Rødt
Osterhaugs gate 27
0183 Oslo

9. april 2010

## Høringsuttalelse om datalagring fra Rødt

Det vises til høringsbrev datert 8. januar 2010 med forslag til implementering av direktiv om datalagring.

I regjeringens høringsnotat er det hovedsakelig tre hensyn som vektlegges:

- behovet for verktøy til å bekjempe kriminalitet
- personvernhensyn
- konkurransen innenfor markedet for elektronisk kommunikasjon

Vi vil i hovedsak gå inn på de samme områdene i vår høringsuttalelse, men tar også opp noen relaterte temaer.

## Kriminalitetsbekjempelse

Politiet har tilgang til visse metoder og virkemidler for å kunne løse oppgavene sine til samfunnets beste, for å kunne for å kartlegge, avdekke og stanse kriminell virksomhet.

I høringsnotatet legges det til grunn at det særlig ved alvorlig og organisert kriminalitet hvor elektronisk kommunikasjon har blitt benyttet under planlegging og gjennomføring av straffbare handlinger, vil trafikkdata, lokaliseringsdata og abonnements-/brukerdata være viktige for politi og påtalemyndighet. Regjeringen mener at om politiet får lettere tilgang til data, vil det kunne føre til at flere kriminelle blir "tatt".

Grunnlaget for å mene det, er først og fremst politiets egen synsing. Det er lite belegg for at datalagring på den skalaen datalagringsdirektivet legger opp til vil føre til at veldig mange flere kriminelle vil bli domfelt. Bevisførselen er oftest anekdotisk, og til dels selvmotsigende. (Jf. for eksempel Baneheia-saken, hvor det mye omtalte mobiltelefonbeviset på det "beste" ikke beviste noe som helst, verken i den ene eller den andre retningen.)

Det er dessuten en ganske enkel sak om man driver med grov kriminalitet å skjule sine elektroniske spor:

- Vanlig e-post kan erstattes av webmail-løsninger som Gmail eller med privatmeldinger via for eksempel Facebook eller lignende.
- Mobilspor kan enkelt skjules ved å kjøpe anonyme mobilabonnementer fra utlandet.
- Aktivitet på nett kan forholdsvis enkelt skjules ved hjelp av anonymiseringstjenester, eller ganske enkelt ved å bruke offentlige maskiner eller åpne trådløse nettverk.

Politiet har allerede, med dagens lover og regler, gode muligheter til å "fryse" og hente inn trafikkdata i saker hvor de har skjellig grunn til mistanke.

### Viktige prinsipper snus på hodet

En av de mest problematiske sidene ved datalagringsdirektivet, er at det snur viktige rettsprinsipper på hodet. I dag har politiet gode ressurser til å overvåke mistenkte, men det må foreligge en konkret mistanke mot en utvalgt person som blir overvåket. Med datalagringsdirektivet blir prinsippet "uskyldig inntil det motsatte er bevist" snudd på hodet – alle blir potensielle mistenkte, og alle overvåkes *i tilfelle* noen av oss blir mistenkte i fremtiden.

### Faren for utglidning

Om direktivet blir innført, og man først har godtatt å tilsidesette personvern og viktige rettsprinsipper, er sjansen stor for at veien videre vil bestå av ytterligere skritt i retning økt lagringstid og lagring av mer innhold - mer overvåkning, med de samme argumentene lagt til grunn som brukes nå. Samtidig er faren stor for at trafikkdataene som vil bli lagret under direktivet vil bli tatt i bruk i flere saker med lavere strafferammer, ikke bare når det gjelder "alvorlige forbrytelser", som det i utgangspunktet legges opp til. I Stor-Britannia har myndighetene blant annet brukt lover laget for å bekjempe terror og alvorlig kriminalitet til å spionere på foreldrene til skolebarn og for å sjekke om hundeeiere plukker opp lort etter bikkjene sine.

