MOTTATT
14 APR 2010

HØGSKOLEN I GJØVIK

Vår dato	Vår referanse
12.04.10	
Deres dato	**Deres referanse**
08.01.2010	09/585-HK

Det Kongelige Samferdselsdepartement
Postboks 8010 Dep
0030 Oslo

Dette er høringsuttalelsen fra Norsk Informasjonssikkerhetslab (NISlab) ved Høgskolen i Gjøvik (HIG) om datalagringsdirektivet. NISlab var ikke nevnt som en av høringsinstansene, men mener at vi med vårt sterke fagmiljø innen informasjonssikkerhet har synspunkter som bør vektlegges i denne høringen. Vi er spesielt sterke innen internettrelaterte teknologier som personvern, anonymitet, sporbarhet, lagringssikkerhet, kommunikasjonssikkerhet, databasesikkerhet og kryptografi.

NISlab tar med denne uttalelsen ikke stilling til om datalagringsdirektivet skal innføres eller ikke. Som en avdeling på en høgskole ønsker vi ikke å ta stilling på vegne av våre forskere, men oppfordrer dem til å trekke sine konklusjoner og delta i den offentlige debatt om dette viktige temaet. Vår høringsuttalelse belyser en rekke uklarheter og mulig konsekvenser i høringsnotatet som er lagt ut. NISlab er av den oppfatning at flere er alvorlige og må utredes.

De spørsmålene som vi stiller i høringsuttalelsen er ment for å belyse uklarheter som etter vår mening må utredes grundigere før beslutningstakere kan se alle aspekter av en eventuell innføring av datalagringsdirektivet. De stedene hvor det er stilt slike spørsmål er det antatt at datalagringsdirektivet er tiltenkt å bli innført og dette er bakgrunnen for hvordan spørsmålene blir stilt.

Som oppsummering anbefaler NISlab at det må etableres en ekspertgruppe som gjennomgår dagens lagringspraksis samt eksisterende sikkerhet, og vurderer denne praksisen mot norske lover. I tillegg må gruppen også se på hva en eventuell utvidelse av dagens lagring i henhold til datalagringsdirektivet vil medføre. Både eksisterende og eventuelle fremtidige løsninger må undersøkes spesielt med fokus på punktene under:

- Sporingsmuligheter, fordeler, ulemper og trusler
- Sensitivitet av lagret informasjon
- Beskyttelse av informasjon
- Tilgang til informasjon
- Lagringssted, innland – utland, sentralt – desentralisert
- Utvidelser, gamle og nye teknologier for kommunikasjon

De følgende punktene er bakgrunnen for vår anbefaling.

Sporingsmuligheter i lokasjonsdatabaser
Som kjent vil en utvidelse av dagens lagring i henhold til datalagringsdirektivet også inneholde lokasjonsinformasjon, det vil si at stedet hvor enhver person i Norge oppholdt seg når han/hun kommuniserte elektronisk med noen. Denne informasjonen vil bli lagret i en eller flere databaser hos de private tjenesteleverandørene.

Dersom noen får tilgang til slik informasjon hos en tjenesteleverandør åpner det seg store muligheter for misbruk. Vi påstår ikke at tjenesteleverandørene vil åpne for dette, men både systemfeil, inkompetanse, og utro ansatte, kan medføre at slik informasjon kommer på avveie. Og med lokasjonsinformasjon lagret i 6-24 måneder sammen med alle kontaktmønstre, blir sensitiviteten i dataene meget stor.

