Notat om ”FRA-loven” og ruting av elektronisk kommunikasjon via Sverige

November 2008

Post- og teletilsynet

Sammendrag

På bakgrunn av den nye svenske loven om signalspaning (”FRA-loven”) har Samferdsels-departementet anmodet Post- og teletilsynet (PT) om en kartlegging av elektronisk kommunikasjon via Sverige. Kartleggingen viser at hovedtyngden av telefontrafikk og datakommunikasjon mellom Norge og utlandet overføres på kommunikasjonsveier som fysisk går over svensk territorium. Noen tilbydere på det norske markedet er datterselskaper av svenske teletilbydere. Deler av den operative virksomheten i enkelte slike selskaper er integrert med morselskapet og er dermed avhengig av svensk infrastruktur også for innenlandsk tjenesteproduksjon av visse typer tjenester.

I tillegg til landbaserte forbindelser via Sverige er det sjøkabelforbindelser til Danmark og til Storbritannia. Sjøkabelforbindelsen til Storbritannia, som går via offshore-installasjoner i Nordsjøen, har ledig kapasitet og kan således representere et alternativ dersom man ønsker å rute mer trafikk utenom Sverige. Norge har også to jordstasjoner for satellittkommunikasjon, men både kostnadsmessig og kapasitetsmessig representerer ikke satellitt noe realistisk alternativ for overføring av store trafikkmengder.

Når det gjelder selve FRA-loven har PT undersøkt lovens rekkevidde, hvilke tillatelser som må gis for signalspaning, myndighetskontroll og hvordan tilretteleggingen skal skje. I den forbindelse ble det avholdt et møte med Post- och telestyrelsen i Sverige for å få nærmere informasjon. FRA-lovens hovedformål er å regulere regjeringens og forsvarsmaktens adgang til å innhente elektroniske signaler. Dette innebærer at operatører som eier kabelnett plikter å føre alle signaler som krysser Sveriges grense til såkalte ”samverkanspunkter” hvor Forsvarets radioanstalt kan utøve sin kontroll.

Det er PTs forståelse at det knytter seg uklarheter til den praktiske gjennomføringen av FRA-loven. Tilsvarende gjelder også for den praktiske tilnærmingen til hvordan trafikk/signaler skal innhentes og bearbeides.

FRA-loven har skapt mye debatt internt i Sverige og i september d.å. sendte den svenske regjerningen ut en pressemelding hvor en del tillegg (”kompletteringar”) til FRA-loven ble presentert. Disse endringene er ikke vedtatt i lovs form. Det fremstår derfor som uklart for PT hvilken rettslig status og rekkevidde denne pressemeldingen har.

PT har også foretatt en vurdering av tilsvarende regelverk i Danmark, Storbritannia og Tyskland. Danmark har ikke noen lovgivning tilsvarende den svenske FRA-loven, men har gjennomført EUs datalagringsdirektiv. I den forbindelse er det gitt pålegg til tilbyderne om omfattende registrering og lagring av opplysninger knyttet til elektronisk kommunikasjon, herunder datatrafikk og bruk av Internett. Storbritannia har heller ikke en lov som er direkte sammenlignbar med FRA-loven, men PT antar at britenes generelle lov om overvåking ”The Regulation of Investigatory Powers Act” (RIPA) gir myndighetene hjemmel for å kunne utføre tilsvarende type masseovervåking som FRA-loven gir. Den tyske loven har likhetstrekk med FRA-loven. Den sier blant annet noe om hvilke søkebegrep som tillates brukt i forbindelse med masseovervåking.

Generelt anbefaler PT at privatpersoner og bedrifter er bevisste på hvilke elektroniske kommunikasjonstjenester man benytter for å overføre sensitiv informasjon. Det kan være hensiktsmessig å benytte krypteringsmetoder for å beskytte sin kommunikasjon der det er mulig.

Innhold

1 Innledning

Den såkalte FRA-loven som ble vedtatt i Sverige 18.juni i år har medført mye medieomtale og debatt både i Sverige, Norge og Norden forøvrig. FRA-loven åpner for en utvidet adgang til kommunikasjonskontroll av signaler som sendes i kabler over svensk territorium. Samferdselsdepartementet har i brev 27.08.08 gitt Post- og teletilsynet (PT) i oppdrag å utrede juridiske og tekniske forhold knyttet til ruting av elektronisk kommunikasjon via Sverige. Departementet har spesielt ønsket å få belyst følgende forhold:

- Rekkevidden av FRA-loven, hvilken myndighetskontroll som skal føres med FRAs virksomhet og hvordan tilrettelegging av kommunikasjonskontrollen skal foregå

- Avklare hvordan transittrafikk som går gjennom Sverige er omfattet av regelverket

- Kartlegge tilsvarende regelverk i andre land som det er naturlig å sammenligne med

- Kartlegge hvordan elektronisk kommunikasjon til/fra Norge i hovedsak blir rutet og undersøke hvorvidt det er alternativer til dagens trafikkruting mot utlandet.

I dette arbeidet har PT hatt kontakt med Post- och telestyrelsen i Sverige for å få en best mulig forståelse av FRA-loven og hvordan den vil bli gjennomført i praksis. Det er også foretatt informasjonsinnhenting og vurdering av tilsvarende regelverk i nære naboland som Danmark, Storbritannia og Tyskland.

PT har i samarbeid med de viktigste teletilbyderne på det norske markedet foretatt en kartlegging av den faktiske situasjonen når det gjelder ruting av elektronisk kommunikasjon til og fra Norge. Det er i denne sammenheng avholdt møter med Telenor, Tele2, TDC, NetCom og BaneTele. I tillegg er det også samlet inn informasjon fra enkelte andre tilbydere. Det er undersøkt hvilke fysiske fremføringsveier som benyttes og hvordan telefoni og datatjenester blir rutet. I tillegg er avhengigheten av svensk infrastruktur i innenlandsk tjenesteproduksjon blitt undersøkt siden flere store tilbydere i Norge er datterselskaper av svenske teletilbydere, og disse har i en del tilfeller en sterk operativ integrasjon med morselskapet.

PT har ikke vurdert personvernmessige konsekvenser av FRA-loven siden Fornyings- og administrasjonsdepartementet har gitt Datatilsynet i oppdrag å utrede dette. Det har vært en uformell kontakt mellom tilsynene i arbeidet med saken.

2 FRA-loven i Sverige

2.1 Rettskilder

”Lag om signalspaning i försvarsunderrättelseverksamhet” (FRA-loven) ble vedtatt av Riksdagen i juni 2008 og skal tre i kraft 1.1.2009. I september d.å. kom imidlertid Regeringskansliet med en pressemelding hvor det gis uttrykk for at man vil foreta visse justeringer i den eksisterende lovgivning. Dette vil bli kommentert i kap. 2.6.

I det følgende vil det gjøres rede for PTs forståelse av FRA-lovens formål og rekkevidde, herunder tilsynsordninger og forholdet til tilretteleggingsplikten.

Vurderingene er foretatt på bakgrunn av lovtekstene i FRA-lagen (lag 2008: 717), ”Lag om försvarsunderrättelseverksamhet” (lag 2000:130), ”Lag om elektronisk kommunikation” (lag 2003:389) samt Regjeringens proposisjon 2006/07:63 ”En anpassad försvarsunderrättelsesvirksomhet” og Regjeringens pressemelding fra 25. september 2008.

