ERHVERVS- OG VÆKSTMINISTERIET

N O T A T

Juni 2012

Oversigt over juridiske og tekniske håndhævelsesmetoder i Danmark og EU

1. Introduktion

I det følgende gives en oversigt over de juridiske og tekniske håndhævelsesmetoder på internettet, som anvendes i Danmark og andre EU-lande. Oversigten er udarbejdet af Erhvervsstyrelsen med inddragelse af Justitsministeriet, Rigspolitiet, Spillemyndigheden, Sundhedsstyrelsen, Konkurrence- og Forbrugerstyrelsen, Patent- og Varemærkestyrelsen, DIFO/DK-Hostmaster, Statsadvokaten for særlig økonomisk kriminalitet samt Kulturministeriet. I oversigten eksemplificeres der bl.a. med indsatsen på det ophavsretlige område, idet dette område frembyder en omfattende praksis.

Der findes ikke en samlet oversigt over europæiske håndhævelsesmetoder på internettet. Oplysninger vedrørende tekniske og juridiske håndhævelsesmetoder i andre europæiske lande er tilvejebragt dels ved en høring af BEREC (Body of European Regulators of Electronic Communications) i sommeren 2011, dels ved en supplerende høring af de europæiske myndigheder, der er repræsenteret i ICANN's (Internet Corporation for Assigned Names and Numbers) Governmental Advisory Committee (GAC) i april 2012. Der er alene medtaget oplysninger fra de europæiske lande, som har afgivet oplysninger herom.

2.1. Generelt om håndhævelse, påtale og sanktioner

Håndhævelse på internettet kan ske igennem tre forskellige kanaler: civilretlig håndhævelse, administrativ håndhævelse og strafferetlig håndhævelse.

Civilretlig håndhævelse finder som om udgangspunkt sted, når en krænket part bliver opmærksom på eventuelle krænkelser af sine rettigheder i henhold til særlovgivningen (fx ophavsretten) på internettet. Den krænkede part kan herefter dokumentere krænkelserne og indbringe eventuelle krænkelser for domstolene. Det er herefter domstolene, der fastsætter passende fogedforbud, sanktioner, erstatning, godtgørelse m.v. ud fra de gældende regler indenfor det relevante lovgivningsområde.

Administrativ håndhævelse på internettet forekommer ikke indenfor ophavsretten, men indenfor fx lægemiddelområdet og spilområdet er de relevante administrative myndigheder givet en række reaktionsmuligheder.

Strafferetlig håndhævelse af ophavsretten kan ske på flere måder. Dels kan der i visse tilfælde ske inddragelse af et bødekrav i en civil retssag. Krænkelser på internettet kan også være underlagt betinget offentlig påtale. Politiet kan iværksætte efterforskning og anklagemyndigheden kan rejse tiltale på grundlag af en indgivet politianmeldelse eller på eget initiativ, i meget alvorlige sager eller hvis almene hensyn gør dette påkrævet.

2.2. Fogedforbud

Reglerne om fogedforbud fremgår af retsplejelovens kapitel 57.

Bestemmelserne betyder, at fogedforbud kan nedlægges, hvis det kan godtgøres eller sandsynliggøres:

- at de handlinger, der søges forbudt, strider mod rettighedshaverens ret
- at den, som fogedforbuddet retter sig imod, vil foretage handlingerne, som søges forbudt
- at formålet vil forspildes, såfremt rettighedshaveren henvises til at gøre sin ret gældende gennem en almindelig rettergang.

I det omfang der nedlægges fogedforbud, skal forbuddet justificeres under en senere retssag. Hvis rettighedshaverne anmoder om, at forbuddet nedlægges over for en mellemmand (fx en hjemmesideudbyder), kan denne intervenere som part i forbudssagen, hvis nedlæggelse af et forbud vil stride imod den pågældendes ret. Indtrædelsen sker ved en erklæring herom til fogedretten.

Fogedforbudsreglerne har blandt andet været anvendt i Danmark til blokering af adgang til hjemmesiderne www.allofmp3.com (2006), www.thepiratebay.org (2010) og www.grooveshark.com (2012).

Der findes tilsvarende europæisk lovgivning og retspraksis vedrørende blokering af adgang til hjemmesider, jf. afsnit 3.

