Samferdselsdepartementet
Postboks 8010 Dep
0030 OSLO

Oslo 7. april 2010

Deres referanse: 09/585-HK

Høringsuttalelse

Vedlagt finner dere Nei til EUs høringsuttalelse om datalagringsdirektivet.

Vennlig hilsen

(sign)
Heming Olaussen
Leder Nei til EU

Vigdis Hobøl
Fagmedarbeider

Nei til EU
Postadresse: Storgata 33, 0184 Oslo
Hjemmeside:www.neitileu.no.
Tlf: 22 17 90 20
E-post: neitileu@neitileu.no

Høringsuttalelse om Datalagringsdirektivet fra Nei til EUs Råd

SAMMENDRAG:

EUs datalagringsdirektiv er en regulering som griper inn i livet til hver enkelt borger ved å redusere verdien av privatliv og integritetsvern, og ved å svekke det godet det er å leve i et demokrati. Direktivet strider dessuten mot norske tradisjoner og eksisterende lover. Argumentene for at direktivet vil bistå politiet i arbeidet med bekjempe kriminalitet er svake og bygger i beste fall på anekdotisk materiale. Samtidig vet vi at direktivet vil koste fellesskapet mange titalls millioner kroner årlig – penger som etter vår mening kunne vært langt bedre benyttet på mer effektive typer kriminalitetsbekjempelse. På bakgrunn av dette mener Nei til EU at Norge må bruke vetoretten i EØS-avtalen mot direktivet, dersom direktivet i det hele tatt bør godtas som EØS-relevant.

Omfanget av direktivet

Regjeringas høringsnotat gjør greit rede for hva slags kommunikasjonsformer og hva slags abonnements-, lokasjons- og trafikkdata som omfattes av direktivet (i det etterfølgende brukes "trafikkdata" om alle disse tre typene data som omfattes av direktivet).

Høringsnotatet fortier imidlertid at det finnes en rekke elektroniske kommunikasjonsformer som *ikke* omfattes av direktivet av praktiske årsaker (de genererer ikke trafikkdata som kan lagres, eller det skjer på måter som gjør trafikkdata utilgjengelig for lagring), eller hvor trafikkdata ikke vil identifisere hvem som kommuniserer. Blant slike kommunikasjonsformer finnes blant annet (listen er ikke utdømmende):

- Bruk av anonyme mobilabonnementer kjøpt fra utenlandske tilbydere.
- De fleste former for bredbåndstelefoni/VoIP (Skype og liknende) som leveres av andre tilbydere enn brukerens primære telekom-leverandør.
- Ulike former for gratis web-baserte e-posttjenester som skjer fra tjenesteleverandører i utlandet og som ikke krever noen for identifisering av brukeren (eks. HotMail, Live og Gmail).
- Ulike former for meldings og chattetjenester over Internett (IRC, MSN, AIM, Spin). I tillegg til dedikerte chattetjenester har nesten alle online-spill en privat chattemodus som kan benyttes dersom man ønsker å kommunisere uten å bli overvåket.
- Nesten alle elektroniske oppslagstavler og sosiale nettsteder (Facebook, Orkut, Biip) har en funksjon for å sende private meldinger mellom individer og grupper.
- Diverse tjenester som benyttes via ulike former for anonymiseringstjenester, inklusive TOR, VPN, og Proxyer.

- Offentlige Internett-terminaler på biblioteker, bydelshus og Internett-kafeer.
- Åpne trådløse nett (disse finnes det for øyeblikket flere tusen av, bare i Oslo).

Etter vår mening vil det være sannsynlig at kriminelle, dersom lagring blir innført, rimelig raskt vil tilpasse seg den omstendighet at data vil bli lagret, og derfor velge å benytte seg av en kommunikasjonsform der data *ikke* blir lagret. Som en følge av dette er det likeledes sannsynlig at formålet med direktivet (kriminalitetsbekjempelse) ikke vil bli oppnådd.

Vi ser allerede eksempler på at slik kunnskap er i ferd med å spre seg. Den 7. januar ble det for eksempel lagt ut på Internett alvorlige trusler mot Kongsbakken videregående skole i Tromsø. Politiet etterforsket saken, men har nå lagt den til side med følgende begrunnelse:

Etterforskningen har blant annet brakt på det rene at det et benyttet avanserte metoder for å skjule dataspor på nettet, og det har ikke vært mulig spore trusselen til en konkret datamaskin. (Pressemelding fra politiet, 2010-02-25)

Det er ikke usannsynlig at trusselen ble framsatt av elever med tilknytning til skolen. Behersker skoleelever teknikker som gjør at de kan skjule sine elektroniske spor for politiet, er det ikke usannsynlig at kriminelle kan skaffe seg de samme kunnskapene.