2.2 Nærmere om Försvarets radioanstalt (FRA)

FRA er i dag en sivil etat underlagt det svenske Forsvarsdepartementet. FRA ble etablert i 1942, og har pr. i dag 650 ansatte og et budsjett for 2008 på 562 millioner svenske kroner. I følge svenske medier planlegger FRA å ansette ytterligere 250 personer.

Ansvaret til FRA kan deles inn i to kjernevirksomheter:

- ”Signalunderrettningstjenesten” - kartlegging av ytre (utenlandske) trusler mot landet, samt gi støtte til svensk utenriks-, forsvars- og sikkerhetspolitikk

- ”Informasjonssikkerhetstjenesten” - bistå statlige etater med sårbarhets- og risikoanalyser i forbindelse med informasjonssikkerhet

FRA mottar i dag sine oppdrag fra følgende myndigheter:

- Regeringen
- Försvarsmakten
- Rikspolisstyrelsen
- Inspektionen för strategiska produkter (statlig myndighet som kontrollerer Sveriges eksport av forsvarsmateriell og andre strategiske produkter)
- Tullverket
- Försvarets materielverk
- Totalförsvarets forskningsinstitut
- Krisberedskapsmyndigheten

2.3 Om FRA-loven og sentrale bestemmelser

2.3.1 Formålsbestemmelse

Slik Post- og teletilsynet oppfatter FRA-loven § 1[1] er det den myndighet som regjeringen utpeker; dvs. signalspaningsmyndigheten, som kan innhente signaler i elektronisk form ved signalspaning. I henhold til regjeringens proposisjon[2] er det Försvarets radioanstalt som skal utøve denne aktiviteten.

Det følger av § 1 første ledd at slik aktivitet kan utøves i "försvarsunderrettelsessvirksomhet" og det henvises i den forbindelse til "Lag om försvarsunderrättelsesvirksomhet".

Denne loven regulerer oppgaver og arbeidsformer for forsvarsetterretningsvirksomhet (jfr. proposisjonens side 18) og ble endret samtidig med at FRA-loven ble vedtatt.

I henhold til "Lag om försvarsunderrättelsesvirksomhet"[3] § 1 skal etterretning utføres til støtte for svensk utenriks, sikkerhets- og forsvarspolitikk, samt kartlegging av ytre trusler mot landet. Det sistnevnte innebærer en endring da det før lovrevisjonen kun var ytre militære trusler som var omfattet av etterretningstjenestens mandat. I proposisjonen (side 33) har man nevnt aktiviteter som terrorisme, spredning av masseødeleggelsesvåpen, internasjonal kriminalitet og trusler mot teknisk infrastruktur; da særlig tele- og datasystem, som konkrete eksempler på hva som nå vil omfattes av regelverket.

Etter PTs forståelse danner formålsbestemmelsen i "Lag om försvarsunderrättelsesvirksomhet" yttergrensen for FRA-lovens virkeområde.

Dersom det er nødvendig for "försvarsunderrättelsesverksamheten" kan signaler i elektronisk form imidlertid også innhentes med den hensikt å følge den tekniske utviklingen for å kunne oppdatere teknisk kompetanse og metodikk som er nødvendig for å utføre etterretning i henhold til FRA-lovens formål jfr. § 1.

2.3.2 Utenlandsk trafikk og signaler, herunder transittrafikk

I henhold til FRA-loven § 2 kan relevant myndighet innhente elektroniske signaler som "förs över Sveriges gräns i tråd som ägs av en operatör".

Slik PT har forstått bestemmelsen innebærer dette at alle elektroniske signaler som føres i alle former for fysiske kabler over Sveriges riksgrense i prinsippet kan innhentes av Försvares radioanstalt. Innenlands trafikk som ikke rutes over grensen vil imidlertid ikke omfattes av loven jfr. side 74 i proposisjonen.

Etter tilsynets oppfatning medfører dette at norsk trafikk i transitt via Sverige, dvs trafikk som verken origineres eller termineres i Sverige også omfattes av FRA-loven.

FRA-loven omfatter kun operatører som eier kabelinfrastruktur. I forhold til operatørbegrepet i den svenske ekomloven kapittel 1 § 7 innsnevres imidlertid FRA-loven til kun å omfatte operatører som har eiendomsretten til de fysiske kablene.

Det uttales i proposisjonen (side 84) at det på bakgrunn av denne begrensningen antas at det er et titalls operatører som vil omfattes av bestemmelsen i FRA-loven § 2.

Som en følge av det ovenfornevnte er tilretteleggingsplikten for disse operatørene endret. En nærmere redegjørelse for PTs forståelse av dette følger i kap. 2.5.

[1] FRA-loven: http://www.riksdagen.se/webbnav/index.aspx?nid=3911&bet=2008:717
[2] Proposition 2006/07:63 http://www.riksdagen.se/webbnav/index.aspx?nid=37&dok_id=GU0363
[3] Lag om försvarsunderrättelsesverksamhet: http://www.riksdagen.se/webbnav/index.aspx?nid=3911&bet=2000:130

2.3.3 Bruk av søkeord

I henhold til FRA-loven § 3 skal innhenting skje automatisert. For å begrense søkene til kun å omfatte relevant informasjon, må Försvarets radioanstalt benytte seg av såkalte søkeord i forbindelse med kontroll av trafikk. Søkeordene skal formuleres og anvendes på et slikt vis at det gir minst mulig inngrep i personlig integritet. Dersom det ikke er av betydelig viktighet for etterretningen kan enkeltpersoners navn, eller opplysninger som kan knyttes direkte til en konkret person, ikke brukes som søkeord. Slik PT har forstått forarbeidene, se proposisjonen side 90, innebærer dette at personnavn, telefonnummer, e-postadresser, IP-adresser og lignende som kan knyttes til en person bare kan anvendes i søkeord dersom det er av "synnerlig vikt for verksamheten" jfr. § 3 siste ledd.

Kombinasjoner av tekniske data og nøkkelord som f.eks. navn på særskilte våpensystem er eksempel på hva søkeord kan inneholde (jf. proposisjonen side 77)

2.3.4 Tillatelse til å utføre signalspaning [4]

Det følger av FRA-loven § 5 at forhåndstillatelse til å drive signalspaning kreves dersom dette anmodes av andre myndigheter enn Regjering eller Regeringskansliet. Tillatelse kan gis for maks seks måneder fra og med dagen beslutning om tillatelse gis. Det presiseres videre i § 5 annet ledd at tillatelse til signalspaning kun kan gis der formålet med innhenting av signaler samsvarer med formålet med forsvarsetterretning slik det er definert i "Lag om försvarsunderrättelsesverksamhet", og der hensynet til etterretningsformål veier klart tyngre enn hensynet til personlig integritet.

I hastetilfeller kan imidlertid myndigheten innhente trafikk uten forhåndstillatelse. Dette skal umiddelbart meddeles organet som skal gi tillatelse, og dersom denne myndigheten finner at vilkår for signalspaning ikke er tilstede skal innhentingen umiddelbart avbrytes.

