

Arbeids- og Inkluderingsdepartementet

Deres ref: 201000161-/ASK

Vår ref: 10/1035

Vår dato: 8. mars 2010

NAV svar på høringsnotat for Datalagringsdirektivet

Vi viser til brev av 21.01.2010, hvor det bes om NAVs synspunktet til høringsnotatet og vurdering av eventuelle konsekvenser for Arbeids- og velferdsetaten dersom datalagringsdirektivet skal innlemmes i EØS-avtalen. I vår tilbakemelding har vi hatt særlig fokus på personvernkonsekvenser av det foreslåtte direktivet, informasjonssikkerhet, telefoni og video, samt konsekvenser for NAV.

GENERELT

Formålet med datalagringsdirektivet og implementeringen av dette er bekjempelse av alvorlig kriminalitet og gi myndighetene bedre muligheter til å hente ut opplysninger om tele- og nettrafikk ifb. med avdekning, etterforskning og rettsforfølgning i straffesaker.

Datalagringsdirektivet reiser en rekke politiske, etiske og juridiske problemstillinger. Målsettingen med datalagringsdirektivet står i utgangspunktet i sterk interessekonflikt i forhold til sentrale personvern hensyn som vern av den enkeltes rett til integritet og privatlivets fred. Registrering av alle borgeres elektroniske kommunikasjon vil over tid kunne gi et svært godt bilde av deres kontaktnett og handlingsmønster, samtidig som dagens overvåkningsnivå ytterligere vil bli utvidet. All informasjonen vil bli lagret uten at noen er mistenkt. Det innebærer en generell overvåking av befolkningen. Det er en stor risiko for at slik omfattende registrering etter hvert vil medføre utglidning av virkeområde til også å omfatte andre formål og aktører enn politiet og rettsvesen. Informasjon om hvem en person ringer eller sender e-post til kan tenkes å være interessant for mange ut fra mange "gode" formål!

Skal datalagringsdirektivet er tenkt gjennomført så må det sikres at personvernet og informasjonssikkerheten ivaretas tilstrekkelig i forhold til den enkelte, slik at dette ikke oppleves som en ytterligere inngripen og risiko. Det er viktig at registrerte har trygghet og den nødvendige tillit til at opplysningene kun brukes til det som er formålet dvs. kriminalitetsbekjempelse av alvorlig kriminalitet. De registrerte må sikres de samme rettigheter som de har etter personopplysningslovens bestemmelser, for eksempel til rett til generelt og individuelt innsyn. De registrertes rettigheter etter personopplysningsloven er for øvrig ikke drøftet i høringsnotatet, og heller ikke vurderinger i forhold til sentrale bestemmelser i personopplysningsloven som nødvendighetskriteriet, behandlingsansvaret, behandlingsgrunnlag og konsesjon til Datatilsynet.

Arbeids- og velferdsdirektoratet // Direktør
Postadresse: Postboks 5 St. Olav Plass // 0130 OSLO

Besøksadresse: Akersgaten 64-68 // 0180 OSLO
Tel: 21 07 00 00 // Faks: 21 07 00 01

www.nav.no //

For å oppnå den nødvendige sikring så må det settes krav i forhold de virksomheter som skal lagre dataene på vegne av myndighetene etter Ekomloven, og til de som skal behandle disse. Det er bekymringsverdig at de enkelte tilbydere blir ansvarlig for informasjonssikkerheten for lagrede data som ligger utenfor deres behandling, formål og egeninteresse. Det er en risiko for at denne mangeartede gruppen av tilbydere ikke vil ha fullgode mekanismer for sikring av trafikkdata mot uautorisert tilgang, endring og spredning.

Det fremgår av oversendelsesbrevet at formålet med høringsnotatet er å få frem et best mulig beslutningsgrunnlag, og tiltak for å forhindre negative personvernmessige konsekvenser. Vi kan ikke, fra vårt faglige ståsted, se at høringsnotatet i tilstrekkelig grad imøtekommer det. Det blir en interesseavveining mellom personvern og kriminalitetsbekjempelse. Selv om hensikten bak direktivet er god, så kan vi ikke se at behovet for slik utvidet og omfattende lagring av personopplysninger gir en så stor vinning for kriminalitetsbekjempelse at et slikt direktiv bør innføres på bekostning av personvernet. Nytteverdien av direktivet bør dokumenteres og konkretiseres ytterligere.

Telefoni og video

Departementet legger til grunn definisjonene av "tilbyder av offentlige elektroniske kommunikasjons tjenester" i ekomloven når det diskuteres hvem som skal lagre i henhold til direktivet.

Slik vi tolker definisjonene i ekomloven § 1-5 vil ikke NAV være pliktig til å lagre trafikk fra etatens telefoni og videosystem.

