protocol [TCP]-pakke). Transportprotokollen gør det muligt for afsender og modtager at sikre sig, at alle data bliver overført, og at der ikke opstår fejl i transmissionen. En TCP-pakke består af en header- og en datastruktur (se figur). TCP-headeren indeholder blandt andet afsenders og modtagers IP-adresse. De eneste oplysninger der er nødvendige for at viderebefordre IP-pakker er indeholdt i IP-headeren og TCP-headeren. Derfor er indholdet af IP-headeren og TCP-headeren de eneste oplysninger, der umiddelbart optræder i systemer der viderebefordrer datakommunikation. Disse informationer omfatter afsender og modtagers IP-adresse, anvendt transportprotokol (fx TCP) og portnummer (fx 80 for webtrafik og 25 for afsendelse af mail via SMTP).

Selve indholdet af kommunikationen findes i TCP-pakkens datastruktur. Ofte følger indholdet en given applikationsprotokol (fx Hypertext Transfer Protocol [HTTP] for webtrafik eller Simple Mail Transfer Protocol [SMTP] for afsendelse af e-post). Den beskrevne struktur medfører at fx domænenavne og e-post-adresser er en del af TCP-pakkens datastruktur. Da kendskab til indholdet af TCP-pakkens datastruktur ikke er nødvendig for at viderebefordre IP-pakker, optræder dette ikke umiddelbart i systemer som alene viderebefordrer datakommunikation. Fordelen ved denne opbygning er at viderebefordrende systemer ikke behøver have kendskab til alverdens applikationsprotokoller. Det betyder også at indholdet i TCP-pakkens datastruktur (fx e-post-adresser) kan være krypteret.

Fremskaffelse af indholdet af TCP-pakkens datastruktur (fx domænenavne eller e-post-adresser) kræver at alle pakker analyseres.. Hvis indholdet i TCP-pakkens datastruktur er krypteret eller applikationsprotokollen er ukendt er det umuligt at fremskaffe disse oplysninger.





## **Trafik**

I det følgende vil problematikken omkring trafik være forsøgt belyst med udgangspunkt i hentning af en hjemmeside til en internetbrowser hos en bruger. Internetbrowseren hos den opkaldende identitet (brugeren) kan kommunikere med den opkaldte identitet (webserveren hvorpå hjemmesiden er tilgængelig) via den såkaldte HTTP protokol (Hypertext Transport Protocol), som er en applikationsprotokol. På brugerens computer genereres en HTTP-besked med en forespørgsel på de informationer som ønskes fra webserveren, og denne besked indeholder blandt andet adressen på den ønskede hjemmeside (fx <http://www.hkhkronprinsen.dk/37000c>).

HTTP-beskeden indkapsles derefter i en transportpakke (ofte en TCP pakke), som består af to elementer:

i) en header (et brevhoved, eller mere præcist et pakke-hoved), som blandt andet indeholder IP-adresserne på opkaldende og opkaldte identitet samt et TCP portnummer, som i en vis udstrækning kan medvirke til identifikation af den underliggende applikationsprotokol (fx port 80 for http), og

ii) en datastruktur (pakkeindhold) som i dette tilfælde vil være selve HTTP-beskeden.

Endelig indkapsles TCP-pakken i en IP-pakke (Internet Protokol pakke), som også består af to elementer:

i) en header indeholdende blandt andet IP-adresserne på opkaldende og opkaldte identitet og  
ii) en datastruktur som i dette tilfælde vil være TCP-pakken.

For den ovenfor omtalte datakommunikation kan der ved trafik som minimum forstås følgende:

1. Den kommunikerede datamængde (antal kilobytes).
2. Kommunikation via Internet Protocol (IP-trafik).
3. Kommunikation via Transmission Control Protocol (TCP-trafik).
4. Kommunikation via Transmission Control Protocol på port 80 (TCP-trafik port 80).
5. Kommunikation via Hypertext Transport Protocol (HTTP-trafik).

De systemer som viderebefordrer kommunikation (dvs. udbyders systemer) mellem opkaldende og opkaldte identitet har alene brug for informationerne i IP og TCP headeren (dvs. opkaldende og opkaldte identitets IP-adresser samt at der er tale om TCP trafik på port 80), hvorfor det sædvanligvis kun er disse informationer som er umiddelbart tilgængelige i udbyders systemer.

Som udgangspunkt er information, om hvilken applikationsprotokol (i dette tilfælde HTTP) kommunikationen anvender, derfor ikke tilstede i udbyders systemer. Dog forholder det sig sådan, at en række applikationsprotokoller som standard anvender velkendte TCP portnumre (fx port 80 for HTTP-trafik), og i disse tilfælde vil det anvendte TCP portnummer derfor være en indikation for hvilken applikationsprotokol der anvendes.

Det er dog uproblematisk at anvende alternative portnumre, hvorfor denne information netop alene kan tjene som en indikation for hvilken applikationsprotokol der anvendes.

Endvidere skal det bemærkes at, idet kendskab til applikationsprotokollen ikke er nødvendig for viderebefordring af kommunikationen mellem opkaldende og opkaldte identitet, datastrukturen (selve indholdet) i transportprotokolpakken (fx TCP pakken) kan være krypteret; dette er eksempelvis tilfældet, når brugere kommunikerer med netbanksystemer.

I disse tilfælde vil det være umuligt for en udbyder, der alene viderebefordrer kommunikationen, at fastlægge hvilken applikationsprotokol kommunikationen anvender.



## **E-post**

Der er tale om en simplificering, når der i vejledningen til bekendtgørelsen skelnes mellem "konvolut" (med oplysninger om afsender og modtager) og indhold ved elektroniske postbeskeder. Såvel afsenders som modtagers e-postadresse er teknisk set en del af indholdet i en e-post.

Afsendelse af e-post kan foregå via applikationsprotokollen SMTP (Simple Mail Transfer Protocol). SMTP-beskeder indkapsles i en transportpakke (ofte en TCP-pakke) som består af

- i) en header som blandt andet indeholder IP-adresserne på opkaldende (bruger) og opkaldte (e-postserver) identitet samt et TCP portnummer (ofte 25 for SMTP trafik), og
- ii) en datastruktur som i dette tilfælde vil være SMTP-beskeden.

TCP-pakken indkapsles derefter i en netværkspakke (ofte en IP-pakke) som består af

- i) en header (indeholdende IP-adresserne på opkaldende og opkaldte identitet), og
- ii) en datastruktur som i dette tilfælde vil være TCP pakken.

De systemer som viderebefordrer kommunikationen mellem opkaldende og opkaldte identitet gør alene brug af informationerne i headerne af IP- og TCP-pakkerne. Derfor er e-postadresserne på afsender og modtager (indholdet i SMTP-beskeden) sædvanligvis ikke umiddelbart tilgængelige i de systemer, som viderebefordrer kommunikationen. Det betyder også at kommunikationen (herunder afsender og modtagers e-postadresser og e-postens indhold) mellem den opkaldende computer og den opkaldte computer kan være krypteret uafhængigt af om selve e-posten er krypteret.