

Samferdselsdepartementet
Postboks 8010 Dep
0030 Oslo

12. april 2010

Anders Brenna
Solhaugveien 77
1337 Sandvika

Høringsuttalelse om datalagringsdirektivet

Undertegnede viser til høringsbrev av 8. januar 2010, og vil med dette belyse noen viktige momenter i forhold til eventuell implementering av Datalagringsdirektivet i norsk lov.

Som far er jeg opptatt av at politiet klarer å avsløre pedofile nettverk, samt oppklare annen alvorlig kriminalitet som truer min egen og mine barns trygghet. Som far er jeg likevel motstander av implementering av Datalagringsdirektivet, fordi jeg med min IT-bakgrunn og min journalistiske erfaring fra kriminalitetsbekjempelse på nettet, vet at Datalagringsdirektivet ikke vil hjelpe politiet i deres arbeid. Som far vil jeg ha et sterkt politi med de nødvendige verktøyene, men jeg vil ikke ha «lat som om du gjør noe»-tiltak.

I dette høringsnotatet vil jeg fokusere på hvorfor Datalagringsdirektivet ikke vil bli det etterforskningsverktøyet politiet tror det blir, samt forklare hvordan det truer kildevernet og personvernet.

Datalagringsdirektivet virker ikke

Det er korrekt at logger fra data- og teletrafikk er et nyttig verktøy i etterforskningsøyemed, men det er nødvendig å påpeke på to grunnleggende forutsetninger:

For det første virker slike logger kun for de kriminelle handlingene der vedkommende ikke tenkte over problemstillingen. Det inkluderer som regel kun mindre alvorlig kriminalitet, samt kriminalitet som ikke var planlagt. Alvorlig overlagte kriminelle handlinger kjennetegnes ved at det tas hensyn til alle kjente utfordringer, og et implementert Datalagringsdirektiv vil være godt kjent for slike kriminelle miljøer.

For det andre er både terrorister og pedofile notorisk paranoide. Undertegnede har vært på kurs i avhørsteknikk med Kripos, og fått begreftet inntrykket fra mediesakene av at pedofile ikke en gang innrømmer for seg selv at de er pedofile. Tilsvarende vil også potensielle terrorister gjøre alt de kan av forberedende mottrekk for ikke å tiltrekke seg oppmerksomhet.

Begge disse målgruppene vil ta nødvendige grep for ikke å bli fanget opp av Datalagringsdirektivets logger, og det samme vil andre avanserte organiserte kriminelle miljøer.

Datalagringsdirektivet truer kildevernet

Selv om politiet ikke med viten og vilje ønsker å etterforske en av pressens kilder, er det en sannsynlig konsekvens dersom en person mistenkt for kriminell handling etterforskes ved hjelp av datalogger som er lagret i henhold til Datalagringsdirektivet.

F.eks. er det offentlig kjent at en finansmann som nylig ble etterforsket har vært kilde i en NRK-reportasje. Dersom vedkommende har vært kilden til flere større avsløringer, ville en eventuell etterforskning med utgangspunkt i Datalagringsdirektivets pålagte logger raskt avslørt når vedkommende eventuelt befant seg i andre redaksjonslokaler.

Denne informasjonen kan enkelt kobles opp mot tidligere oppslag, og selv om ikke politiet aktivt er på kildejakt, vil kilden i slike tilfeller avsløres under den etterforskningen.

Datalagringsdirektivet truer nettettersforskningen

Datakrimavdelingen i Kripos har etter eget utsagn kun kapasitet til å etterforske 5 sakskomplekser av større omfang i året. Dette har blant annet vært til stor frustrasjon for opphavseiere som har måtte ty til privat etterforskning i et forsøk på å komme problemet til livs.

Datalagringsdirektivet vil gjøre jobben vanskeligere og mer komplisert for politiet, ettersom en eventuell implementering vil gjøre mottiltak mer utbredt blant ulovlige fildelere og andre kriminelle miljøer. Disse mottiltakene inkluderer blant annet kryptering og proxy-tjenester som skjuler brukerens IP-adresse.

Dette vil føre til et våpenkappløp et underbemannet politi ikke vil klare å henge med på, og det er dessverre lite som tyder på at politiet vil få verken mer eller bedre nettettersforskningskapasitet i årene fremover.

Datalagringsdirektivet kan ikke garantere for dataene

Undertegnede har som journalist jobbet mye med en sak der advokatfirmaet Simonsen på vegne av filmbransjen har krevd utlevering av personinformasjon for en IP-adresse mistenkt for ulovlig opplasting av filmen «Max Manus» til et piratnettverk. Post- og teletilsynet, som er ansvarlig for å sikre personvernet, opphevet taushetsplikten. Dermed endte saken i rettsapparatet.

Hva som er utfallet der er ukjent, ettersom to rettsinstanser har hemmeligholdt kjennelsen. Dette viser at det ikke vil være tilfredsstillende verken med oppsyn av Teletilsynet eller av domstolene.

Det er også kjent blant alle som jobber med IT-sikkerhet, at IP-adressen er en av de mest kritiske nøkkelopplysningene hackere bruker for å bryte seg inn i nettverk. Det er derfor stor grunn til å tro at slike logger vil bli svært attraktive på et kriminelt marked.

Datalagringsdirektivet truer personvernet

Selv om Datalagringsdirektivet ikke skal lagre innholdet i kommunikasjonen på internett, er det mye som kan avsløres ved hjelp av IP-adresser.

Ved å sjekke hvilke sider som besøkes, kan man finne ut svært mye om en person. Hvis f.eks. en person som jevnlig besøker nettstedet med homoerotisk innhold, religiøse debattforum eller dedikerte nettsamfunn for psykiske lidelser, vil det gi mye informasjon om vedkommende som er av svært privat karakter.

Datalagringsdirektivet gjør alle kriminelle

Til slutt vil jeg komme med en bemerkning som jeg i denne sammenheng synes er veldig viktig: Den dagen staten behandler alle som kriminelle, er dagen alle blir det.

Med dette mener jeg at dersom Datalagringsdirektivet implementeres, vil politiet miste sin naturlige og nødvendige autoritet blant store deler av befolkningen. Undertegnede anser seg selv som en lovlydig borger som ønsker et sterkt velfungerende politi, slik at vi unngår borgervern og aksept for kriminelle grupperinger. Dersom Datalagringsdirektivet implementeres, vil store deler av samfunnet stille seg svært skeptisk til politiets handlinger, og undertegnede frykter for samfunnskonsekvensene ved en slik utvikling.

Mvh
Anders Brenna
Medieutvikler