Trafikkdata som bevis

I høringsnotatet hevdes det at trafikkdata har vært «viktige bevis» i en rekke større kriminalsaker. Rent spesifikt nevnes Baneheia-saken, «Operasjon ENEA» og NOKAS-saken (ss. 39-41).

Det er etter vår oppfatning feil at trafikkdata bidro til oppklaring av Baneheia-saken. Tvert i mot kan det argumenteres for at trafikkdata tilsynelatende ga hovedtiltalte alibi, jf.:

Telenor Mobil har i all hemmelighet gjennomført nye tester av mobildekningen i Baneheia. Målingene konkluderer på nytt med at det er umulig å ringe fra drapsåstedet via basestasjonen Eg A. [VK] skal på drapstidspunktet ha sendt tekstmeldinger via denne basestasjonen.
– Vi har ikke klart å gjenskape en slik situasjon, sier dekningsdirektør Bjørn Amundsen i Telenor Mobil. (Dagbladet 2001-12-09, s. 11)

Mens basestasjonen Eg A altså ikke dekker Baneheia, dekker den området rundt tiltaltes hjem, som er der tiltalte ifølge egen forklaring oppholdt seg på det tidspunktet drapene skjedde.

Heller ikke firmaet Teleplan, som av retten var oppnevnt som sakkyndig, klarte noensinne å oppnå mobildekning fra basestasjon Eg A på Baneheia. Teleplan konkluderte imidlertid med at nevnte trafikkdata var usikre og derfor ikke kunne gi tiltalte alibi, jf.:

Fram til ankesaken tidligere i år, ble firmaet Teleplan oppnevnt som uavhengig rettsoppnevnte sakkyndige i mobilspørsmålet. Deres konklusjon var at det var umulig å si noe sikkert om dekningsgraden for basestasjonen den aktuelle drapsdagen, 19. mai 2000. (Adresseavisen 2002-09-14, s. 12

Det skal ut fra dette godt gjøres å tolke overstående dit hen at trafikkdata fra tiltaltes mobiltelefonbruk var et «viktig bevis».

«Operasjon ENEA» var en større koordinert aksjon som politiet i Norge og Danmark i 2004 gjennomførte mot fildelingsnettverket Kazaa. I et fildelingsnettverk eksponerer de som deltar i nettverket sin IP-adresse. Politiet overvåket nettverket i tre døgn. Filene som ble utvekslet, ble automatisk sammenliknet med for politiet kjente bilder som viser overgrep mot barn. Totalt 850 000 bilder ble brukt som referansedatabase for operasjonen. På den måten identifiserte politiet IP-adressene til de som utvekslet overgrepsbilder som befant seg i politiets referansedatabase. Ved å koble disse IP-adressene med trafikkdata hos Internett-tilbydernes abonnementsregister kunne politiet identifisere hvilke datamaskiner og abonnementer som utvekslet overgrepsbilder. I Norge ble det i etterkant av aksjonen aksjonert mot ca. 250 abonnenter, noe som resulterte i 253 straffesaker, med 149 domfellelser og flere forelegg. Det er ingen tvil om at «Operasjon ENEA» var en viktig og vellykket politiaksjon mot de som utveksler overgrepsbilder på Internett.

Vi mener imidlertid det ikke er korrekt å anføre denne aksjonen som begrunnelse for å innføre langtidslagring av trafikkdata. Politiet overvåket nettverket i sann tid, og hadde dermed løpende oversikt over de relevante IP-adresser. I dag lagrer Internett-tilbyderne de data politiet er interessert i i tre uker. Det burde være tilstrekkelig med tid for politiet til på å rette henvendelse til tilbyderne for å sikre bevis. Dersom politiet har behov for mer enn tre uker for å analysere materialet har straffeprosessloven flere bestemmelser (jf. §§ 203, 210 og 216b) som gir politiet fullmakter til å sikre de nødvendige bevis. I høringsnotatet hevdes det (s. 39), på bakgrunn av den lange etterforskningstiden i ENEA-saken at «Politiet erfarer i dag at de ikke får tilgang på nødvendige data fordi disse rettmessig er slettet av tilbyderne.» Dette kan ikke være riktig, og i den utstrekning data politiet hadde behov for i ENEA-saken var slettet er dette politiet selv som må bære ansvar for, fordi de ikke utviste den nødvendige aktivitet for å sikre disse bevisene i tidsvinduet på tre uker etter at overvåkingen fant sted. Den omstendighet at politiet i en konkret sak valgte ikke å benytte seg av de rettsmidler de hadde til rådighet, kan ikke være noe argument for å innføre en slik ordning med generell langtidslagring av data.