2.3. E-handelsloven – generelle ansvarsprincipper

Lov nr. 227 af 22. april 2002 om tjenester i informationssamfundet, herunder visse aspekter af elektronisk handel (e-handelsloven) indeholder en række regler, der normerer ansvaret for internetmellemmænd. Loven gennemfører Europa-Parlamentets og Rådets direktiv 2000/31/EF af 8. juni 2000. Tjenester i informationssamfundet er tjenester, der har et kommercielt sigte og som leveres online (ad elektronisk vej over en vis distance) på individuel anmodning fra en tjenestemodtager. De internetmellemmænd, der er omfattet af loven, kan eksempelvis være indholdsudbydere (af fx hjemmesider) eller internetudbydere.

Ansvarsreglerne for indholds- og internetudbyderne findes i e-handelslovens §§ 14-16, som vedrører tjenesteudbydere, der foretager videreformidling, caching og oplagring af indhold. Fælles for disse tre ydelser er overordnet set, at de vedrører behandling af information, som ikke stammer fra tjenesteudbyderen selv. For at indholds- og internetudbyderne kan undgå at ifalde ansvar, skal tjenesteudbyderens aktivitet være af udelukkende teknisk, automatisk og passiv karakter, og tjenesteudbyderen må ikke have hverken kendskab til eller kontrol over de informationer, der transmitteres eller oplagres. Det betyder også, at tjenesteudbyderen ikke må ændre de informationer, der bliver videreformidlet. Er disse betingelser ikke opfyldt, kan udbyderen gøres ansvarlig for medvirken til en ulovlig handling efter de almindelige erstatningsretlige eller straferetlige regler.

Det følger af e-handelsdirektivet, at medlemsstaterne ikke må pålægge indholds- og internetudbyderne en generel forpligtelse til at overvåge den information, der transmitteres eller oplagres i udbydernes net. Indholds- og internetudbydere må heller ikke pålægges en generel forpligtelse til aktivt at undersøge forhold eller omstændigheder, der tyder på ulovlig virksomhed. Disse skal imidlertid reagere, hvis de bliver gjort bekendt med ulovligheder.

2.3.1. ” Notice and take down”

For så vidt angår ansvaret for indhold på populære indholdstjenester, som eksempelvis www.youtube.com, forudsætter ansvarsfritagelsen i e-handelsloven blandt andet, at en indholdsudbyder ikke er bekendt med det aktuelle ulovlige indhold på sine tjenester. Bliver en indholdsudbyder gjort bekendt med ulovligt indhold på sin tjeneste og ikke reagerer eller handler herpå, bortfalder indholdsudbyderens ansvarsfrihed. Disse ansvarsprincipper har i visse europæiske lande udmøntet sig i egentlige “notice and take down” modeller. Proceduren i sådanne modeller er typisk den, at den ansvarlige indholdstjenesteudbyder skal fjerne krænkende materiale, når de bliver gjort opmærksom på det. Disse kendes også som ”notice and take action” modeller. Som eksempler herpå kan nævnes:

- Holland, hvor der mellem rettighedshavere og internetudbydere er indgået aftale om et adfærdskodeks, der beskriver en ”notice and take down”-procedure i forbindelse med krænkelse af ophavsrettigheder.

- Tyskland, hvor der anvendes ”notice and take down” til bekæmpelse af børnepornografisk materiale på internettet. Proceduren er baseret på en samarbejdsaftale mellem politiet, internetudbydere og selvregulerende organer, f.eks. International Association of Internet Hotlines (Inhope).

- Ungarn, hvor der i den ungarske lov om elektronisk handel og internetsamfundets tjenester i forbindelse med krænkelse af ophavsrettigheder anvendes "notice and take down".