2.3.5 Myndighetsorgan som skal gi tillatelse [4]

Tillatelse skal gis av den myndighet regjeringen bestemmer jfr. FRA-loven § 6. I henhold til PTs forståelse følger det av proposisjonen side 100-101 at det er Försvarets underrättelsesnämnd[5]som skal gi tillatelser til å innhente trafikk i henhold til lov om signalspaning. Nemndens oppgaver er pr. dags dato å føre tilsyn med signalspaningsmyndigheten og annen forsvarsetterretning. Nemnden kontrollerer også behandling av personopplysninger i forsvarsmaktens etterretningstjeneste, det militære sikkerhetspolitiet og Försvarets radioanstalt. Försvarets underrättelsesnämnd utfører tilsyn gjennom inspeksjoner og andre undersøkelser.

2.4 Tilsyn med loven

Den myndighet som regjeringen bestemmer skal kontrollere at loven følges jfr. FRA-loven § 10. Denne myndigheten kan beslutte at pågående signalspaning skal opphøre eller at innhentede opplysninger skal ødelegges, dersom innhentingen ikke kan sies å være forenlig med FRA-loven.

[4] Endringer fremkommer av Regeringskansliets pressemelding av 25 september se kap. 2.6

[5] Nemndens mandat reguleres i Förordning (2007:852) med instruktion för Försvarets underrättelsenämnd: http://www.riksdagen.se/webbnav/index.aspx?nid=3911&bet=2007:852

Slik PT oppfatter loven jamført med proposisjonen (side 116) er det Försvarets underättelsesnämnd som skal ha tilsynsfunksjon med regelverket. I henhold til § 10 er det et særskilt organ innenfor nemnden som skal føre tilsyn. Medlemmene skal utnevnes av regjeringen for en bestemt tid, minst fire år. Leder og nestleder skal være, eller ha vært, ordinære dommere.

Det presiseres i § 10 siste ledd at den delen av myndigheten som gir tillatelse i henhold til § 5 ikke skal delta i tilsynsvirksomheten.

2.5 Tilretteleggingsplikt og forholdet til "Lag om elektronisk kommunikation"

2.5.1 Fysisk overlevering av signaler

Vedtagelsen av FRA-loven har medført endringer i tilbydernes tilretteleggingsplikt, og som en følge av dette har man fått ny § 19a i ekomlovens kapittel 6[6] som skal tre i kraft 1.1.2009.

Bestemmelsen innebærer at operatører som "äger tråd i vilka signaler som förs över Sveriges gräns" er pliktige til å føre signalene til såkalte "samverkanspunkt". På bakgrunn av proposisjonen er det PTs oppfatning at denne tilretteleggingsplikten retter seg kun mot tilbydere som eier kabel (tråd) jfr. drøftelse under pkt. 2.3.2

"Samverkanspunkt" er beskrevet (proposisjonen side 85 flg) som en plass der trafikk skal overlates fra kabeleiende tilbyder til myndighetene; dvs. Försvarets radioanstalt. Operatøren har ansvaret for at trafikken overføres til disse punktene, og må bære kostnadene ved å bringe signalene til "samverkanspunkt" som operatøren har valgt. Operatøren har imidlertid ikke ansvar for oppføringen eller kostnader knyttet til "samverkanspunkt", og det er signalspaningsmyndigheten som forvalter signalene når trafikken er overført til punktene.

I henhold til svensk ekomlov kap 6 § 19a kan Regjeringen eller tilsynsmyndigheten gi forskrifter om "samverkanspunkt". Forhold som antas å være aktuelle er antall punkter, beliggenhet, sikkerhetsnivå og myndigheters tilgang. Etter PTs oppfatning er det svenske Post- och telestyrelsen som kan gi forskrifter på området. Pr. dags dato er det ikke gitt forskrifter knyttet til dette, og etter PTs forståelse er det heller ikke satt i gang forskriftsarbeid på bakgrunn av ekomloven kap. 6 § 19a.

2.5.2 Tilbydere som ikke eier eget kabelnett

Det følger av ekomloven §19a annet ledd at samtlige operatører som fører signaler i kabel over Sveriges grense skal overlevere informasjon til myndighetene med det formål å gjøre det enklere å behandle innhentede signaler.

Bestemmelsen er kommentert på side 86 i proposisjonen, og etter PTs forståelse skal begrepet operatør i denne sammenhengen tolkes i henhold til legaldefinisjonen i ekomloven kapittel 1 § 7. Dette innebærer at også tilbydere/operatører som ikke har juridisk eiendomsrett til kabel omfattet av plikten i annet ledd; i følge proposisjonen omfattes "trådägare, Internet Service Providers (ISP) m.fl." Det sies videre at dersom formålet med signalspaning skal kunne oppfylles, må signaler i elektronisk form enkelt kunne håndteres av signalspaningsmyndigheten. Dette innebærer blant annet at myndigheten må begrense mengden informasjon som innhentes, og

[6] Lag om elektronisk kommunikation: http://www.riksdagen.se/webbnav/index.aspx?nid=3911&dok_id=SFS2003:389&rm=2003&bet=2003:389

irrelevante informasjonsmengder sorteres bort. Dersom dette skal kunne gjennomføres trenger signalspaningsmyndigheten i enkelte sammenhenger informasjon fra operatørene; også fra de som ikke er kabeleiere. Dette kan for eksempel være opplysninger som beskriver teknisk og logisk arkitektur, båndbredde, signaleringstyper m.m. Det følger også av proposisjonen at slike opplysninger er nødvendige for FRAs videre foredling av innhentet informasjon.

Slik PT forstår proposisjonen (side 86) er utlevering av detaljopplysninger om spesielle parametre for integritets- og kommunikasjonsvern, for eksempel krypteringsløsninger som operatøren tilbyr direkte til kunder, ikke omfattet av plikten etter § 19a annet ledd.

2.6 Meddelelsen fra Regeringskansliet 25.9.2008

Den 25.09 2008 publiserte Regeringskansliet en pressemelding[7]hvor det sies at alliansepartiene (regjeringspartiene) har kommet til enighet om tillegg til FRA-loven. Disse endringene har til hensikt å forsterke personlig integritet ved å innføre tydeligere regulering og forbedrede kontrollmuligheter av signalspaningen.

Endringene er fremlagt som en liste med 15 punkter. De forhold som anses mest sentrale gjengis i det følgende:

- Tillatelse til å bedrive signalspaning skal gis av domstol[8]
- FRA må søke tillatelse for all signalspaning, også i forbindelse med anmodninger fra Regjeringen
- FRA skal bare få tilgang til de "trafikkstråk"[9] domstolen bestemmer
- Det skal tydeliggjøres i loven at FRA ikke kan signalspane på trafikk som ikke passerer Sveriges riksgrense
- FRA kan bare bedrive signalspaning etter anmodning fra Regjeringen, Regeringskansliet og forsvarsmakten
- Det skal settes i gang en utredning for å kartlegge politiets og sikkerhetspolitiets behov for etterretningsopplysninger
- Søkeord som direkte kan knyttes til et enkeltindivid kan ikke benyttes uten særskilt tillatelse
- Kontrollmyndighetens selvstendighet og forutsetninger for juridisk etterhåndskontroll skal forsterkes
- Råmateriale skal ikke lagres lenger enn ett år

Disse endringene er ikke vedtatt i lovs form. Det fremstår derfor som uklart for PT hvilken rettslig status og rekkevidde denne pressemeldingen har i forhold til "Lag om signalspaning i försvarsunderrättelseverksamhet".