I NOKAS-saken i 2004 var de impliserte seg bevisst at politiet benyttet trafikkdata fra mobiltelefoner for å kartlegge bevegelsesmønster. Ifølge boka «Dødsranet» (Hans Petter Aass og Rolf J. Widerøe, Gyldendal 2009) la derfor ranerne mobiltelefonene sine igjen i Oslo, slik at de ikke skulle kunne knyttes til Stavanger ved hjelp av lokasjonsdata. Ranerne var imidlertid ikke klar over politiet også benytter trafikkdata til å kartlegge sosiale nettverk. Ved hjelp av trafikkdata fra Telenor og Netcom var således politiet i stand til å kartlegge hvilke personer i ransmiljøet som sto hyppig i forbindelse med hvem i forkant av ranet, og på den måten å peke ut de mest sannsynlige mistenkte.

Det er ingen tvil om at politiets bruk av trafikkdata til å kartlegge kommunikasjonsmønstre i ransmiljøet var viktig for oppklaringen av NOKAS-ranet og opprullingen av det sentrale ransmiljøet på Østlandet. Det er imidlertid mer tvilsomt om dette vil fungere like godt i fremtiden. Som eksemplet fra NOKAS viser, har også profesjonelle kriminelle evne til å lære. På samme måte som NOKAS-ranerne hadde lært seg om politiets bruk av lokasjonsdata for å kartlegge bevegelser, vil etter alt å dømme kriminelle med «lærdommen» fra NOKAS-saken avholde seg fra å avsløre forbindelser seg imellom å bruke kommunikasjonskanaler som kan analyseres av politiet på denne måten. I fremtiden vil profesjonelle kriminelle derfor tilpasse seg ved å kommunisere på måter som ikke er sporbare på denne måten.

Presidenten for *European Confederation of Police*, Heinz Kiefer, sier i en kommentar til datalagrings-direktivet at han er:

sceptical as to whether [data retention] will actually help criminal investigations. [...] [I]t remains easy for criminals to avoid detection through fairly simple means, for example mobile phone cards can be purchased from foreign providers and frequently switched. The result would be that a vast effort is made with little more effect on criminals and terrorists than to slightly irritate them. (Europe wide retention of telecommunications data unlikely to help law enforcement agencies in the fight against terrorism[1], EuroCOP 2005)

Vi mener denne uttalelsen fra Heinz Kiefer er dekkende for hva slags effekt en innføring av datalagringsdirektivet vil ha på kriminalitetsbekjempelse.

Det er ingen ting som tilsier at effekten av den foreslåtte lagring mht. kriminalitetsbekjempelse vil være noe annet enn marginal. Samtidig vet vi at kostnadene for samfunnet vil være på mange millioner. Dermed må det stilles spørsmål om forventet nytteverdi ved lagring rettferdiggjør kostnadene for samfunnet. Vi mener at samfunnet hadde fått bedre uttelling i forhold til kriminalitets-bekjempelse dersom de samme pengene hadde vært brukt på andre og mer effektive former for kriminalitetsbekjempelse.

Personvernkommisjonen etterlyste flere steder i sin sluttrapport (ss. 24, 70, 222) en grundigere klargjøring i form av dokumentasjon av behovet for lagring, og viste i den sammenheng til dokumentasjonskravet om nødvendigheten av inngrepet som følger av artikkel 8 i EMK (Den Europeiske Menneskerettighets Konvensjon). Nei til EU konstaterer at det i høringsnotatet ikke gjøres noe seriøst forsøk på å levere noen for dokumentasjon for behovet for lagring, eller nytteverdien av lagring for kriminalitetsbekjempelse, ut over anekdotiske referanser til tre konkrete kriminalsaker. Etter vår mening er to av de tre saker som trekkes fram misvisende referert. Således bekrefter høringsnotatet Personvernkommisjonens inntrykk av at nødvendigheten av datalagring for kriminalitetsbekjempelse ikke er tilstrekkelig dokumentert til å oppfylle EMK art. 8.