- I Sverige anvendes en "notice and take down"-procedure, hvorefter en tjenesteudbyder er forpligtet til at fjerne ulovligt materiale, fx ophavsretskrænkende materiale, børnepornografisk materiale, markedsføring af ulovlige lægemidler m.v. fra internettet eller på anden måde forhindre udbredelsen af sådant materiale, når udbyderen bliver opmærksom på det ulovlige materiale. Hvis tjenesteudbyderen ikke efterkommer denne forpligtelse, kan vedkommende ifalde strafferetligt ansvar. I overensstemmelse med den svenske lovgivning, skal en tjenesteudbyder fjerne eller på anden måde forhindre udbredelse af meddelelser på tjenesteudbyderens tjeneste, hvis indhold tilskynder til overtrædelse af forhold omfattet af den svenske straffelov, fx oprør, agitation mod etniske grupper, børnepornografi og vold m.v. Tjenesteudbyderen skal kontrollere sin tjeneste i et omfang, der er rimeligt, omfanget af og formålet med tjenesten taget i betragtning.

Konkurrence- of Forbrugerstyrelsen har oplyst, at den ikke er bekendt med sager i Danmark om brugen af e-handelslovens §§ 14-16, herunder "notice and take down".

2.4. Spilleloven – forbud mod transmission og betalingsformidling

Ved lov nr. 848 af 1. juli 2010 om spil blev der i lovens § 65 indført et specifikt forbud, hvorefter betalingsformidling af indsatser og gevinster til og fra en ulovlig spiludbyder samt transmission af information på et kommunikationsnet til et ulovligt spilsystem ikke er tilladt. Bestemmelsen omfatter internetudbydere, der stiller internettets navneservere (Domain Name Service – se afsnit 3.1) til rådighed for egne slutbrugere eller andre udbyderes slutbrugere ved at transmittere information (levere internetadgang) til et bestemt internetdomæne med et ulovligt spilsystem.

Spillemyndigheden vil i henhold til § 65 rette henvendelse til internetudbyderen eller betalingsformidleren i form af en henstilling. Henstillingen skal alene tjene det formål at give internetudbyderne og betalingstjenesteudbyderne oplysning om, fra hvilke internetdomæner der efter Spillemyndighedens opfattelse udbydes ulovlige spilsystemer, eller hvilke konti der efter Spillemyndighedens opfattelse ikke må overføres betaling af indsats til og gevinst fra. Internetudbyderne og betalingstjenesteudbyderne vil normalt ikke have kendskab til, hvilke spiludbydere der er ulovlige, og de har ikke en pligt til løbende at kontrollere, hvorvidt der formidles internetadgang eller betalinger af indsats og gevinst til og fra en spiludbyder, der overtræder dansk lov.

Såfremt en henstilling til en internetudbyder eller en betalingstjenesteudbyder ikke følges, kan Spillemyndigheden søge bestemmelsen håndhævet ved nedlæggelse af forbud i fogedretten efter reglerne i retsplejeloven, jf.

afsnit 2.2. Spillemyndigheden har på nuværende tidspunkt kun haft indledende administrative tiltag i forbindelse med internetblokering og dermed ikke en egentlig administrativ praksis eller domstolspraksis endnu. Blokering af adgang til ulovlige hjemmesider med henvisning til spilleloven er anvendt første gang ultimo maj 2012. Håndteringen af betalingsblokering er under fortsat afklaring.

2.5. Lægemiddelloven – forbud mod transmission

Ved lov nr. 464 af 18. maj 2011 om ændring af lov om lægemidler mv. blev der med en ny § 39 b indført et specifikt forbud for internetudbydere mod at formidle adgang til en hjemmeside, hvorfra der forhandles lægemidler til forbrugerne i strid med lægemiddellovens §§ 7, 39, stk. 1, eller 60, stk. 1. Forbuddet i § 39 b retter sig kun mod de internetudbydere, der har det umiddelbare abonnementsforhold til slutbrugere (kunderne). Sundhedsstyrelsen kan i henhold til den foreslåede ordning rette henvendelse til internetudbyderen i form af en henstilling om at blokere for internetadgangen til hjemmesiden.

Der er en række sagsbehandlingsmæssige forudsætninger for afgivelsen af en henstilling, herunder bl.a. at Sundhedsstyrelsen forinden har forsøgt at bringe de ulovlige aktiviteter til ophør ved at rette henvendelse til hjemmesidens ejer, med mindre dette er vurderet som formålsløst, og at etableringen af en blokering af internetadgangen til hjemmesiden konkret må anses for et proportionalt indgreb. Forbuddet omfatter ikke internetudbyderes adgang til at formidle internetadgang til hjemmesider ejet af forhandlere, som er etableret i Danmark eller et andet EU/EØS-land. Det fremgår af bemærkningerne til loven, at hensigten med forbuddet er at etablere et klart retsgrundlag, på baggrund af hvilket Sundhedsstyrelsen kan indlede en retssag mod en internetudbyder, som overtræder forbuddet.