GJØVIK UNIVERSITY COLLEGE

Postadresse:	Besøksadresse:	Telefon:	Telefax:	E-post:
Postboks 191	Teknologiveien 22	61 13 51 00	61 13 51 70	postmottak@hig.no
2802 Gjøvik	2815 Gjøvik			

Dersom man tenker seg at et stort selskap som for eksempel Statoil snakker med potensielle samarbeidspartnere eller oppkjøpskandidater og holder møter i utlandet over en lengre periode for å diskutere dette, vil informasjon om dette lagres hos en, eller muligens flere, tjenesteleverandører. I tillegg vil noen kunne benytte denne informasjonen til å identifisere grupper av personer som oppholder seg i samme område samt hvem personene fra Statoil har kommunisert med. Slik informasjon er mye verdt og særdeles sensitiv for et stort selskap. Når personer har tilgang til databaser med slik verdifull informasjon over lengre tidsperioder vil det åpne seg muligheter for misbruk i en helt annen størrelsesorden enn tidligere. Det er ikke vanskelig å se at slik lokasjons- og kommunikasjonsinformasjon også vil være sårbart for Regjering, politi og andre samfunnskritiske institusjoner.

I og med at størstedelen av en privatpersons kontaktliste vil antas å bli benyttet gjennom den foreslåtte 6-24 måneders lagringsperioden vil man også enkelt kunne koble hvem av disse personene som vedkommende enten har møtt fysisk, eller hatt muligheten til å møte, i den samme 6-24 måneders perioden. Dette er en mulighet til overvåkning av enkeltpersoners og gruppers privatliv som ikke tidligere har eksistert. (Men teleleverandørene kan nok ha hatt mulighet til mye av dette, men vi regner med at de per dags dato verken lagrer sensitiv informasjon så lenge – eller misbruker den).

NISlab mener at en slik utvidet lagring av både lokasjon og kontaktmønstre inneholder så mye ny informasjon at før man kan ta stilling til om datalagringsdirektivet skal innføres må man gjennomføre en komplett vurdering av potensialet (sårbarheten) for en slik database. Dette må skje både med de positive og de negative sidene av en slik samling av sensitiv informasjon. En høringsrunde som dette er ikke nok for å oppnå en slik avklaring, selv om innspillene vil dekke mange viktige elementer for begge "sider" av spørsmålet.

En implementering av datalagringsdirektivet vil i vesentlig grad endre risikobildet for mange interessenter. Endringen i risikobildet vil i stor grad være en konsekvens av måten datalagringsdirektivet blir implementert rent teknisk og administrativt. Det anbefales derfor at det utføres en risikoanalyse opp mot alle de relevante implementeringsstrategiene der en i særlig grad får belyst endringer i risikobildet med hensyn på blant annet:

- Industrispionasje
- Økonomisk kriminalitet
- Spionasje mot Rikets sikkerhet
- Personvern f eks med hensyn på politisk overvåkning, følsomme helseopplysninger

Dette er nærmere illustrert i scenarier og eksempler nedenfor.

E-post og utdatert teknologi

Vi stiller spørsmålstegn ved at e-post er nevnt spesifikt ettersom dette er en kommunikasjonsmåte som ikke inneholder noen av de grunnleggende sikringsmulighetene på Internett. Det finnes i de foreslåtte loggene verken bekreftelse av hvem som faktisk har sendt en e-post, hvem som faktisk har mottatt den, hvor den ble sendt fra opprinnelig, hvem som eventuelt leste e-posten, hvor vedkommende befant seg når de leste e-posten, eller om den ble slettet før den ble lest. Ettersom e-post er helt uten integritetsbeskyttelse vil man ikke kunne ha tiltro til logger hvor bare fra-til informasjon er lagret. Av denne grunn er det merkelig at e-post er nevnt spesielt ettersom mange nyere teknologier for elektronisk kommunikasjon ikke vil bli berørt av direktivet. Dette kommer også frem av høringsnotatet som beskriver at dette er et problem som kan dekkes senere. Kort kan man nevne populære teknologier som MSN, Yahoo, Google Talk, Skype, SILC, IRC, Facebook, Twitter, som ikke vil bli berørt. Samtidig må man også stille spørsmålet om såkalt søppelpost (spam) skal berøres av direktivet? Dersom en leverandør sletter noe den antar er spam før mottakeren har fått det til sin e-postkasse – skal e-posten lagres i loggene hos leverandøren eller er den "ikke-eksisterende"? Og kan man benytte en slik e-post som grunnlag for annen informasjonsinnhenting når integriteten i slik informasjon er ikke-eksisterende?

