

Tilburg University

Anonymitet og ansvar på Internettet

C Roosendaal, A.P.

Published in:
Lov & Data

Publication date:
2006

[Link to publication in Tilburg University Research Portal](#)

Citation for published version (APA):
C Roosendaal, A. P. (2006). Anonymitet og ansvar på Internettet. *Lov & Data*, 86(2-2006), 25-27.

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Riktig god sommer!

Dansk regelverk	
Internettauksjoner	24
Politi- og domstolreform	24
Diverse	
Bug	23
Historisk søking	34
Jusnytt.no	35
Kompetanseforhold	31
Piray-tegneserie	8
Domenenavn/varemerke	
ATF-praksis	20
Ergonia.dk	23
Nettfinn og Finn	12
Tvisteløsning	14
Weisse Seiten	19
Dyplinking	
Home og Ofir	1
Finn og Supersøk	4
Konferanser	19
Litteratur	
Artikler	33
Bøker	33
CompLex	33
Lovsang	11
Lovdata	36
Opphavsrett	
Dansk lovforslag	30
Musikk	32
Personvern	
EU-rapport	29
Lycos v. Pessers	25
Personopplysninger til tredjeland	30
Vampyrer	28
Telekommunikasjon	
Dansk lovforslag	30
Direktiv om lagring av teledata	31

Principiel dom i OFIR-sagen af Janne Glæsel

OFiR **home**
det gør ikke noget man er foran

Sø- og Handelsretten i Københavns dom af 24. februar 2006 i sag V-108-99 home a/s (advokat Dorte Wahl) mod OFIR a-s (tidligere: Søndagsavisen a-s) (advokat Janne Glæsel).

Dom om databaserettigheder, robottering, god markedsføringskik og deep linking.

Indledning

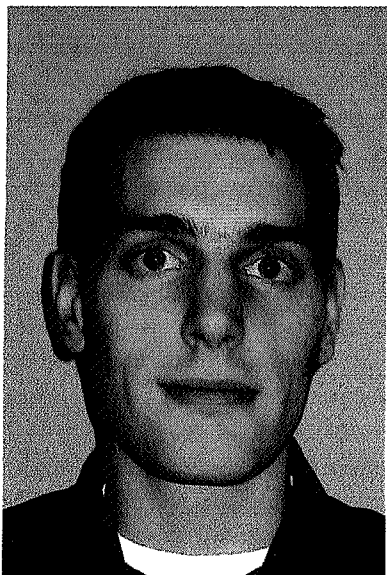
Sø- og Handelsretten i København har ved sin dom af 24. februar 2006 afgjort denne sag, som har verseret for retten siden 1998. Sagen var anlagt af home a/s («Home») - en af de største ejendomsmæglerkæder i Danmark - mod OFIR a-s («OFIR»), som er et selskab under det danske bladhus Søndagsavisen. Dommen har været ventet med spænding i IT-branchen, fordi rækkevidden af beskyttelsen efter den danske ophavsretslovs § 71 har været usikker og retsstillingen omkring deep linking ligeledes har været uafklaret.

Sagens omstændigheder

Homes forretningsmodel er baseret på en franchise, hvorunder Home bl.a. stiller en række faciliteter til rådighed for franchisetagerne. Det drejer sig bl.a. om hjemmesiden *home.dk* og en landsdækkende database med oplysninger om ejendomme til salg. Databasen er tilgængelig via hjemmesiden *home.dk*, hvor hjemmesidens brugere har mulighed for - ved at vælge blandt nogle på forhånd definerede kriterier - at søge på ejendomme, som er sat til salg gennem Home. En sådan søgning på Homes hjemmeside vil generere en resultatliste med links til de ejendomsannoncer, som matcher de valgte søgekriterier. De enkelte ejendomsannoncer findes således som undersider til *home.dk*. Ejendomsmæglerne i homekæden driver de enkelte ejendomsmæglerforretninger i selvstændige juridiske enheder. Ejendomsmæglerne overfører oplysningerne om de ejendomme, der annonceres til

Anonymitet og ansvar på Internettet

av Arnold Roosendaal



Den nederlandske dommen

I Nederland har høyesterett tatt stilling til spørsmålet om anonymitet i avgjørelsen *Lycos v Pessers*. Pessers solgte frimerker på nettstedet «<http://www.ebay.com>». Kjøpere kan gi uttrykk for sine erfaringer ved å skrive til nettsiden, og selgere kan svare på dette – hver får en linje til disposisjon. Denne «korrespondansen» er tilgjengelig for allmennheten. Pessers hadde 24.787 positive, 299 negative og 217 nøytrale reaksjoner fra kjøpere.

