Rättsliga strategier mot upphovsrättsintrång på nätet - en analys*

Den faktiska efterlevnaden av upphovsrätten är bristande i nätmiljön. I denna artikel undersöker Daniel Westman, doktorand i rättsinformatik vid Stockholms universitet, förutsättningarna för olika rättsliga strategier för att motverka intrång. Vilka förutsättningar har de olika strategierna för att vara såväl effektiva som förenliga med andra grundläggande rättigheter och bevarandet av vad som har kommit att betecknas ett öppet internet?

Bakgrund

På pappret har upphovsrätten aldrig varit starkare än i dag. Anpassningen av upphovsrättslagstiftningen till den digitala miljön har i huvudsak inneburit att ensamrätten har gjorts heltäckande och att användares möjligheter att förfoga över ett verk med stöd av inskränkningar har begränsats. Rättighetshavarnas position har dessutom förstärkts genom ett särskilt rättsligt skydd för s.k. tekniska åtgärder, t.ex. kopieringsspärrar.

Samtidigt är den faktiska efterlevnaden av upphovsrätten bristande i nätmiljön. Verk och andra skyddade prestationer (t.ex. musik, filmer, texter eller datorprogram) kopieras och tillgängliggörs i stor omfattning på ett sätt som strider mot upphovsrätten, t.ex. genom s.k. fildelning peer-to-peer (direkt mellan enskilda användare) eller genom uppladdning på olika centrala lagringstjänster där prestationerna blir tillgängliga för andra användare.

De flesta kan nog vara överens om att denna diskrepans mellan lagstiftningens innehåll och nätanvändarnas faktiska agerande är otillfredsställande och att den åtminstone på längre sikt riskerar att urholka respekten för lagstiftningen i en nätmiljö. I den allmänna debatten om upphovsrättens funktion och framtida utformning, liksom i den rättsvetenskapliga litteraturen, har det emellertid dragits vitt skilda slutsatser om vad som behöver göras.

Något förenklat kan man i dag tala om tre olika upphovsrättsliga diskurser. Dessa kan i varierande grad relateras till den här diskuterade frågan om intrång på nätet.

A. En diskussion har tagit sin utgångspunkt i ensamrättens nuvarande utformning och inriktats mot olika *rättsliga strategier för att motverka intrång på nätet*. De rättsliga förutsättningarna för att identifiera de användare som begår intrången och att hålla dessa straff- eller civilrättsligt ansvariga för sina handlingar samt ansvaret för tillhandahållare av kommunikationstjänster som används vid intrången har därvid hamnat i fokus. Mer konkret har diskussionen rört rätts- och bevisfrågor förknippade med det gällande regelverkets tillämpning i en nätmiljö, men också behovet av att utveckla nya ansvarsregler, nya regler som underlättar insamling av bevis och nya regler om förbud som tar sikte på tillhandahållare av kommunikationstjänster har berörts. Även ”självreglering” och ”frivilliga åtgärder” av kommunikationsleverantörer har diskuterats.

B. En annan diskurs har handlat om själva upphovsrättens utformning och behovet av reformer. Förekomsten av omfattande intrång har i detta sammanhang uppfattats som en, bland flera, signaler om att *balansen i dagens upphovsrätt* inte är den rätta. Kritik som går ut på att den nuvarande ensamrätten inte är legitim eller att den inte har en rationell utformning i förhållande till de ändamål som den avser att befrämja har förts fram. Kortare skyddstider, begränsningar i den grundläggande ensamrätten (”fri fildelning” för icke kommersiellt bruk), fler och mer flexibla inskränkningar i ensamrätten (t.ex. införande av ett fair-use-undantag i europeisk rätt) samt ett ökat fokus på ersättningsrätt i stället för ensamrätt har framhållit som möjliga lösningar på problemet (t.ex. ”fri fildelning” kopplad till en ”bredbandsavgift”). Dessa reformförslag har i praktiken varit mer eller mindre radikala.

** Denna artikel är baserad på ett föredrag som hölls vid Svenska föreningen för upphovsrätts studiedag den 2 december 2011.*

C. En tredje diskurs har handlat om behovet av att förenkla det lagliga tillgängliggörandet av skyddade verk, utan att för den skull ändra ensamrätten i grunden. Det faktum att det finns ett omfattande olagligt

Ny Juridik 2:12 s 35

utnyttjande av skyddat material på nätet uppfattas som en signal om att det finns ett behov av att möta efterfrågan på tillgång till verk med ”lagliga alternativ” i denna miljö. Diskussionen har rört såväl tillgången till kommersiella tjänster, för t.ex. ny musik eller film, som utmaningarna förknippade med de nya möjligheterna att digitalisera och tillgängliggöra det s.k. kulturarvet. Åtgärder som har förordats är t.ex. förändrade licensieringsstrategier hos framför allt producenter (t.ex. vad avser paketering av erbjudandet, prissättning eller strategier med s.k. visningsfönster för nya filmer), behovet av en börs för enkel handel med rättigheter, särskild lagstiftning som underlättar användningen av s.k. föräldralösa verk (t.ex. i samband med digitaliseringen av arkiv) samt en utbyggd kollektiv rättighetsklarering med stöd av s.k. avtalslicenser (dvs. licenser som av lagstiftningen ges en utsträckt verkan till rättighetshavare som inte är medlemmar i den avtalsslutande rättighetshavarorganisationen).