Sundhedsstyrelsen har oplyst, at fogedretten ved Københavns Byret, den 5. september 2011 afsagde kendelse i den første og hidtil eneste prøvelse vedr. lægemiddellovens § 39 b, stk. 1, og at kendelsen gav Sundhedsstyrelsen medhold i den nedlagte påstand. Justifikationssagen er afsluttet ved dom af 23. april 2012, hvorved Sundhedsstyrelsen ligeledes fik medhold i den afsagte kendelse og blev tilkendt sagens omkostninger, der således skal bæres af internetudbyderne. Fogedrettens kendelse gav Sundhedsstyrelsen (tidl. Lægemiddelstyrelsen) medhold i begæring om fogedforbud mod 7 parter, der som udbydere af elektroniske kommunikationsnet eller -tjenester (internetudbydere) til slutbrugere formidlede adgang til en hjemmeside, der solgte farlige ikke-godkendte lægemidler til danske forbrugere. Endvidere tilpligtede fogedretten, i overensstemmelse med Sundhedsstyrelsens påstand, de 7 internetudbydere at etablere en såkaldt DNS-blokering eller tilsvarende blokering over for den pågældende hjemmeside.

2.6. Børnepornofilteret – frivillig brancheordning

Rigspolitiet har siden 2005 samarbejdet med Red Barnet og størstedelen af internetudbydere i Danmark i bestræbelserne på at forhindre adgang via internettet til børnepornografisk materiale - børnepornofilteret. Børnepornofilteret er baseret på en frivillig aftale mellem internetudbyderne, Red Barnet og Rigspolitiet. Som led i samarbejdet med internetudbyderne videregiver Rigspolitiet løbende på grundlag af konkrete samarbejdsaftaler oplysninger til internetudbyderne om internetadresser, der efter Rigspolitiets vurdering indeholder materiale, som det efter straffelovens § 235 er strafbart at udbrede, besidde eller gennem internettet eller mod vederlag at gøre sig bekendt med. Netfilterordningen er således en ordning, der alene er rettet mod danske internetudbydere med henblik på direkte blokering fra udbyderens side af hjemmesider med børnepornografisk materiale.

Administrationsdelen varetages udviklings- og driftsmæssigt af Rigspolitiets Nationale IT Efterforskningscenter (NITEC)'s IT-afdeling, mens blokeringsarbejdet foretages af afdelingens IT-efterforskere. Blokeringsdelen varetages af de enkelte internetudbydere, som har tilpasset deres systemer til at kunne modtage netfilterets lister over sider, der skal blokeres. Dagligt gennemser efterforskere hos NITEC indholdet på en række hjemmesider. Indholdet vurderes, og det besluttes herefter, om den enkelte side skal blokeres via netfilteret. Hvis det vurderes, at en side skal blokeres, bliver den sat til blokering i netfilterets database. En gang i timen genererer netfilteret automatisk en liste over sider, der pt. står til blokering. En gang i døgnet henter internetudbyderne disse opdaterede lister, og bruger dem til at DNS-blokere for adgangen til siderne. Siden fjernes ikke fra nettet og er således stadig tilgængelig via IP-adressen. En side er som udgangspunkt i netfilteret i et halvt år. Ud fra logfiler genereres statistik om siden, og hvis der ikke har været aktivitet vedrørende hjemmesiden i det halve år, ophæves blokeringen. Efterforskerne kan forlænge blokeringen, ligesom de også kan annullere den i løbet af det halve år.

Der er fire måder, hvorpå NITEC kan modtage hjemmesider til vurdering:

- Når en blokeret side forsøges tilgået, bliver det skrevet i en logfil hos internetudbyderne med information om, hvor brugeren kom fra, da den pågældende forsøgte at få adgang til den blokerede side. Disse logfiler tilsendes NITEC en gang i døgnet. Logfilen er anonym og indeholder ingen data, der kan identificere brugeren, men udelukkende data om, hvilke sider der ledte frem til en i forvejen blokeret side. Disse sider vurderes dernæst.
- Anmeldelser fra borgere.
- Sider dukket op under efterforskning af sager.
- Internationalt politisamarbejde, herunder Interpol og Europol.