Når det kommer forslag om en ny lov som presumptivt skal gi bedre kriminalitets-bekjempelse, er det forkjempernes oppgave å sannsynliggjøre at den nye loven vil føre til det forventede resultatet, og at dette resultatet er omfattende nok til å oppveie ulempene forslaget vil føre til. Dette har ikke blitt sannsynliggjort, og med mindre denne høringsrunden frambringer slike bevis og dokumentasjon, er det ingen grunn til å forutsette at de eksisterer.

## Personvern

I høringsnotatet forsøker regjeringen å veie personvern opp mot nødvendige tiltak for "effektiv kriminalitetsbekjempelse". Det framstilles som om spørsmålet er om datalagring er nødvendig for å bekjempe kriminalitet, men det er ikke *det* vi trenger å ta stilling til. Data *lagres* i dag, og når politi og påtalemyndighet trenger det, har de mulighet til å få lagra trafikkdata langt ut over den vanlige lagringstida hos teleleverandørene.

Men som regjeringen selv sier det, i høringsnotatet sitt:

> *Registrering av alle borgeres elektroniske kommunikasjon vil over tid gi et svært godt bilde av deres kontaktnett og bevegelser. Dette inngrepet i kommunikasjonsfriheten og det ubehaget borgerne kan føle ved å vite at noen sitter med denne informasjonen, er i seg selv en integritetskrenkelse. Denne forsterkes ytterligere av de registrertes frykt for at informasjonen kan misbrukes eller komme uvedkommende i hende.*
>
> *Et viktig element i personvernet er, som ovenfor nevnt, at samfunnets overvåkings- og kontrollnivå skal være så begrenset som mulig.*

### Ytringsfrihet og fri forsamlingsrett trues

De fleste av oss vil oppfatte lagring av all data om våre elektroniske bevegelser som et overgrep mot retten vår til å ha privatlivet i fred. Alene vissheten om at informasjon om våre

bevegelser og kommunikasjon blir lagret, kan virke alvorlig hemmende på friheten vår – det kan virke begrensende på hva du gjør, hvem du kontakter, og hva du planlegger.

Dette vil legge alvorlige hindringer i veien for potensielle varslere, det vil true kildevernet, og vil generelt være i veien for alminnelig ytringsfrihet.

Det kan også være en potensiell trussel mot den frie forsamlingsretten, da det blir kartlagt hvor man befinner seg om man for eksempel har med og bruker en mobiltelefon. Når man vet at dette blir kartlagt, kan det heve terskelen for å delta på aktiviteter.

## Konkurranseutjevning

I følge EU handler dette direktivet om å hindre konkurransevridning og at det derfor er EØS-relevant. Formålet med datalagringsdirektivet skal være å harmonisere regelverket for datalagring for å sikre at det indre marked fungerer. Intensjonen er at teletilbydere innafor det indre marked skal møte de samme forpliktelsene overalt.

Om så var, skulle man kanskje vente at direktivet faktisk regulerte forhold som faktisk påvirker kostnadssiden, men de detaljene er i hovedsak overlatt til de enkelte land å bestemme. Lagringstid (utover minimum 6 mnd), krav til sikkerhet og kontroll, hvem som skal betale for lagring og uthenting av data – alt dette er det opp til de enkelte land å bestemme. Vi kan ikke se at dette på noen måte vil motvirke konkurransevridning og mener at direktivet ikke er EØS-relevant.

## Konklusjon

Rødt vil gå mot en implementering av datalagringsdirektivet i norsk lov, først og fremst av personvernhensyn og fordi vi mener konsekvensene av direktivet vil virke hemmende på utøvelsen av alles rett til å ytre seg og forsamles fritt.

Vi kan heller ikke se at direktivet er EØS-relevant, ettersom det tar få til ingen grep for å utjevne konkurransesituasjonen for teleleverandører innafor det indre marked.

Med hilsen

Marit Halse
Rødts IT- og personvernutvalg