Strategisk informasjonsanalyse

I høringsnotatet åpnes det opp for at politiet skal få tilgang til lagrede data dersom det finnes skjellig grunn til mistanke, selv om mistanken ikke kan knyttes til en konkret person (s. 48).

Dersom direktivet blir implementert i en slik versjon, innebærer dette i praksis at man i Norge åpner opp for å gjøre de lagrede data tilgjengelig for såkalt «strategisk informasjonsanalyse» (*data mining*). Dette er en teknikk der man analyserer store mengder data med det sikte på å finne mønstre som kan identifisere mulige gjerningsmenn. Teknikken er ikke helt ukjent, for eksempel benytter politiet i dag en slik teknikk dersom en forbrytelse er begått på eller nær et sted der det skjer videoovervåkning. Politiet vil da gjerne gå gjennom tilgjengelige overvåkningsvideoer for å kartlegge hvilke personer som befant seg på eller nær åstedet.

Det er ingen tvil om at strategisk informasjonsanalyse kan være nyttig for politiet i arbeidet med å identifisere mulig mistenkte og oppklare en forbrytelse. Samtidig er dette en teknikk som ansees som svært inngripende i forhold til personvernet. Dette blant annet fordi den gjør samtlige som er registrert i datamaterialet gjenstand for etterforskning, og fordi det gir politiet tilgang til såkalt overskuddsinformasjon som kan angå andre forhold enn det som er under etterforskning. Høyesterett i flere saker bekreftet at politiet har rett til å benytte seg av overskuddsinformasjon.

Vi mener at politiets analyse av overvåkningsvideoer befinner seg innenfor rammen av det som er forholdsmessig. Teknikken omfatter et lite antall personer (de som faktisk befant seg på eller nær

[1] http://www.eurocop-police.org/pressreleases/2005/05-06-02%20PRESS%20JHA%20Council_E.pdf

åstedet på et bestemt tidspunkt), gir politiet tilgang til forholds lite sensitiv informasjon (hvem som befant seg på et offentlig sted på et bestemt tidspunkt), og gir samtidig politiet anledning til å identifisere mulige vitner og gjerningsmenn. Når det gjelder å gi politiet adgang til at strategisk informasjonsanalyse av trafikkdata er dette etter vår oppfatning ikke forholdsmessig. For det første ligger det i datalagringsdirektivets natur at all kommunikasjon mellom norske borgere registreres og lagres, og det er derfor mulig at et data som gjelder for svært stort antall personer blir underlagt analyse. For det andre gir teknikken politiet mulighet til å kartlegge personers sosiale nettverk, som etter vår oppfatning er forholdsvis sensitiv informasjon. For det tredje er faren forholdsvis stor for at uskyldige blir trukket inn i etterforskningen (såkalte «falske positive») ved bruk av denne teknikken forholdsvis stor. Det å være uskyldig mistenkt og etterforsket for en forbrytelse er en stor belastning for de som det måtte gjelde, og er altså et uforholdsmessig sterkt inngrep i den enkeltes integritet. Norge bør på ingen måte åpne opp for politimessige metoder som øker befolkningens eksponering for dette.

Forholdet til kildevernet

I høringsnotatet (s. 50ff) gjøres det et poeng ut av at kildevernet ikke svekkes ved innføring av direktivet. Dette medfører etter vår mening ikke riktighet. Kildevernet etter gjeldende rett innebærer at politiet ikke kan etterforske saker ved å gjøre ransaking eller beslag i presselokaler. Beslag av journalists PC-er vil for eksempel kunne fortelle hvilken kilde som har gitt en journalist informasjon om en bestemt ved bruk av e-post, men et slikt beslag kan politiet i dag ikke gjøre pga. rettspraksis mht. kildevernet.

Denne retten uthules utvilsomt dersom man innfører bestemmelser som innebærer at politiet kan kartlegge hvem journalisten har kommunisert med, ved å hente ut trafikkdata om journalistens e-postkorrespondanse fra en teletilbyder. Dersom direktivet innføres i norsk lov må derfor kildevernet styrkes ved at det innføres bestemmelser som ikke bare beskytter redaksjonslokalene og journalisters utstyr mot beslag, men også mot utlevering av trafikkdata om kommunikasjon til og fra journalister og avisredaksjoner.