[7] Regeringskansliets pressemelding av 25.9-08: http://www.regeringen.se/sb/d/10911/a/112332
[8] Det fremgår ikke av meddelelsen hva slags domstol dette dreier seg om
[9] Det er uklart for PT hva som legges i dette begrepet

.

3 Situasjonen i andre land

3.1 Danmark

Danmark har ikke noen lovgivning tilsvarende den svenske FRA-loven. Med hjemmel i Retsplejeloven[10] ble imidlertid datalagringsdirektivet (Europaparlaments- og rådsdirektiv 2006/24 EF av 15. mars 2006) gjennomført i dansk rett med virkning fra 15. september 2007. Nærmere bestemmelser om gjennomføringen er gitt i Justisministeriets tilhørende bekjentgjørelse av 28. september 2006[11] som fastsetter plikter for tilbydere av elektroniske kommunikasjonsnett og –tjenester til sluttbruker til å foreta registrering og oppbevaring (lagring) av opplysninger om teletrafikk.

Bekjentgjørelsen gir omfattende plikter til å registrere og lagre opplysninger om teletrafikk. For fastnett og mobilkommunikasjon samt SMS og MMS skal blant annet følgende registreres og oppbevares: A- og B-nummer samt navn og adresse på abonnent eller registrert bruker, eventuelle IMSI- og IMEI-numre, basestasjonsopplysninger, tidspunktet for start og avslutning for kommunikasjonen, samt for anonyme telekort tidspunktet for første aktivering.

Når det gjelder internett skal tilbyder med forbehold om teknisk mulighet registrere følgende om sesjonens innledende og avsluttende pakke: Avsenders og mottakers Internetprotokoll-adresse samt portnumre, transportprotokoll samt tidspunktet for kommunikasjonens start og avslutning. Videre skal blant annet følgende opplysninger om sluttbrukers adgang til Internett registreres: Tildelt brukeridentitet og telefonnr. der kommunikasjonen inngår i et offentlig telenett, navn og adresse på abonnent eller bruker samt vedkommendes Internettprotokoll-adresse, brukeridentitet eller telefonnr og tidspunktet for kommunikasjonens start og avslutning. For tilbydere av trådløs tilgang til internett til sluttbrukere skal det også registreres opplysninger om det lokale nettverkets geografiske eller fysiske plassering samt identiteten til det benyttede kommunikasjonsutstyr. Den fastsatte lagringstid er 1 år.

Dansk lovgivnings regler om tilgang til lagrede data tilsvarer i stor grad det som gjelder for politiets adgang til kommunikasjonskontroll etter reglene i norsk straffeprosess. Etter reglene i den danske Retsplejeloven må det foreligge mistanke om overtredelse av konkrete straffebestemmelser og det gjelder i hovedsak et krav om straffenivå. Tillatelse til kommunikasjonskontroll må gis av en dommer. Kommunikasjonskontroll kan ikke foretas av andre enn politiet. Det gjelder også andre rettsikkerhetsbestemmelser, blant annet om rett til forsvarer og underretning om kommunikasjonskontroll som gjennomføres.

3.2 Storbritannia

I Storbritannia er det "The Regulation of Investigatory Powers Act"[12] (RIPA) fra år 2000 som regulerer myndighetenes adgang til overvåking. Loven er generell og den er derfor vanskelig å sammenligne direkte med FRA-loven som dekker et mer begrenset område. PT vil imidlertid gjøre rede for de forhold som antas å dekke de samme forhold som FRA-loven.

RIPA er teknologinøytral og defininerer overvåking i section 2 (2) som ethvert inngrep eller modifikasjon i elektroniske kommunikasjonssystemer med sikte på å gjøre kommunikasjonen

[10] https://www.retsinformation.dk/Forms/R0710.aspx?id=116587
[11] https://www.retsinformation.dk/Forms/R0710.aspx?id=2445
https://www.retsinformation.dk/Forms/R0710.aspx?id=2446
[12] RIPA-loven: http://www.opsi.gov.uk/acts/acts2000/ukpga_20000023_en_1

tilgjengelig til en person som ikke er avsenderen eller den tilsiktede mottakeren. Loven vil derfor gjelde overvåking av elektronisk kommunikasjon i kabel. Overvåkning er ulovlig med mindre bestemmelsene i RIPA gir hjemmel for at myndighetene kan drive overvåkning.

PT oppfatter RIPA slik at den også dekker overvåking av elektronisk kommunikasjon i kabel som krysser grensene til Storbritannia.

Secretary of State (en person på ministernivå) kan gi tillatelse til overvåkning. Et vilkår for å kunne utstede en tilltatelse til overvåkning er at den er påkrevet (”necessary”) i forhold til nasjonal sikkerhet, bekjempelse av alvorlig kriminalitet og hensynet til ”safeguarding the economic well-being of the United Kingdom”. En tilltatelse vil også kunne utstedes på bakgrunn av gjensidig avtale med et annet land. Overvåkning må videre være forholdsmessig i forhold til det som søkes oppnådd ved overvåkningen.

I section 6 er det fastsatt hvilke myndighetspersoner som kan søke om en tillatelse til overvåkning. Direktøren for Government Communications Headquarters (GCHQ) har blant annet rett til å søke om tillatelse. GCHQ har tilsvarende oppgaver som FRA.

RIPA stiller krav til at tillatelsen må beskrive personen eller de fysiske lokasjonene som skal overvåkes. Videre må tillatelsen inneholde en nærmere beskrivelse av overvåkningen, slik som for eksempel hvilke telefonnummer og e-postadresser som skal overvåkes. RIPA section 9 inneholder videre krav til tillatelsens varighet, opphør og fornyelse.

Opplysningene fremskaffet ved overvåkning kan som hovedregel ikke brukes som bevis. Opplysningene brukes for å forebygge/forhindre alvorlig kriminalitet og terroristhandlinger.

RIPA fastsetter at det skal oppnevnes en person som skal føre tilsyn med at overvåkningen av kommunikasjon skjer i henhold til regelverket. Vedkommende rapporterer til statsministeren dersom det blir funnet avvik. RIPA fastsetter videre at det skal være et klageorgan for personer som mener seg utsatt for ulovlig overvåkning.

Gjeldende lovgivning, og ikke minst praksis, i Storbritannia har blitt utsatt for kritikk. Loven gir i utgangspunktet en begrenset krets av myndighetsorganer rett til å søke om tillatelse til overvåkning. Denne kretsen er blitt sterkt utvidet og inkluderer også lokale myndigheter. I pressen er det flere eksempler på at overvåking som skal ha gått utover de formål som loven angir.

I saken ”Liberty and Others v. The United Kingdom”[13] fra 2008 som blant annet gjaldt Storbritannias overvåking av teletrafikk fra Irland kom Den europeiske menneskerettighetsdomstolen frem til at Storbritannia hadde opptrådt i strid med artikkel 8 i Den europeiske menneskerettighetskonvensjonen. Denne saken er imidlertid basert på loven som gjaldt før RIPA.