Påstanden om at e-postadresser ikke inneholder sensitiv informasjon er ikke korrekt. Når en personlig e-postadresse i slike logger kobles til (reelle) e-postadresser som contact@aids.gov , info@prochoiceactionnetwork-canada.org , prolife@princeton.edu , kyoung@breastcancer.org , info@prostatecancerfoundation.org , vil dette være informasjon

som kan antas å være både sensitiv og personlig. Når denne informasjonen i tillegg skal lagres hos private selskaper uten bedre sikring av informasjonen vil dette ikke være i tråd med personvernet.

Private tjenester og utvidelse av direktivet
Det er uklart hvordan direktivet skal håndtere privatpersoner som tilbyr (gratis)tjenester på sine datamaskiner. Her må det til en klargjøring. Høringsnotatet antyder at det senere kan komme utvidelser som kan dekke nye og andre former for kommunikasjon. Hvem skal ta slike avgjørelser? Dette er et vesentlig spørsmål i og med at andre land allerede er i ferd med å utvide lagringen til for eksempel også å gjelde alle nettadresser som en bruker besøker fra en nettleser. Skal slike utvidelser kunne skje i et departement eller må Stortinget (og/eller andre) igjen involveres ved en eventuell senere utvidelse av lagringen? NISlab mener dette er så prinsipielt viktig at det ikke kan være noen tvil rundt dette spørsmålet dersom direktivet vurderes innført.

Lagringssikkerhet og uthenting av informasjon
I høringsnotatet mangler det en del essensielle krav for å kunne ivareta god lagringssikkerhet av den innsamlede informasjonen. Det er i de fleste av dagens eksisterende lagringssystemer muligheter for ansatte i bedriften å forandre på loggene i etterkant. Selv om dette ikke er tillatt har myndighetene nå en unik mulighet til å stille krav om dette slik at data forblir beskyttet også etter at de er samlet hos en leverandør. Derfor mener NISlab at det i et nytt lagringssystem må benyttes maskinvare og programvare hvor slik manipulasjon i etterkant ikke er mulig og integriteten av loggene kan ivaretas for ettertiden. Spesielt viktig er integritetsspørsmålet ettersom man her snakker om å benytte informasjonen i juridiske saker og man må derfor stille slike krav til systemene. Det tas som en selvfølge at all tilgang til dataene logges og er påtvunget en tilsvarende sikker lagring som beskrevet over. Man må også foreslå lagringsperioder på slike logger av informasjonsuthenting.

I et system som lagrer data for senere oppslag er flere faktorer viktige. For det første bør er slik system være helt frakoblet Internett og være et lukket system som leverandøren bare kan benytte i samarbeid med politiet. Det er teknologisk mulig å sikre de lagrede dataene slik at de kun kan aksesseres når både politiet og leverandøren samarbeider. Det vil medføre at verken politiet eller leverandøren har tilgang til dataene alene. Denne teknologien (for eksempel Secret Sharing Systems) er både enkel, rimelig og tilgjengelig. I tillegg må man ha gode rutiner for å slette dataene i systemet så snart tidsfristen for lagring er passert. Dette vil også måtte gjelde backup og eventuelle mellomlagringer som har blitt foretatt internt hos tjenesteleverandøren. Når man stiller krav om sikring av dataene bør man også vurdere om leverandøren skal være pålagt å benytte sertifiserte systemer for innhenting, lagring, uthenting og sletting av data.

Sted for lagring
Ettersom det åpnes for tjenesteleverandøren kan lagre dataene i utlandet stiller NISlab spørsmål ved hvordan norske tilsyn skal føre kontroll med at personvernet ivaretas og om sikkerheten til de lagrede dataene er god nok. Norske tilsyn har ingen myndighet i utlandet og leverandørene vil slippe unna eventuelle norske krav til sikkerhet i systemet dersom dette tillates.