Problemformulering, syfte och avgränsning

Denna artikel handlar om *olika strategier* för att motverka intrång i upphovsrätten (punkt A ovan). Det övergripande syftet är att undersöka förutsättningarna för att de olika strategierna ska kunna vara såväl *effektiva* som förenliga med (andra) *grundläggande rättigheter* (yttrandefriheten, skyddet för den personliga integriteten och rätten till en rättssäker behandling) och bevarandet av vad som har kommit att betecknas *ett öppet internet*. Vad som närmare avses med dessa begrepp kommer att beskrivas i följande avsnitt.

Anledningen till att denna uppläggning valts är att det ska vara möjligt att ta ett helhetsgrepp över sanktionsfrågan i en nätmiljö. Därigenom möjliggörs dels en utvärdering av vilken eller vilka strategier som i första hand bör väljas, dels en övergripande analys av sanktionernas roll och behovet av åtgärder av det slag som diskuteras under punkt B och C ovan.

En avgränsning är att fokus riktas mot ”*piratkopiering*”, dvs. kopiering och tillgängliggörande av hela verk som redan finns tillgängliga på marknaden. Situationer där endast delar av ett verk utnyttjas (t.ex. i bakgrunden till en privat video som läggs upp på nätet) eller situationer där det finns påtagliga yttrandefrihetsintressen förknippade med ett visst tillgängliggörande behandlas inte. De intressen som gör sig gällande i dessa fall är delvis andra, och det är tydligt att lösningar här i huvudsak måste sökas i förenklad rättighetsklarering och eventuellt i

Ny Juridik 2:12 s 36

förändringar i ensamrätten (t.ex. nya inskränkningar eller tvångslicenser).

En bedömning av de rättsliga strategiernas effektivitet och deras förhållande till olika motstående intressen förutsätter tämligen ingående kännedom om *internetmiljöns egenskaper*, t.ex. olika tekniska miljöer där intrång sker. De tekniska förutsättningarna blir många gånger helt avgörande för om en strategi kan bli effektiv och om sanktioner kan utformas på ett proportionerligt sätt. Exempelvis är det vid en utvärdering av olika policyalternativ viktigt att ha kännedom om möjligheterna att säkra bevisning som binder en viss person till ett visst intrång och om möjligheterna att blockera just sådana informationsöverföringar som är intrångsgörande.

Det breda angreppssättet gör att det inte är möjligt att analysera alla de rättsliga frågor som aktualiseras. Innehållet i gällande rätt redovisas endast översiktligt, i syfte att tydliggöra de principiella frågor som är förknippade med respektive strategi. Ambitionen är att framställningen ska ge en *översikt* över ett område som är ytterst komplext, bl.a. eftersom det befinner sig i skärningspunkten mellan juridik, teknik och politik. Därigenom lämnas samtidigt ett litet bidrag till en mer fullständig och strukturerad *analys av policyalternativen* på området.

Översikt över olika rättsliga strategier mot intrång på nätet

En analys av svensk och internationell lagstiftning, rättspraxis och litteratur gör det möjligt att identifiera ett antal olika strategier för att motverka intrång på nätet.

En strategi är att identifiera den *egentlige intrångsgöraren* (typiskt sett den enskilde användare som gör en skyddad prestation tillgänglig för allmänheten i strid med upphovsrätten) och hålla denne ansvarig för intrånget. Detta får anses vara huvudstrategin när intrång sker utanför nätet. Identifiering kan ske inom ramen för en förundersökning och leda fram till en straffrättslig process om brott mot upphovsrättslagen eller med hjälp av de nya civilrättsliga reglerna om informationsföreläggande och leda fram till en utomrättslig uppgörelse eller till en civilrättslig skadestånds- eller förbudsprocess. Om åklagare och rättighetshavare har framgång i de processer som drivs, kan detta antas ha en viss avskräckande effekt.

En annan strategi är att tillämpa straff- och skadeståndsrättsliga *ansvarsregler på sådana tillhandahållare av tjänster som används för att begå*

Ny Juridik 2:12 s 37

intrång eller som underlättar sådana intrång. I de flesta fall handlar det rent rättsligt om att tillämpa allmänna regler om medhjälp till brott. De tjänstetillhandahållare som kan vara aktuella i sammanhanget är t.ex. leverantörer av internetaccess, leverantörer av tjänster som lagrar och tillgängliggör material som användarna sänder in (värdtjänster) och söktjänster och leverantörer av annons- och betaltjänster som mer indirekt underlättar den fortsatta driften av sådana tjänster där det sker direkt eller indirekt upphovsrättsintrång.