Den annen part var Lycos, et globalt internetselskap. Lycos tilbyr blant annet vertstjenester på Internettet. Domenet <http://members.lycos.nl> inneholdt en nettside som kalte seg «stopthefraud». Inntil 4.8.2003 inneholdt nettsiden den følgende teksten:

Har du noen gang blitt lurt av Pessers på eBay, så støtt kampen for rettferdighet! Hvordan opererer han? Du kjøper en liten post. Som han sender til deg. Slik får han din tillit. Du føler deg trygg nok til å kjøpe en dyrere post. Da slår han til! Han beholder pengene og du får ingen frimerker. Og det er ikke alt. Noen av ofrene hans forteller at han selger falske merker. Er du blitt lurt og øn-

sker å offentliggjøre din historie? MAIL historien din til stopthefraud@hotmail.com ...”

Det var enkelte «historier» på nettstedet – forfatterne var bare angitt med initialer – om problemene man hadde hatt med å kjøpe frimerker fra Pessers.

Pessers sendte 1.8.2003 et e-brev til nettstedet og ba operatøren om å stanse virksomheten og identifisere seg. Da han ikke fikk svar, sendte Pessers en faks til Lycos hvor han ba om at nettstedet skulle stenges, og om å få navn, adresse og fødselsdato til operatøren av nettstedet. Lycos svarte ved brev 4.8.2003 at selskapet ikke ville etterkomme anmodningen. Samme dag ble følgende tekst postet på nettstedet: «Nettstedet er fjernet for å unngå rettlige tiltak!»

Pessers anla straks sak mot Lycos. Retten sondret mellom de to kravene. Siden nettstedet var fjernet av operatøren, ble dette kravet avvist. Retten vurderte deretter Pessers krav om å bli gjort kjent med brukerens navn og adresse. Fødselsdatoen ble ansett som irrelevant. Pessers hevdet at han trengte navn og adresse for å stevne brukeren av nettstedet med krav om erstatning. Høyesterett kom til at Lycos måtte gi ham disse opplysningene.

Høyesterett nærmet seg avgjørelsen skritt for skritt, og vurderte hvert skritt i forhold til ansvarsregimet i EUs ehandelsdirektiv (direktiv 2000/31/EF). Lycos hevdet at direktivet ikke tillot at man ble dømt til å oppgi identifiserende opplysninger. I det minste krevde direktivet at det inkriminerende innholdet var åpenbart urettmessig i forhold til den krenkende part. *Dette argumentet* var basert på oppfatningen av at direktivet har en begrensende regulering, noe som

betyr at visse avgjørelser bare tiltales hvis betingelsene i artikkel 14 ikke er oppfylt. Retten forkastet dette synet, og mente at det var flere argumenter i direktivet som støttet en ikke-begrensende tolkning. Begrensningene av nettleverandørens ansvar utelukker ikke plikten til å påta seg ansvar for å spore og unngå ulovlige handlinger. Dette følger særlig fra fortalen pkt 48 og bekreftelsen av dette i pkt 15, 45 og 52. Fortalens pkt 54 understreker også at de påbudte sanksjonene i direktivet ikke står i veien for nasjonale sanksjoner eller muligheter til å fremme krav. Dessuten kreves det etter direktivet et høyt nivå for beskyttelsen av generelle interesser, særlig vern av menneskelig verdighet og forbrukere (fortalen pkt 10). Dette må garanteres av effektiv beskyttelse av ofre for ulovlige handlinger på Internettet. Nederlandske forarbeider understreket dette ved å si: «Tjenesteleverandører kan være forpliktet til å gi opplysninger som identifiserer brukerne av deres tjenester ... For fullstendighetenes skyld finnes muligheten også i privatretten for dommeren til å bestemme at tjenesteleverandøren må gjøre kilden for opplysningene kjent.» (Forarbeidene til loven som implementerer direktivet om elektronisk handel, Kamerstukken II 2001-2002, 28 197, nr 3, blz 28).