Direktivet i forhold til ytringsfriheten

I tillegg til at datalagringsdirektivet er ytterst problematisk sett fra et personvernperspektiv, mener Nei til EU at direktivet også er problematisk i forhold til ytringsfriheten.

Rent spesifikt mener vi at nytteverdien av lagring bør veies opp mot effekter på frimodighet, og at dette gjelder selv om formelle friheter ikke berøres, og selv om de registrerte data kun skal være tilgjengelige for politiet under regulerte forhold. Vissheten av at trafikkdata og lokasjonsdata om alle dine kontakter og kommunikasjoner både i det virkelige rommet og på Internett blir registrert, og at disse i kan gjøres gjenstand for politimessig etterforskning og analyse, kan være nok til å hemme borgere i utøvelsen av sine friheter til å samles, til å ytre seg, til å søke kontakt med andre individer, og til å søke opplysninger. Dette er helt grunnleggende rettigheter i et demokrati, som kommer til uttrykk både i norsk lovgivning og i Den europeiske menneskerettskonvensjon (EMK). Etter Nei til EUs oppfatning vil innføring av direktivet i norsk utvilsomt svekke rettsnytelsen hva angår privatliv og privat kommunikasjon, og vil dermed være et uforholdsmessig inngrep i ytringsfriheten.

Direktivets relevans for EØS-avtalen

Som det framgår av høringsnotatet eksisterer det nå en dom i EF-domstolen (som 2009-02-10, sak C-301/06 Irland mot Ministerrådet og EU-parlamentet) som slår fast at direktivet er vedtatt med hjemmel i artikkel 95 i EF-traktaten og derfor gjelder for det indre markedet som omfatter EØS.

Begrunnelsen for denne avgjørelsen er at tilbydernes plikt til å lagre data innebærer kostnader, og at harmonisering av reglene for datalagring i EØS-området derfor er viktig for å hindre konkurransevridning i det indre markedet.

Samtidig overlates det til medlemsstatene selv å bestemme lagringstiden og, ut over visse minimumskrav, hvilke krav det skal stilles til tilgangskontroll, kryptering, logging, systemseparasjon, og annen sikring av de lagrede data, samt hvorvidt kostnadene ved lagring skal dekkes av teletilbyderne eller av det offentlige. Det er åpenbart at når så mange forhold som påvirker kostnadssiden ved å innføre direktivet er overlatt til medlemslandene og utforme gjennom nasjonal lovgiving, er det en ren illusjon at direktivet innebærer en harmonisering av konkurransesituasjonen på telekommunikasjonsområdet. Ut fra dette mener vi at Norge bør argumentere for at direktivet ikke er EØS-relevant.

Dessuten: Gjennom de mange frihetsgradene mht. implementering av direktivet ligger det et klart incentiv for myndigheter og teletilbydere om å holde kostnadene ved lagring lave. Det er også dette Teleplan har lagt til grunn for sin analyse, jf: «Analysen tar som en forutsetning at tilbydere vil velge et sikkerhetsnivå for lagring av data som tilfredsstiller regelverket, men ikke høyere for å begrense kostnader.» (Teleplan 2006, s. 21).

Nei til EU oppfatter en slik tilnærming som svært bekymringsverdig. Utvidelsen med nye datatyper og den utvidede lagringstiden innebærer at sensitiviteten til dataene økes. Det tilsier at dersom disse data skal lagres, så må de beskyttes godt. Nei til EU oppfatter det som bekymringverdig at høringsnotatet ser ut til å legge til grunn en kostnadsmodell ved implementeringen der datasikkerheten ender opp som salderingspost.

Sikkerheten ved de data som lagres

Høringsnotatet berører bare summarisk hvordan de data som skal lagres skal sikres, og legger klare føringer på at dagens tekniske løsninger skal benyttes mer eller mindre uendret. Mye tyder imidlertid på at diverse organisasjoner som i dag lagrer data, ikke har fullgode mekanismer for sikring av trafikkdata mot uautorisert spredning.