3.3 Tyskland

I Tyskland er det ”Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses”[14] fra 1968 som regulerer myndighetenes adgang til overvåking. Loven kalles ofte ”G-10-gesetz” da den har sitt utspring fra grunnlovens artikkel 10. Adgangen til overvåking ble vesentlig utvidet i 1994 i forbindelse med en ny lov om kriminalitetsbekjempelse.

Loven regulerer myndighetenes adgang til å overvåke post og telekommunikasjon og gir adgang til både individuell overvåking av personer og masseovervåking. Myndighetene som kan søke om å få tillatelse til overvåking er ”das Bundesamt für Verfassungsschutz” og ”die Verfassungsschutzbehörden der Länder”. Dette er organer som har med beskyttelse av

[13] Dommen er omtalt her: http://www.echr.coe.int/echr/
[14] Tysk overvåkingslov: http://www.gesetze-im-internet.de/g10_2001/BJNR125410001.html

grunnloven å gjøre. Ellers har militær etterretningstjeneste og ”Bundesnachrichtendienst” (BND) rett til å søke om tillatelse. Sistnevnte organisasjon har tilsvarende oppgaver som FRA.

Tillatelser til overvåking gis etter det PT forstår av ministeren som har sektoransvaret for den etaten som søker om overvåkning. I saker som har med beskyttelse av grunnloven å gjøre er det i noen tilfeller øverste regionale myndighet som gir tillatelsen.

Generell overvåkning i form av signalspaning kan ifølge lovens § 5 bare iverksettes når innhenting av informasjon er nødvendig for å avverge væpnede angrep mot Tyskland, terroranslag, ulovlig våpenhandel, ulovlig innføring av større partier narkotika, destabilisering av pengevesenet på bakgrunn av pengeforfalskning i utlandet og organisert hvitvasking av penger.

PT forstår det slik at det er Bundesnachrichtendienst (BND) som utfører overvåkingen.

”G-10-gesetz” stiller krav om hvilke søkebegrep BND kan benytte i forbindelse med masseovervåking. BND har bare lov til å bruke søkebegrep som er egnet til å avdekke informasjon om forholdene angitt i tillatelsen til overvåkning. Søkebegrepene skal fremgå av tillatelsen og må som hovedregel utformes slik at de ikke er rettet mot bestemte telefontilknytninger.

Overvåkingen er underlagt parlamentarisk kontroll og en spesialoppnevnt kommisjon (G 10-kommisjonen).

I beslutningen ”Weber and Saravia v. Germany”[15] fra 2006 som også gjaldt masseovervåking avviste Den europeiske menneskerettighetsdomstolen at Tyskland hadde opptrådt i strid med Den europeiske menneskerettighetskonvensjonen.

[15] Dommen er omtalt her: http://www.echr.coe.int/echr/

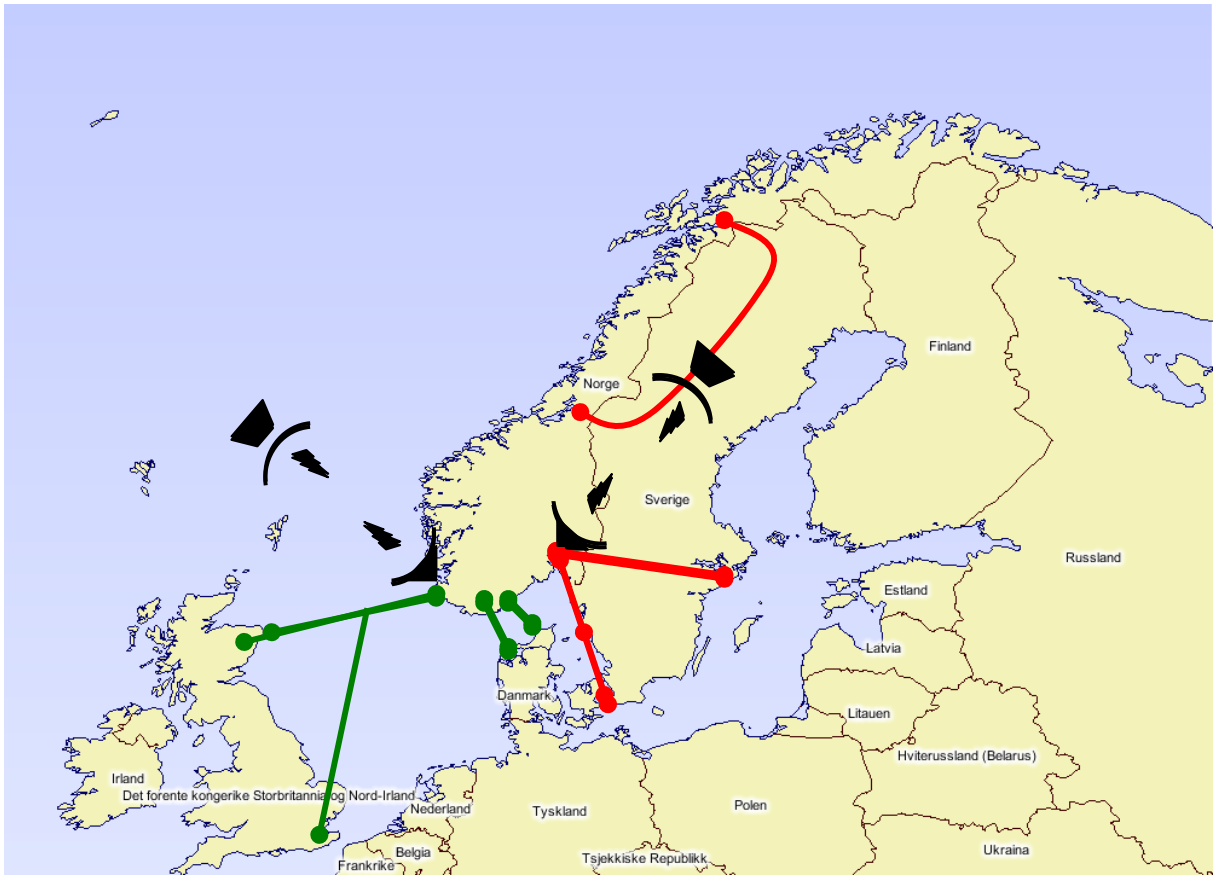
4 Ruting av elektronisk kommunikasjon til/fra Norge

4.1 Fysiske kommunikasjonsveier ut av Norge

Offentlige ekomnett i Norge er forbundet med ekomnett i andre land via kabler over land og sjø, samt via satellitt. Mesteparten av trafikken inn og ut av Norge formidles over høykapasitets fiberforbindelser.

Trafikk til og fra utlandet termineres i all hovedsak i svitsjepunkter i Østlandsområdet, hvor det meste av sentral infrastruktur for nasjonal tjenesteproduksjon av ekomtjenester er lokalisert. Normalt sikrer de ulike tilbydere redundans i nettet ved å benytte to ulike forbindelser for ruting av trafikk og dette oppnås typisk gjennom ringstrukturer.

Figuren nedenfor indikerer kommunikasjonsveiene ut av Norge slik de benyttes pr. i dag. Figuren viser de landbaserte (**røde**), sjøbaserte (**grønne**) og satelittbaserte (**svart**) hovedforbindelsene.