Dette betyr at direktivet skal tolkes som ikke inneholdende begrensninger. En annen tolkning ville dessuten ha det uheldige resultat at en gruppe ofre for ærekrenkelser på Internettet ville mangle effektiv rettslig beskyttelse.

Det andre argumentet til Lycos var at et krav om å få tilgang til identifiserende opplysninger bare tillates som et subsidiært krav sammen med et primært krav rettet mot den ulovlige handlingen. Derfor måtte Lycos ha vært an-

svarlig for en ulovlig handling ut-
over det å nekte tilgang til identifi-
serende opplysninger. Dette ble
også forkastet av høyesteretten. Et
krav om tilgang til identifiserende
opplysninger må vurderes uav-
hengig av den ulovlige handlingen.
I visse situasjoner kan det å unnla-
te å gi slike opplysninger være
ulovlig i seg selv fordi det strider
mot plikten til å styrke sosial at-
ferd. Dette betyr at det ikke er en
generell regel, men at hvert enkelt
tilfelle må vurderes konkret.

Det tredje argumentet til Lycos be-
sto av to deler. Den første delen
angikk standarden for å vurdere
den urettmessige handlingen til Ly-
cos. Lycos hevdet at hvis innholdet
ikke klart var ulovlig, så må man i
prinsippet ikke oppgi identifiserende
opplysninger med mindre
situasjonen er helt spesiell. Dess-
uten er prinsippet for vurdering så
generelt at det ville ha uheldige
virkninger utenfor Internettet.
Lycos mente også at det var en
selvmotsigelse, ettersom Lycos på
den ene siden ikke var forpliktet
til å fjerne innholdet fra nettstedet,
mens det på den annen side skulle
være en rettslig forpliktelse å gjøre
kjent de identifiserende opplys-
ningene og dermed bryte taushets-
plikten i forhold til kunden. Retten
svarte ved å fremheve at avgjør-
elsen bare gjaldt i det enkelte til-
fellet. Innvendingene til Lycos ble
avvist fordi det i ethvert tilfelle er
nødvendig å ta hensyn til de fore-
liggende omstendighetene og inter-
essene.

Den andre delen refererer seg
til personvern og ytringsfrihet og
kravet til proporsjonalitet. Anony-
mitet kan også være vernet av
ytringsfrihet under Den europeis-
ke menneskerettighetskonven-
sjonen art. 10 hvis det offentlig-
gjorte skader andre og ikke er
knyttet til alvorlige krenkelser.
Høyesteretten fant at man ikke
uten videre kunne se bort fra hen-
synet til ytringsfrihet, men at det
ikke er en absolutt rettighet.

Videre hevdet Lycos at det ikke
var risiko for videre formidling og
at det var et realistisk strafferetts-
lig alternativ for å kreve tilgang til
de identifiserende opplysningene.
(Dette i motsetning til hva som
var tilfellet i Deutsche Bahn/
XS4All, Vzr Rb Amsterdam
25.4.2002, *Mediaforum* 2002-6 nr
24 og Hof Amsterdam 7.11.2002,
Mediaforum 2003-1 m nt AH Ek-
ker, hvor avslaget på å identifisere
kunden ble ansett urettmessig *fordi*
faren var tilstede for videre for-
midling.) Risikoen for videre for-
midling av det krenkende material-
et måtte ses atskilt fra kravet om å
få tilgang til identifiserende materi-
ale. Dessuten ville ikke straff nød-
vendigvis sikre raske og effektive
tiltak. «Straffeprosesslovens 126a
har strenge krav til bruk av be-
stemmelsen, som betyr at den
vil brukes i begrenset utstrekning»
(Vzr Rb Utrecht, 12.7.2005, KG-
nr 194741/KGZA 05-462,
BREIN/Providers, ro 4.6.) *Det*
siste argumentet til Lycos var at den
nederlandske lovens bestemmelse
ikke oppfylte kravene til Den
europeiske menneskerettighets-
konvensjon art. 8(2), og at be-
grensningene av rettighetene etter
konvensjonens art. 8 og 10 ikke
var nødvendige i et demokratisk
samfunn. Høyesteretten tilbakevis-
te dette argumentet fordi den
nederlandske lovgivningen nettopp
angir at disse interessene skal veies
mot hverandre, særlig hensynet til
personvern.