Lagringstid
Dersom direktivet vedtas vil det medføre en periode for lagring på 6-24 måneder. Kan man være sikker på at denne perioden ikke kan utvides uten at en sak blir forelagt Stortinget?

Høringsnotatets bruk av andre land
NISlab reagerer også på at kun noen andre EU-nasjoners implementering av direktivet er berørt – og disse kun i korte ordlag. Det har vært store diskusjoner i flere land enn Danmark, Finland og Sverige. Kanskje spesielt i Tyskland har direktivet vært omdiskutert lenge og når tysk rett nå har konkludert med at datalagringsdirektivet bryter

med "basis rettigheter til privatliv og korrespondanse" gjør dette at direktivet helt klart må avklares mot blant annet personvernloven før man foreslår å innføre det.

Effekt av innføringen
Dersom man i flere land nå har innført datalagringsdirektivet og hatt tilsvarende løsninger i flere år bør man kunne få data om bruk, sikkerhet, lagringssteder, tilgangskontroll, etc. Dette vil kunne gi en pekepinn på hvordan effekten av innføringen har vært. Flere land har rapportert at effekten har vært liten, men noen større forskningsrapporter av en slik effekt kan man ennå ikke henvise til. Det er viktig at alle land gjennomfører slik forskning.
Det bør være beskrevet måter å måle bruken og nytten av datalagringsdirektivet, slik at man senere med basis i konkrete målinger og standarder, kan vurdere hvor effektiv innføringen eventuelt har vært. Dermed bør man vurdere om det eventuelle direktivforslaget selv kan foreslå at det kan fjernes dersom man ikke får en signifikant samfunnsmessig gevinst på innføringen.

Anonyme ytringer på nett
Det argumenteres ofte for at man ikke skal kunne opptre anonymt på nett, men dette er en grunnleggende rettighet i likhet med det å kunne kjøpe (lovlige) varer kontant, bevege seg på lovlige steder uten å bli overvåket (det vil si uten å bli gjenkjent og logget i en sentral database), snakke med andre på gaten eller i ditt eget hus uten at dette blir loggført, osv. Det er en like stor rettighet å bruke Internett lovlig uten at noen skal passe på hva du gjør. Vi nevner kort noen eksempler; hvem du snakker med, hvilke personer og organisasjoner du sender brev til, hvem som sender informasjon til deg, hvem som kontakter deg på telefon.

Umulig for pressen å beskytte sine kilder?
Dersom all elektronisk kommunikasjon skal loggføres vil det være umulig for en anonym person å snakke med en journalist på telefon eller mobiltelefon. Tipseren vil heller ikke kunne sende e-post og må sannsynligvis enten møte journalisten i egen person eller benytte kommunikasjonsmetoder som ennå ikke er påkrevet å bli loggført. Det er spesielt viktig å bemerke at datalagringsdirektivet gjør en slik sporing mulig og det er dette som må vurderes som en trussel mot presse- og ytringsfrihet.

Må bryte loven for å tipse politiet anonymt?
Av samme grunn kan politiet glemme å motta anonyme tips dersom datalagringsdirektivet innføres. Ingen vil stole på at tipserne ikke vil bli oppsporet når informasjonen om hvem de er befinner seg i en database som politiet kan få tilgang til. Dette er ikke reversibelt og kan ikke "innføres igjen" senere dersom politiet skulle ønske det. Bare at kommunikasjonen er lagret er en trussel som vil forhindre at noen stoler på eventuelle løfter om ikke å benytte de lagrede data.

Med vennlig hilsen,

Morten Irgens
Dekan ved avdeling for
Informatikk og Medieteknikk

Patrick Bours.

Patrick Bours
Seksjonsleder NISlab