I Sverige benyttes DNS-blokering – på samme måde som i Danmark - i forbindelse med bestræbelserne på at forhindre adgang til børnepornogra-

fisk materiale på internettet. Der er tale om en frivillig ordning i et samarbejde mellem politiet (fører en liste over hjemmesider, der udbreder børnepornografisk materiale), Sveriges Post og Telestyrelse (PTS), internetudbyderne (der foretager selve blokeringen af de pågældende hjemmesider), samt ECPAT International (en organisation, der arbejder på bekæmpelse af seksuel udnyttelse af børn).

2.7. Domæner – private forretningsbetingelser

DK Hostmaster A/S er ansvarlig for tildeling og registrering af domænenavne under .dk-domænet i Danmark**.** DK Hostmasters regler for suspension, blokering eller sletning af domænenavne fremgår af DK Hostmaster A/S' forretningsbetingelser afsnit 8.3.

DK Hostmaster har i maj 2012 oplyst, at DK Hostmaster i enkeltstående tilfælde (med undtagelse af tilfælde af typosquatting, som er registrering af domænenavne, hvor der bevidst spekuleres i forvekslingsrisiko med andre domænenavne) har anvendt mulighederne i DK Hostmasters forretningsbestemmelser for at suspendere, blokere og slette domænenavne. For så vidt angår DK Hostmasters suspension og efterfølgende blokering eller sletning af et domænenavn i tilfælde af typosquatting, har DK Hostmaster i 2011 behandlet 256 klager, hvoraf 141 domænenavne er blevet suspenderet med efterfølgende sletning og 41 domænenavne er blevet suspenderet med efterfølgende blokering. Afgørelserne om typosquatting offentliggøres på DK Hostmasters hjemmeside.

DK Hostmaster oplyser, at tilsvarende muligheder for suspension eksisterer og har været anvendt i andre europæiske lande, men at reglerne herfor og anvendelsen heraf varierer i de forskellige lande. I Slovakiet anvendes eksempelvis DNS-blokering til blokering af .sk domæner med retsstridigt materiale. Som udgangspunkt kontakter den relevante myndighed tjenesteudbyderen af det pågældende domæne inden for myndighedens ressortområde for at løse det pågældende forhold uden om det juridiske system. Hvis ikke dette tiltag lykkes, kan myndigheden eller domstolene træffe beslutning om blokering af det pågældende domæne. Blokeringen sker i samarbejde mellem myndigheden (evt. domstolene) og administrator af .sk domænet. Reglerne herfor fremgår bl.a. af administratorens forretningsbetingelser.

2.8. Brevmodeller

I flere europæiske lande anvendes forskellige varianter af såkaldte brevmodeller, hvor der på forskellig vis rettes direkte kontakt til abonnenter, fra hvis internetforbindelse, der er mistanke om overtrædelse af lovgivningen.

Brevmodellen er ikke anvendt i Danmark.

2.8.1. Målrettede informationsbreve vedr. overtrædelser af ophavsretslovgivningen

Udsendelse af informationsbreve kan foregå ved, at der på begæring af en rettighedshaver sendes et antal informationsbreve til en internetabonnent, hvis forbindelse mistænkes for at være anvendt til krænkelse af ophavsretten. Informationsbrevet kan indeholde oplysninger om, at rettighedshaveren har en formodning om, at der er foregået ophavsretskrænkende aktiviteter via den pågældende internetabonnents internetforbindelse (specifik IP-adresse).

Eksempelvis indeholder den britiske Digital Economy Act 2010 en brevmodel, hvorefter det er internetudbyderne, der skal sende meddelelser til internetabonnenter, hvis internettilslutninger anvendes til formodede ulovlige aktiviteter.