Det kan knyttes noe usikkerhet til dette spørsmålet da NAV per i dag tilbyr telefoni og videotjenester også til eksterne enheter, som kommunale tjenester i NAV - kontor og Helsetjenesteforvaltningen. Vi mener at NAV likevel faller utenfor tilbyderbegrepet jf. diskusjonen om interessefelleskap. Vi viser blant annet til forarbeidene til ekomloven Ot.prp.nr.58 (2002-2003) s.87 og Ot.prp.nr.36 (1994-1995) s.29, der det heter at "avgjørelsen av om en brukergruppe utgjør en allmennhet vil blant annet bero på antall og interessefelleskap. Desto sterkere brukerne har felles i annen enn selve kommunikasjonen (fag-, bransjeinteresser osv.), jo større må antallet være for å utgjøre en allmennhet." Brukere som NAV tilbyr sine tjenester til, inkludert kommunale tjenester i NAV - kontor og Helsetjenesteforvaltningen, har samme fag-/bransjeinteresse. Vi viser videre til høringsnotatet punkt 4.6 Hvem skal lagre i henhold til lovforslaget, hvor det gis eksempler på virksomheter som normalt faller utenfor tilbyderbegrepet i ekomloven.

Samtidig står det i høringsnotatet at myndighetene kan pålegge lagringsplikt også for de som ikke faller inn under tilbyderbegrepet, når det blir nødvendig for å oppfylle formålet med bestemmelsen. Arbeids og velferdsdirektoratet påpeker derfor at det er noe uklart i høringsnotatet og ber departementet komme med en avklaring på dette, før vi eventuelt utreder de systemmessige og driftsmessige konsekvensene for dette.

Forutsatt at NAV selv ikke er berørt av direktivet vil implementeringen av direktivet i Norge ha som konsekvens for etaten at trafikkdata fra alle telefonisamtaler mellom etatens medarbeidere og eksterne og fra alle samtaler (både interne og eksterne) med tjenstemobiltelefon lagres hos tilbyderne. Dette gjelder ikke bare NAV, men generelt i Norge. Trafikkdata fra etatens masse utsendelse av SMS vil også bli lagret hos tilbyder.

Det finnes imidlertid noen telefon- og videotjenester hos NAV som er rettet mot et spesifikk tjeneste/fagområdet der innholdet taushetsbelagt eller sensitivt. F eks Bildetolk-tjenesten (for døve) og Gjeldstelefonen (ikke sensitivt, men taushetsbelagt). NAV operer også med eget telefonnummer for de som har hemmelig adresse fordi de har et beskyttelsesbehov (Kode 6). Dette betyr at også trafikkdata uten samtaleinnhold i seg selv blir sensitive. Hvis direktivet blir innført må det stilles høye sikkerhetskrav til tilbyderne, særlig med tanke på tilgangskontroll til de registrene der trafikkdata lagres. I ytterste konsekvens kan en oppleve at brukerne slutter å bruke slike tjenester, hvis det oppleves som et brudd på konfidensialitet og risiko for misbruk. Dette vil ramme NAVs mulighet til å yte gode tjenester overfor slike utsatte grupper. Dette er forhold som vil gjelde flere offentlige etater og type varslings-tjenester i det norske samfunn.

Hvis det fra norske myndigheters side velges en finansieringsmodell der tilbyderne må dekke alle kostnader som implementeringen av direktivet vil medføre, kan dette generelt gi økte priser for telefonitrafikk. Dette er negativt for NAV som er en stor kunde av slike tjenester. En sentralisert finansieringsmodell bør vurderes.

Fellesregistre

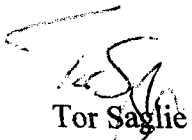
Vi kan ikke se at dette har noen konsekvenser for etatens fellesregistre.

VURDERINGER I FORHOLD TIL EVENTUELLE KONSEKVENSER FOR NAV

Implementering av datalagringsdirektivet vil få konsekvenser for NAV ved at all tele- og nettrafikk til og fra NAV vil bli lagret i tjenestetilbyders databaser. Selv om innholdet i kommunikasjonen ikke lagres, kan datastrømmene likevel kartlegge sensitive personopplysninger og brukergrupper. For eksempel opprigning til bestemte servicetelefoner i NAV som gjelder bestemte brukergrupper som gjeldstelefonen, kontakttelefon for hørselshemmede og døve. Denne informasjonen, som vil kunne være på sensitivt nivå, og vil sette krav til informasjonssikkerhet hos de ulike aktører som skal lagre, utlevere og behandle disse opplysningene.

En stor del av vår kommunikasjon med publikum foregår via telefon, sms og ulike nettløsninger. Det må ikke bli slik at ved innføring av datalagringsdirektivet, så benytter publikum seg heller av andre kommunikasjonskanaler i kontakt med NAV i frykt for overvåking, selv om kontakten med NAV i og for seg er legitim nok. Visse brukere vegrer seg for å oppsøke et NAV kontor. Dersom de samme brukerne vil vegre seg for elektronisk kommunikasjon, så skaper dette utilsiktede konsekvenser for etatens håndteringen av sin samfunnsmessige oppgave.

Det er åpenbart at det grove og organiserte kriminelle miljøet vil tilpasse seg datalagringsdirektivet og nasjonale lovbestemmelser, og derfor benytte seg av alternative kommunikasjonskanaler som ikke er sporbare



Tor Saglie
Arbeids-og velferdsdirektør



Nina Aulie
IKT-direktør