(kartkilde: www.globalis.no)

Figur 1. Oversikt over de viktigste kommunikasjonsveiene ut av Norge

Overføringskapasiteten i en kabel er avhengig av antall fiberpar og type multipleksingssystem som kan utnytte hvert fiberpar i form av flere optiske kanaler (bølgelengder). PTs forståelse er at behovet for fysiske kabler synes å være dekket av eksisterende kabelinfrastruktur og at trafikkveksten håndteres ved hjelp av økt kapasitet ved multipleksing.

4.1.1 Landbaserte forbindelser

Alle landsbaserte forbindelser mellom offentlige ekomnett i Norge og ekomnett i andre land går via Sverige.Trafikken rutes via 4 knutepunkter (Halden, Kongsvinger, Stjørdal og Narvik) hvorav de to sørligste formidler hovedtyngden av trafikk mot utlandet og disse inngår dessuten i en nordisk ringstruktur.De to nordligste knutepunktene har lavere kapasitet og benyttes mest for å sikre redundans i forbindelsen mellom Nord-Norge og det øvrige Norge.

De fysiske kablene som brukes eies dels av Jernbaneverket med BaneTele AS som operatør, og dels av Telenor som eier og operatør. Det er samarbeid mellom norske og svenske operatører om gjensidig utnyttelse av fiberkabler på hver side av grensen.

4.1.2 Sjøbaserte forbindelser

I tillegg til de landbaserte kommunikasjonsforbindelsene mot Sverige benyttes også fiberoptiske sjøkabler. To hovedforbindelser er i bruk. Den ene sjøkabelen går fra Kristiansand/Arendal over Skagerak til Danmark. Den andre sjøkabelen går fra Stavanger/Haugesund over Nordsjøen til Storbritannia. I forhold til de landbaserte hovedforbindelsene via Sverige representerer de sjøbaserte forbindelsene mindre kapasitet, både med hensyn til antall fiberpar og antall multipleksede kanaler.

De sjøbaserte kablene opereres av TDC Norge AS og North Sea Communications (NSC).

Disse sjøkabelforbindelsene representerer et mulig alternativ til ruting via Sverige og er nærmere omtalt i kapittel 4.5.

4.1.3 Satellittbaserte forbindelser

Satellittbaserte forbindelser går via jordstasjoner i Norge. Det er per i dag to slike jordstasjoner (i Rogaland og Akershus) som formidler trafikk til/fra norske offentlige ekomnett via satellittnettverk som Inmarsat, Thuraia og Iridium. Kapasiteten er svært lav sammenlignet med de kabelbaserte forbindelsene, i praksis representerer dette promiller av kapasiteten totalt.

Jordstasjonene eies av Apax Partners og opereres av Vizada (inkluderer tidligere Telenor Satellite Services).

Disse satelittforbindelsene representerer på grunn av lav kapasitet ikke noe reelt alternativ til ruting via Sverige. Tradisjonelt er det også satellittkommunikasjon som spesielt har vært gjenstand for den type overvåking som FRA og tilsvarende organisasjoner utfører.

4.2 Status for ruting av internasjonal trafikk

4.2.1 Telefoni

Telefonitrafikken mot utlandet til/fra norske kunder inkluderer fasttelefoni, mobiltelefoni og bredbåndstelefoni. I all hovedsak rutes denne trafikken for de fleste tilbydere via kabelforbindelser mellom Norge og Sverige. Internasjonale aktører som bl.a Telenor Global Services og Telia Sonera International Carrier benyttes i stor grad som transportører. Disse har infrastruktur som inngår i en nordisk ringstruktur med internasjonale forbindelser via Sverige (Stockholm og Malmø).

En mindre del av trafikken rutes direkte mellom Norge og Danmark via TDC Wholesale International's nett.

En svært liten del av telefonitrafikken formidles via jordstasjoner for satellitt.

Ved ruting av telefonitrafikk kan signaleringen knyttet til samtalen og selve talesignalet rutes over forskjellige forbindelser. Dette gjelder også for samtaler mellom Norge og utlandet. Kommunikasjonskontroll av en telefonsamtale krever tilgang til begge typer informasjon.

4.2.2 Datakommunikasjon

Datatrafikken mot utlandet omfatter bl.a tjenester som SMS, MMS, Internett og e-post. Kommunikasjonen kan skje over ulike aksesstyper, både faste og mobile.

Internasjonal datatrafikk rutes i all hovedsak via kabelforbindelser mellom Norge og Sverige, og over de samme fysiske transmisjonsnett som benyttes for telefoni.

En mindre del av trafikken rutes via sjøkabelforbindelser mellom Norge og hhv. Danmark og Storbritannia. En svært liten del av datakommunikasjon formidles via jordstasjoner for satellitt.

Internasjonal Internettrafikk formidlet via NIX[16] i Norge rutes i hovedsak også via Sverige.

Signalene (datapakker) som er knyttet til en bestemt dataoverføring (sesjon) mellom brukere i Norge og utlandet, kan bli spredd på ulike ruter som kan involvere flere av de fysiske forbindelsene til utlandet.

4.3 Innenlandstrafikk i transitt via Sverige

4.3.1 Telefoni

I følge informasjon som PT har fått fra telefonitilbydere som er kontaktet rutes innenlandske telefonsamtaler via transmisjonsforbindelser internt i Norge unntatt ved feilsituasjoner i nettet.

Enkelte tilbydere har noen tjenesteplattformer og støttesystemer i Sverige, i det vesentlige gjelder dette ruting av porterte nummer og meldingstjenester for mobiltelefoni. Se også kapittel 4.4.

[16] NIX er en betegnelse på Norwegian Internet eXchange. NIX sørger for utveksling av Internetttrafikk mellom norsk tilbydere. Se http://www.uio.no/nix/ .

Tilbydere av transporttjenester for elektronisk kommunikasjon i Norge har planlagt og lagt til rette for å utnytte transmisjonsnett i Sverige ved feil i det norske nettet. Dette gjelder spesielt for kommunikasjon mellom Nord-Norge og landet for øvrig. Forbindelsene via Sverige er reservevei for ruting av trafikk og vil kun anvendes i situasjoner med omfattende feil i norsk del av nettet (brudd på flere forbindelser i Norge). De siste årenes utbygging av redundante forbindelser på norsk side har redusert betydningen av og bruken av forbindelser via Sverige.

4.3.2 Datakommunikasjon

For datakommunikasjon rutes trafikk mellom norske kunder i hovedsak via transmisjons-forbindelser i Norge da samtrafikk mellom tilbyderne i stor grad skjer via punkter lokalisert i Norge.

Enkelte tilbydere har noen tjenesteplattformer utenlands, i det vesentlige gjelder dette Internett, e-post og meldings-/innholdstjenester for mobiltelefoni. Se også kapittel 4.4.

Datakommunikasjon er tradisjonelt ikke strukturert på samme måte som telefoni med hensyn til ruting. Ruting av innenlands datakommunikasjon kan derfor i større utstrekning enn for telefoni skje via svensk infrastruktur av andre grunner enn feilsituasjoner. Dette skyldes dels prisbildet for transmisjonskapasitet, og at systemer for datakommunikasjon i større grad enn for telefoni utnyttes på tvers av landegrenser (for eksempel Internett og e-post). Det kan derfor være til dels store variasjoner mellom ulike tilbydere i hvilken grad tjenesteproduksjonen medfører ruting via Sverige.