Ifølge Teleplans analyse vil lagring, inklusive sikring, koste mellom 207 og 261 millioner NOK over en femårsperiode (s. 52). Så vidt vi kan forstå tar Teleplan i så fall ikke høyde for kostnader forbundet med bedre sikring av data enn minimumskravene. Telenor har ifølge Berit Svendsen vurdert kostnaden til å ligge på 250 millioner NOK pr år[2]. Vi kan ikke gå inn på disse konkrete tallene, men mener at dersom data skal lagres, så må de sikres vesentlig bedre enn det ser ut til at Teleplan har lagt til grunn.

Nei til EU vil i den forbindelse vise til den såkalte Tele2-saken, hvor Tele2 våren og sommeren 2007 lot kredittopplysninger om et sekssifret antall personer tilflyte uvedkommende. En enda større skandale fant sted i Storbritannia høsten 2007, hvor to ukrypterte disker med personopplysninger

[2] http://www.liberaleren.no/2008/03/13/referat-fra-horingen-om-datalagringsdirektivet/

vedrørende alle familier i Storbritannia med barn under 16 år kom på avveie[3]. Det øker utvilsomt risikoen for misbruk når man øker mengden med data som lagres, og når man forlenger tiden data skal lagres. Dette må kompenseres med at det fra myndighetens side settes krav til bedre sikring i form av kryptering og deponeringsmekanismer (eschrow) som hindrer at så vel teletilbyderen selv, som myndighetene, kan få tilgang til lagrede data før korrekt rettslig grunnlag for tilgang kan fremlegges. Det må også sikres at enhver tilgang som gis, avgrenses til kun de data det skal være lovlig tilgang til, og det må etableres sikringer – tekniske og organisatoriske så vel som juridiske – mot at det lagrede materialet kan brukes til strategisk informasjonsanalyse eller andre former for generell informasjonssøking. I forhold til den tekniske siden vil dette innebære at det må utvikles helt nye, finmaskede systemer for tilgangskontroll og datasikring som, dersom de tekniske problemene knyttet til slik utvikling overhode lar seg løse, kommer til å koste langt mer i utvikling og drift enn de lagringsløsninger som benyttes i dag.

Direktivet i forhold til den Europeiske Menneskerettighets Konvensjon (EMK)

EMK artikkel 8 annet ledd åpner for at det kan gjøres inngrep i personvernet. For at et slikt inngrep skal være forsvarlig må det blant annet være nødvendig i et demokratisk samfunn. Dette berører i høringsnotatet på sidene 26-28. I høringsnotatet hevdes det at et slikt nødvendighetsprisnipp eksisterer.

Men i høringsnotatet underslås det at det etter praksis i Den Europeiske Menneskerettighetsdomstolens (EMD) framgår at «nødvendig» må tolkes strengt. EMD sier at det må være en «pressing social need» for å gripe inn i personvernet. Det holder ikke at det er hensiktsmessig, rimelig eller ønskelig. Vi mener at dette vilkåret på ingen måte er oppfylt. Dette blant annet fordi politiet allerede i dag gjennom blant annet straffeprosessloven har de fullmakter de trenger for å innhente og sikre bevis i saker der trafikkdata er viktige for kriminalitetsbekjempelse.

I tillegg til nødvendighetskravet følger det av EMDs praksis at inngrepet i personvernet som gjøres må være proporsjonalt i forhold til formålet som ønskes oppnådd. Proporsjonalitetsprinsippet drøftes ikke i høringsnotatet.

Den omfattende lagringsplikten som følger av direktivet kan etter Nei til EUs oppfatning være problematisk i forhold til både nødvendighetsprinsippet og proporsjonalitetsprinsippet som følger av EMK art. 8.

Konklusjon

Nei til EU mener at datalagringsdirektivet innebærer sterke personvernulemper, mens nytteverdien i forhold til kriminalitetsbekjempelse verken er tilstrekkelig dokumentert eller rimelig å anta. Nei til EU mener således at direktivet ikke er forenlig med EMK art. 8, og dermed heller ikke med menneskerettsloven § 2, og at Norge derfor av sitt eget lovverk er forpliktet til å bruke vetoretten nedfelt i EØS-avtale mot direktivet - jf. også utredningen for Samferdselsdepartementet om direktivet og EØS-avtalen av professorene Arnesen og Sejersted. Etter Nei til EUs oppfatning er direktivet, slik det er utformet, ikke relevant i forhold til EØS-avtalen.

[3] Se: *Brown apologises for records loss*, BBC News, 21. november 2007, http://news.bbc.co.uk/2/hi/uk_news/politics/7104945.stm.