Resultatet ble at Lycos måtte
oppgi de identifiserende opplys-
ningene slik at Pessers kunne reise
sak mot ærekrenkeren. Avgjørel-
sen er svært konkret, og bygger på
en avveining av motstridene inter-
esser i forhold til de aktuelle be-
stemmelsene. Dette synes å måtte
kreves for hvert tilfelle. Det gene-
relle prinsippet er at retten til ano-
nymitet ikke er absolutt når ano-
nymitet misbrukes for ærekrenk-
else. Enkelte virkninger av denne
avgjørelsen diskuteres nedenfor.

Konsekvenser av den nederlandske avgjørelsen

Det synes ikke å foreligge klare
regler ansvar for internettleveran-
dører. EU-direktivet gir noen indi-
kasjoner, men i den første
rapporten fra Kommisjonen om
anvendelsen av direktivet, er det
allerede bemerket at «et par av de
vedtatte lovene har problemer
særlig i forhold til betingelsene for
ansvar for mellombbrukere til
Internettet». (Report from the
Commission to the European Par-
liament, the Council and the Euro-
pean Economic and Social Com-
mittee – First Report on the appli-
cation of Directive 2000/31/EC
of the European Parliament and
of the Council of 8 June 2000 on
certain legal aspects of informa-
tion society services, in particular
electronic commerce, in the Inter-
nal Market (Directive on electro-
nic commerce), § 3.3 – [http://
www.europa.eu/eur-lex/en/com/rpt/
2003/com2003_0702en01.pdf](http://www.europa.eu/eur-lex/en/com/rpt/2003/com2003_0702en01.pdf))

I tillegg til den mangelen på
klarhet som gjelder for direktivet,
har medlemsstatene frihet til også
å regulere andre situasjoner (*Id*
§ 64.) Det synes klart at EU i
direktivets art. 15 forhindret at
medlemsstater «i forhold til aktivi-
teter dekket av art. 12-14 krever
en generell overvåking av opplys-
ninger som formidles eller lagres,
eller en generell plikt til aktivt å
lete etter fakta eller forhold som
indikerer ulovlig virksomhet. Det-
te er viktig, ettersom alminnelig
overvåking av millioner av nett-
steder eller -sider i praksis ville væ-
re umulig, og ville ha ført til ufor-
holdsmessige byrder for mellom-
brukerne og høyere kostnader for
brukeres tilgang til grunnleggende
tjenester» (*Id* § 72). Kommisjonen
har ikke til formål å innføre en
generell forpliktelse til overvåking.
Internettleverandører kan holdes
ansvarlig, men på hvilke vilkår
dette skjer, vil være opp til nasjo-
nal lovgivning. Fra dette synspunkt
har den nederlandske høyesterett

valgt riktig når den har veid sammen de relevante interessene for å komme til sin avgjørelse.

Problemet er imidlertid at denne avgjørelsen, som støttes av europeisk lovgivning, åpner veien for utallige lignende krav. Organisasjoner som BREIN, den nederlandske interesseorganisasjonen for rettighetshavere til musikk, film og datamaskinprogrammer, har allerede hevdet at det er en prinsippavgjørelse. «Lycos v Pessers handler om et offer kan holde noen ansvarlig for ærekrenkelse. Det samme prinsippet må gjelde hvis BREIN ber en internettleverandør om identifiserende opplysninger om en person som krenker rettigheter så de kan anlegge sak i forbindelse med ulovlig utnyttelse av musikk, filmer eller interaktive programmer (Hoge Raad: ISP mot et NAW-gegevns afstaan, http://www.anti-piracy.nl/Nieuws/bericht_0064.html [2006-01-29]). I henhold til avgjørelsen må internettleverandøren avgi opplysningene hvis «urettmessigheten er sannsynliggjort og den fornærmede har begrunnet sine interesser. Fornærmede må ikke anlegge sak for å tilfredsstillende dette kravet.»