2.8.2. "3-strikes"-model

En 3-strikes-model er en brevmodel, hvor der sendes breve til en internetabonnent ved konstatering af en lovovertrædelse fra abonnentens IP-adresse. Til forskel fra fx en målrettet informationsbrevmodel vil fortsat eller gentagen overtrædelse af lovgivningen, eksempelvis ophavsretslovgivningen, kunne medføre en konsekvens for abonnenten, fx lukning af abonnentens internetforbindelse.

Frankrig anvender en 3-strikes-model, der har hjemmel i den franske lov om beskyttelse af intellektuelle ejendomsrettigheder på internettet (HADOPI-loven). I Frankrig er det den særlige myndighed Hadopi (Haute Autorité pour la Diffusion des Oeuvres et la Protection des Droits sur Internet), der udsender e-mails og breve til internetabonnenterne.

I Irland har Irish Recorded Music Association (IRMA) og den irske internetudbyder Eircom, på baggrund af en retssag anlagt af IRMA, indgået forlig om en frivillig procedure efter en 3-strikes-model. Den irske højesteret har vurderet, at den irske model er lovlig.

3. Retshåndhævelse – anvendte tekniske metoder

En teknisk blokering af internetbrugernes adgang til udvalgte servere med et generelt indhold af ulovligt materiale er primært set gennemført ved hjælp af DNS-blokering og IP-adresse-blokering. Disse blokeringsmetoder bliver nærmere beskrevet i det efterfølgende. Beskrivelserne af de tekniske metoder er baseret på beskrivelser i Kulturministeriets rapport fra 2009 fra møderækken om håndhævelse af ophavsretten på internettet og suppleret med korte henvisninger til nyere eksempler fra dansk og europæisk retspraksis.

3.1. DNS-blokering (også kaldet URL-blokering)

En DNS-blokering er den mest enkle form for teknisk blokering, hvis man ønsker at forhindre brugernes adgang til bestemte hjemmesider eller indhold på internettet. Blokeringen sker i internetudbyderens DNS-database (Domain Name Service), som på internettet foretager en nødvendig oversættelse af en given hjemmesides navn (fx www.evm.dk) til en IP-adresse (fx 217.114.86.126). IP-adresser anvendes på internettet til

at identificere, hvor al trafik mellem de forskellige servere og pc'er skal sendes til og kommer fra. Ved DNS-blokering fjernes denne nødvendige oversættelse af et navn til en IP-adresse i en internetudbyders DNS-database, så brugerne hos denne internetudbyder ikke umiddelbart vil være i stand til at kommunikere med den pågældende hjemmeside ved at skrive hjemmesideadressen. Omkostningerne ved at udføre en DNS-blokering er relativt begrænsede, og blokeringen kan forholdsvist nemt omgås af it-brugere.

I de danske sager om blokering for ulovlige hjemmesider med ophavsretligt beskyttet indhold, jf. afsnit 2.2, er der brugt DNS-blokering.

I oktober 2011 blev to belgiske internetudbydere af de belgiske domstole pålagt at blokere for adgang til The Pirate Bay hjemmesiden på DNS niveau.

3.2. IP-adresse-blokering

Ved en IP-adresse-blokering forhindrer man en brugers pc i at kommunikere med en hjemmeside på internettet ved at hindre adgang til selve IP-adressen. Denne type blokering er mere omkostningskrævende at indføre end URL-blokering, og selvom den er mere effektiv, er den også nem at omgå for den it-kyndige.

I en nyere sag (juli 2011) i UK (MPA vs. British Telecom) blev BT pålagt at bruge et såkaldt "Cleanfeed" system, der indebærer en URL- eller IP- blokering ved hjælp af en undersøgelse af visse af "pakkerne" i en transmission (kaldet DPI - Deep Packet Inspection). Metoden kan anvendes til blokering af dele af en hjemmeside eller for én af flere hjemmesider, der deler samme IP-adresse, men hvor ikke alle sider skal blokeres.

I oktober 2011 blev den finske internetudbyder Elisa pålagt at blokere for adgang til The Pirate Bay hjemmesiden på DNS- og IP-niveau.

Fem store internetudbydere i Storbritannien er ved en foreløbig kendelse i februar 2012 blevet pålagt at blokere for The Pirate Bay-tjenesten. Blokeringen er tilsyneladende en kombination af IP- og DNS-blokering.