4.4 Andre avhengigheter av svensk infrastruktur

Noen tilbydere på det norske markedet er eid av svenske teleselskaper og deler av den operative virksomheten i noen av disse selskaper er knyttet sammen med morselskapet i Sverige. Enkelte tjenester blir produsert med støtte i tekniske systemer som fysisk er plassert i Sverige.

Hos noen tilbydere blir driftstekniske systemer for nettovervåkning og kontroll plassert i Sverige også benyttet til driftskontroll av det norske nettet. Spesielt utenfor normal arbeidstid er det vanlig at slike funksjoner kan utføres fra Sverige.

Administrative systemer for ordremottak, fakturering og andre kundedata kan også i stor grad være integrert med IT-systemene i det svenske morselskapet. Det innebærer at en rekke data om norske kunder sendes til Sverige og blir lagret i datasystemer på svensk jord.

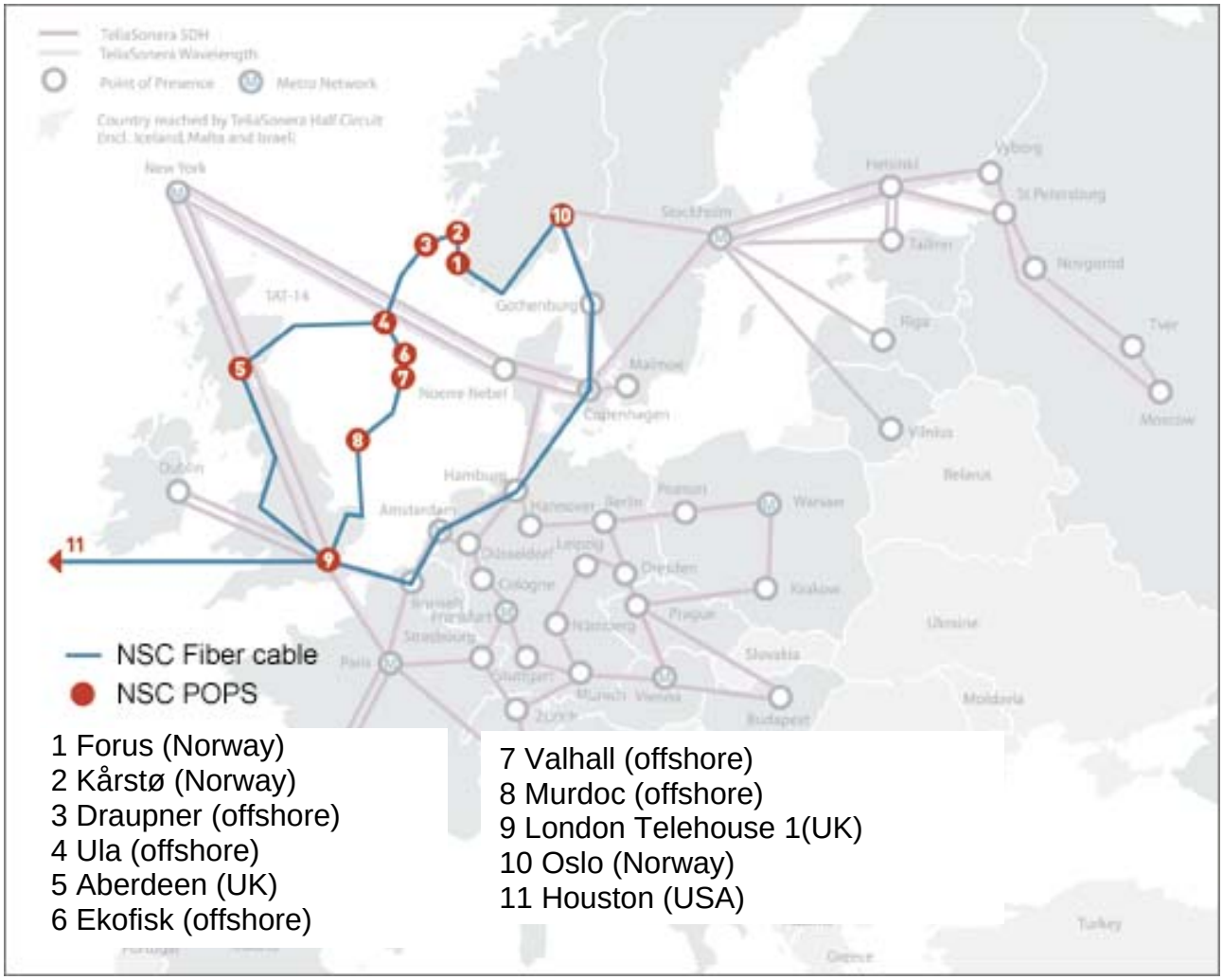
Enkelte selskaper opplyser at det stadig utvikles mer integrerte løsninger på tvers av grensen fordi dette gir synergigevinster og dermed kostnadsbesparelser for selskapet totalt sett. Det vil derfor medføre betydelige merkostnader å etablere helt separate tjenesteplattformer og støttesystemer for å betjene det norske markedet alene.

4.5 Alternative tekniske løsninger

Dersom mer utenlandstrafikk skal rutes utenom svensk territorium er det i praksis sjøkabelforbindelser over Skagerak og Nordsjøen til henholdsvis Danmark og Storbritannia som kan benyttes. Satellittforbindelser er også mulig, men denne kommunikasjonsformen er kostbar, har kapasitetsbegrensninger og benyttes i dag i lite omfang for vanlig telefoni og datakommunikasjon totalt sett.

Selskapet North Sea Communications (www.norseacom.com) tilbyr transmisjonskapasitet på sjøkabel mellom Norge og Storbritannia via offshore-installasjoner i Nordsjøen. Denne forbindelsen har både et tradisjonelt SDH-system og et moderne optisk multiplekssystem (DWDM) som gir kapasiteter på ca. 10 Gigabit/s mellom nettverksnodene. På henvendelse fra PT opplyser selskapet at det er mye ledig kapasitet på denne forbindelsen og selskapet selger gjerne mer kapasitet til norske tilbydere. Selskapet eies av TeliaSonera og inngår i et større internasjonalt nettverk.

Figur 2 viser et kart over forbindelsen som North Sea Communications opererer og hvilke tilkoplingspunkter som er tilgjengelig. I London har selskapet forbindelse til andre internasjonale nettverk for videre transitt. Men hvorvidt denne forbindelsen via Storbritannia er et bedre alternativ i forhold til muligheten for kommunikasjonskontroll av norsk trafikk er et annet spørsmål og det vises til omtale av regelverket i Storbritannia (se kap. 3.2)



Figur2. Sjøkabel til Storbritannia (kilde: North Sea Communications, www.norseacom.com)

Selskapet TDC Norge AS (www.tdc.no) tilbyr transmisjonskapasitet på sjøkabel mellom Norge og Danmark. Det er ikke klarlagt i hvilken grad disse sjøkablene har tilgjengelig kapasitet for ytterligere trafikk, da slik informasjon ikke har blitt gjort tilgjengelig for PT. Selskapet eies av det danske morselskapet TDC og kan tilby kommunikasjonsløsninger som inngår i et større internasjonalt nettverk (TDC Wholesale Infrastructure).