BREIN har allerede forsøkt å få tilgang til identifiserende opplysninger om brukere av peer2peer-programmer fra internettleverandører. Alle betingelser for å få tilgang til disse opplysningene, var oppfylte. Men rettssaken låste seg fordi BREIN hadde behandlet data på en måte som ikke var tillatt etter nederlandsk lovgivning og vilkår stilt av den nasjonale personvernmyndigheten. For å samle IP-adresser, hadde de rekruttert tjenestene til et privat, amerikansk selskap. Retten sier: «USA kan ikke anses som et land med et tilsvarende nivå for vern av personlige opplysninger.» (Vzz Rb Utrecht, 12.7.2005, KG-nr 194741/KGZA 05-462 (BREIN/Providers) ro 4.26). Dessuten had-

de det amerikanske selskapet skaffet seg tilgang til «shared folders» for de aktuelle IP-adressene. «Blant disse filene kan det også være filer som ikke krenker rettighetene til andre eller som kan ha en personlig karakter.»

Hvis betingelsene hadde vært oppfylt, kunne man kanskje ha vunnet frem med kravet. Dette betyr at hvis identifiserende data forespørres fra krenkede parter (eller en person som hevder å være offer for en ærekrenkelse), må internettleverandørene selv vurdere de ulike interessene: På den ene siden den anonyme leverandørens interesse i å formidle opplysninger eller innhold basert på ytringsfriheten. På den annen side interessen i den som hevder å være krenket, i å bringe ærekrenkelsene til opphør og kreve erstatning fra krenkeren. Internettleverandørens stilling er vanskelig. Vurderingen av innholdets lovlighet må baseres på en personlig oppfatning, eventuelt støttet av uttalelser fra eksperter. Men det er alltid en risiko for at man «tar feil». Hvis internettleverandøren ikke fjerner siden og gir fra seg de identifiserende opplysningene, kan en senere rettsavgjørelse holde leverandøren ansvarlig for ikke å ha hindret videreformidling. Og hvis leverandøren fjerner siden og avgir identifiserende opplysninger, kan en senere avgjørelse gå ut på at innholdet ikke var ærekrenkende – da vil retten til anonymitet og ytringsfriheten være krenket. Også i slike tilfeller kan leverandøren bli ansvarlig. Leverandøren vil velge den utvei som har den laveste risikoen. Handlingene til leverandøren vil i praksis ha betydning for ytringsfriheten. Dette betyr at strenge regler for ansvar kan ha en «chilling effect» på informasjonssamfunnet. Internettleverandørene vil være for forsiktige, med den virkning av selvreguleringen begrenser tilbudet av informasjon på Internettet. For å unngå dette proble-

met har justisministeren foreslått opprettelsen av et nasjonalt institutt med eksperter som kan gjøre vurderingen. Instituttet vil utvikles av det nasjonale senteret for høyteknologisk kriminalitet (NHTCC, jf. Kamerstukken II, vergaderjaar 2004-2005, 28 197, nr 22).

Dette understreker et forhold som er sterkt sammenvevet med anonymitet. En avgjørelse om å fjerne anonymitet må treffes med forsiktighet fordi den er irreversibel (jf. Vzz Rb Utrecht 9.7.2002 (Teleatlas/Planet), KG 2002, 209 *Computerrecht* 2002/5 m nt WAM Steenbruggen). Anonymitet kan ikke gjenopprettes hvis avgjørelsen senere viser seg å være uriktig. Anonymitet har derfor en svært sensitiv karakter. Internettleverandøren bør ikke gjøres ansvarlige for å vurdere interessene til ulike aktører knyttet til Internettet. Andre løsninger er velkomne. Den nederlandske løsningen er generelt gunstig, men det løser ikke alle spørsmål tilfredsstillende.

Arnold Roosendaal er forsker ved Tilburg Institute for Law, Technology and Society (TILT), Universitetet i Tilburg, Nederland.

Artikkelen er et utdrag av «Elimination of anonymity in regard to liability for unlawful acts on the Internet», Sylvia Mercads Kirkegaard (ed) *Legal, Privacy, and Security Issues in Information Technology* (vol 2), Institutt for rettsinformatikk, Oslo 2006:213-227.