Endringer i radioamatørforskriften – innspill til høring

Jeg har innspill til §9.

1. Overskrift og struktur

§9 handler om digital kommunikasjon og bruk av kryptering er en del av dette. Derfor foreslår jeg å endre overskrifta til: "*Digital kommunikasjon*" og at den består av to ledd hvor det første sier: "*Ved digital kommunikasjon skal det brukes allment tilgjengelige protokoller* … ". Det andre leddet kan starte med "*Bruk av kryptert samband er ikke tilllatt. Kryptering av innenlandsk samband tillates likevel….*"

2. Krav til at protokoller skal være åpent tilgjengelig

Forskriften sier: "*Ved digital kommunikasjon skal det brukes alment tilgjengelige protokoller. Innholdet i meldinger skal kunne leses av alment tilgjengelige programmer*". Når mye amatørradio trafikk blir digital er dette viktige prinsipper og jeg spør om de faktisk blir fulgt. Hensikten er ikke bare at myndigheter skal kunne få innsyn i kommunikasjonen men at amatørradio skal være inkluderende og fremme eksperimentering og læring. Man bør ikke komme dit at noen blir ekskludert fordi riktig programvare (eller utstyr) ikke er tilgjengelig. Det bør ikke være slik at man blir avhengig av en bestemt leverandør som har monopol i markedet eller hvor *virkemåten ikke er offentlig kjent*. Det er også ønskelig at man ikke skal trenge å være avhengig av en PC med et helt bestemt operativsystem for å kunne kommunisere. Det kan hindre noen fra å delta.

Det ideelle er at alle protokoller som benyttes er *åpent tilgjengelige* slik at alle som har muligheten kan lage programvare (eller utstyr) etter spesifikasjonen. Det kalles *åpne standarder.* Åpen kildekode vil også være en fordel siden det gir frihet til å undersøke hvordan ting virker, eksperimentere med modifikasjoner, distribuere modifikasjoner til andre, samt at det er lettere å benytte på flere platformer. Åpne standarder og åpen kildekode er i *radioamatørbevegelsens ånd*.

Man bør lese kravet om "*alment tilgjengelige protokoller*" som at s*pesifikasjonen* skal være åpent tilgjengelig. En protokoll er strengt tatt en *spesifikasjon*. Det bør være mulig for alle sette seg inn i hvordan den virker og eventuelt lage programmer etter denne. Er regelen praktisert slik? Det virker som man tolker det slik at det er greit så lenge det finnes et program (eller utstyr), selv om programmet er lukket kildekode og proprietært og selv om protokollen ikke er publisert. Jeg mener derfor det er behov for en klargjøring: Protokollen *skal* være alment tilgjengelig. Det bør gjøres klart at det betyr at *spesifikasjonen* av protokollen skal være alment (åpent) tilgjengelig eller at det finnes en åpen kildekode referanseimplementasjon.

3. Bruk av kryptografiske metoder

I utgangspunktet er det ikke tillatt med kryptert samband. Samtidig legges det nå opp til at kryptering av innenlands samband likevel skal være tillatt ved organisert krise- og redningssamband samt trening til dette. Jeg mener det er riktig og nødvendig å myke opp dette, men det må heller ikke føre til at man utstenger legal bruk.

GDPR har strenge regler for behandling av personopplysninger. I nødsambandstjeneste vil man kunne måtte behandle opplysninger som kommer inn under dette reglementet. Hvordan kan man beskytte sensitive opplysninger men samtidig sikre at man følger intensjonen om åpen kommunikasjon? Vi kommer heller ikke bort fra behovet for sikkerhet. Applikasjoner som kommuniserer digitalt over amatørradio vil kunne ha behov for å autentisere og autorisere brukere. Eller å kunne verifisere

meldingers autentisitet. Dette vil kunne kreve bruk av kryptografiske metoder, og aktørene som kommuniserer må holde på hemmeligheter, dog kan man gjøre mye uten å kryptere meldingers innhold. Man kommer langt med å benytte kryptografisk hash-funksjoner, digitale signaturer o.l. hvor selve innholdet er ukryptert. Det kan imidlertid tenkes tilfeller hvor informasjon knyttet til selve autentiseringsmekanismen må sendes i krypterte meldinger. F.eks. bør passord aldri sendes klartekst.

Mye av poenget med amatørradio er jo læring og eksperimentering. Forståelse av informasjons- og kommunikasjonsteknologi som man opparbeider gjennom amatørradiovirksomhet er ment å gi en nytteverdi for samfunnet ellers. Vi skal ikke undervurdere hvor viktig forståelsen av kryptografi som teknikk er for forståelsen av digitalisering og internett. Derfor tror ikke at man kommer utenom bruk av kryptografiske metoder og bruk av teknologier som ikke opprinnelig var tenkt for amatørradio.

Det er et krav om at protokoller og programvare skal være alment tilgjengelig. Dette bør naturligvis også gjelde ved bruk av kryptografi. Ikke minst for at man skal ha mulighet til å vurdere om metoden er sikker nok! En kan også spørre om det burde være lov å kryptere meldinger hvis man også offentliggjør nøkkelen? Det gir mulighet til å teste og trene på bruk, og avgrense tilgangen til nøkkelen hvis behovet oppstår. Uansett bør det gjøres tydelig at det kun er nøkkelen som trenger å holdes hemmelig i de tilfeller hvor kryptografi tillates. Det bør gjøres klart at det *skal* brukes kjente kryptometoder og åpne protokoller.

Kan det være ønskelig med en definisjon av hva som menes med “*innenlands”* samband? Digitale meldinger vil videresendes av flere noder, ofte over internett. Da er det lett å tenke at enhver stasjon som sender en kryptert melding over amatørradio, må være innenfor landets grenser, mens internett-trafikk ikke har slike restriksjoner.

Med hilsen
Øyvind Hanssen, [redacted]