5 Andre relevante forhold

Når det gjelder potensiell overvåking av elektronisk kommunikasjon til/fra Norge kan det også være av interesse å kjenne til systemer og aktiviteter i andre land enn Sverige. Nedenfor er det gitt en kort omtale av noen relevante forhold.

5.1 "Echelon"-systemet

Echelon er en allianse mellom USA, Canada, Storbritannia, Australia og New Zealand om tilgang til-, og utveksling av etterretningsinformasjon framskaffet via overvåkning av elektronisk kommunikasjon. Man antar at systemet har vært i drift siden den kalde krigen og ble opprettet for å overvåke radiokommunikasjon i eller til Sovjetunionen og Øst-Europa. Systemets eksistens ble allment kjent som et resultat av en rapport[17] fra EU-parlamentets teknologivurderingsorgan STOA (Scientific Technology Options Assessment). Siden alliansen selv nektet å gi noen kommentar om systemets eksistens vedtok EU-parlamentet å nedsette en komité for å vurdere Echelons eksistens og metoder. Komiteens rapport konkluderte med at systemet finnes, og at formålet er å overvåke privat og forretningsmessig kommunikasjon, herunder satellittkommunikasjon, mobiltelefoni, radiolinjesystemer og kommunikasjon via fiberoptisk transmisjonssystemer. Rapporten antyder også at det er stor sannsynlighet for at det er flere nasjoner som bidrar til utveksling av innsamlet informasjon enn de som nevnes ovenfor.

Echelon synes å basere seg på noenlunde samme metoder som FRA ønsker å benytte i sin overvåkning. Kommunikasjonsmønstre gjennomgår spesielle analyser i kraftige datamaskiner hvor innholdet skannes for interessante søkeord. Meldinger som identifiseres av systemet som interessante kopieres så for manuell analyse.

Systemet er i dag basert på at det skal utføres total overvåking, hvilket medfører at alle former for elektronisk kommunikasjon – telefonsamtaler, SMS-er, fakser, e-post og internettrafikk – skal kunne overvåkes. For å ha mulighet til å drive denne formen for overvåkning må en anta at eier av anlegg og tekniske systemer, eller den som normalt har tilgang til disse, gir den som ønsker å overvåke fysisk tilgang til transmisjonsmediene.

Rapporten fra EU hadde en rekke anbefalinger vedrørende beskyttelsestiltak. Ett av dem var at EU aktivt gikk inn og støttet aktiviteter som hadde til formål å utvikle sikrere krypteringsmekanismer innenfor elektronisk kommunikasjon. Komiteens rapport påpekte at private brukere, bedrifter og myndigheter bør ha tilgang til mekanismer som gir mulighet til å beskytte seg mot Echelon og tilsvarende overvåkningssystemer.

5.2 Initiativ relatert til krypteringsteknikker

I 2004 ble et industriinitiativ, SECOQC (Secure Communication based on Quantum Cryptography), opprettet for å utvikle sikrere nøkkeldistribusjons- og krypteringsløsninger for fiberoptiske transmisjonssystemer. SECOQC ble samme år godkjent som et prosjekt under EUs 6. rammeprogram, og har i løpet av de fire siste årene mottatt 11 millioner Euro i støtte.

[17] http://www.fas.org/irp/program/process/rapport_echelon_en.pdf

Basert på resultatet fra SECOQC, opprettet ETSI (European Telecommunications Standards Institute) 28. juli 2008 ISG[18] (Industry Specification Group). Hovedansvaret til ISG blir å følge opp det arbeidet som SECOQC har gjennomført ved å utvikle globale standarder for nøkkeldistribusjon og kryptografiteknologi.

Om denne aktiviteten medfører at det utvikles tekniske løsninger som tilfredsstiller alle behov som anses nødvendig for å sikre konfidensialitet og integritet ved elektronisk kommunikasjon er usikkert på det nåværende tidspunk. ETSI skriver i sin pressemelding i forbindelse med opprettelse av ISG at det er økende interesse for å kunne beskytte seg mot "total" overvåkning (all-embracing surveillance).

I tilegg til denne komiteen finnes også ETSI SAGE (Security Algorithms Group of Experts). Denne ekspertgruppen utarbeider krypteringsalgoritmer som retter seg direkte mot utvalgte ekomtjenester, bl.a. GSM, GPRS, UMTS og TETRA. Denne komiteen har hatt norsk deltakelse.

I tillegg er det en rekke andre initiativ, både nasjonale og internasjonale, vedrørende utvikling av krypteringssystemer. PT har på det nåværende tidspunkt ikke kartlagt disse aktivitetene i større omfang enn det som framkommer i denne rapporten.

6 Avsluttende kommentarer

Det er en naturlig grunn til at trafikken rutes som den gjør i dag. Dette er i stor grad basert på et resultat av geografi, optimalisering av trafikkruting, økonomi og tett nordisk næringsvirksomhet. I praksis er det teknisk og kommersielt mulig å rute mer trafikk utenom Sverige ved bruk av sjøkabelforbindelser til Danmark og Storbritannia. Men det er neppe nok ledig kapasitet på disse forbindelsene til fullt ut å erstatte kommunikasjonsveiene gjennom Sverige. Storbritannia har tilsynelatende et regelverk som åpner for mye av den samme type kommunikasjonskontroll som FRA-loven i Sverige.

Generelt bør både privatpersoner og bedrifter være bevisst på hvilke tjenester man benytter for å overføre sensitiv informasjon. Dersom man vil sikre seg en høy grad av konfidensialitet er det hensiktsmessig å benytte krypteringsmetoder for å beskytte sin kommunikasjon. Det er en rekke kommersielle løsninger på markedet. Flere av disse løsningene er utviklet for å gi brukere mulighet til å beskytte sensitiv kommunikasjon, f.eks ved at programvare installeres på en bedrifts mobiltelefoner og PC'er. På den måten kan kommunikasjonen mellom interne brukere til en viss grad beskyttes.

[18] http://etsi.org/website/newsandevents/2008_07_qkd.aspx

7 Referanser

1. ”Lag om signalspaning i försvarsunderrättelseverksamhet” (FRA-loven) (lag 2008: 717)
2. ”Lag om försvarsunderrättelseverksamhet” (lag 2000:130)
3. ”Lag om elektronisk kommunikation” (lag 2003:389)
4. Svensk regjeringsproposisjon 2006/07:63 ”En anpassad försvarsunderrättelsesvirksomhet”
5. Pressemelding fra Regeringskansliet i Sverige 25.9 – 2008 om ”kompletteringar til signalspaningslagen”
6. ”Retsplejeloven” i Danmark (nr 594 af 20.6 – 2008)
7. ”Bekendtgørelse nr 988 af 28.9 – 2006 (logningsbekendtgørelsen)”, Danmark
8. “Regulation of Investigatory Powers Act 2000”, Storbritannia
9. ”Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses“, Tyskland
10. “Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI)), European Parliament, 2001