Ytterligare en strategi är att utverka ett domstols- eller myndighetsbeslut, t.ex. ett interimistiskt *förbud*, som innebär en skyldighet för en tjänstetillhandahållare att agera på ett sådant sätt att intrång förhindras eller försvåras. Denna strategi är, till skillnad från de två föregående, inriktad på framtida intrång. I teorin är det naturligtvis möjligt att tänka sig förbud riktade mot alla typer av tjänstetillhandahållare, men under senare år har den dominerande strategin i Europa varit att kräva förbud riktade mot leverantörer av internetaccess. I praktiken kan dessa förbud ha olika utformning och effekt. I det följande talas om *avstängning* (skyldighet att upphöra med att leverera access till en intrångsgörare), *blockering* (skyldighet att förhindra att leverantörens kunder från att nå viss adress etc.) och *filtrering* (skyldighet att automatiskt granska information som passerar genom nätet och hindra kommunikation som utgör upphovsrättsintrång från att nå sin mottagare).

De strategier som har diskuterats i det föregående är i princip baserade på en tillämpning av allmänna regler om straff- och skadeståndsansvar och förbud, även om anpassningar, t.ex. när det gäller förutsättningar för bevisinsamling etc., kan behöva göras till de särskilda förutsättningar som råder i en internetmiljö. En fjärde strategi är emellertid att utveckla helt *nya rättsliga ordningar* som tar hänsyn till de särdrag och utmaningar som finns i denna miljö. Till denna kategori kan vi t.ex. hänföra system med varningsbrev, särskilda ordningar för avstängning av abonnemang som använts för intrång och statligt beslutade spärrlistor med domännamn eller IP-adresser som accessleverantörer föreläggs att blockera. Specialanpassad lagstiftning av dessa slag har i viss omfattning införts eller föreslagits i andra länder (Frankrike, UK m.fl.).

En femte strategi, som har en annan karaktär än de tidigare nämnda, är att ”frivilligt” försöka få olika tjänstetillhandahållare att vidta ”*självreglering*” i syfte att förhindra intrång som användare av deras tjänster begår. Denna strategi ligger t.ex. till grund för att de flesta

Ny Juridik 2:12 s 38

större svenska accessleverantörer i dag blockerar kommersiella webbplatser som tillgängliggör barnpornografi. Strategin har emellertid tillämpats också på immaterialrättsområdet. Exempelvis uppmuntrar vissa internationella rättsakter samarbete mellan rättighetshavare och tjänstetillhandahållare. Inriktningen på samarbetet kan i praktiken variera. Det kan t.ex. handla om system för att skicka ut varningsbrev till abonnenter eller om att blockering av vissa webbplatser införs utan särskilt rättsligt stöd och utan rättsliga processer.

Upphovsrättsintrång på nätet - några faktiska utgångspunkter

Intrång i upphovsrätten har alltid förekommit. Varje ny distributionsteknik har emellertid sina speciella egenskaper när det gäller vilka ansträngningar som krävs för att begå intrång och när det gäller förutsättningarna att upptäcka och förhindra intrång. Risken för att olaglig distribution i betydande grad ersätter den lagliga marknaden är därmed mer eller mindre påtaglig i olika tekniska miljöer. En analys av olika strategier mot intrång på nätet kräver därför närmare kännedom om vissa faktiska förhållanden.

Den digitala miljön kännetecknas av att all kommunikation - även sådan som innebär ett upphovsrättsintrång - kan ske *enkelt* och med *hög kvalitet*. De negativa egenskaperna hos en fysisk piratkopia saknas typiskt sett i denna miljö. Lättillgänglig programvara och användning av *generella kommunikationstjänster* gör att intrångsgörande material alltid finns nära till hands, samtidigt som det i många fall är svårt att ingripa mot intrången med precision *och* effektivitet. Nätets *öppenhet och gränslöshet*, kombinerat med de kraftfulla *sökmöjligheterna* gör att ett otillåtet tillgängliggörande av skyddade prestationer någonstans i världen enkelt kan utnyttjas av en användare här i landet.

En effektiv distribution av fysiska piratkopior kräver tämligen omfattande investeringar, samtidigt som upptäcktsrisken inte är obetydlig. Intrång i en internetmiljö är i många fall - men inte alla - användardrivna och i stor utsträckning *decentraliserade*. Ofta sker delar av den kommunikation som leder fram till intrånget i sådana slutna kommunikationskanaler där användaren har ett rättsligt befogat anspråk på ett starkt integritetsskydd. Många gånger är det även av andra skäl svårt att säkra tillräcklig bevisning om vem som ligger bakom ett visst intrång. Detta beror i sin tur t.ex. på möjligheterna att enkelt ansluta sig till

olika delar av nätet och på att loggar över kommunikation inte alltid är åtkomliga när ett intrång ska utredas.

Användares *drivkraft* för att begå intrång i en internetmiljö är sällan att de ska få en direkt ekonomisk ersättning. Detta förhållande påverkar rättsliga bedömningar om t.ex. proportionalitet och straffvärde. De intrång som varje enskild användare begår är många gånger relativt begränsade, men sammantaget kan många sådana intrång påverka marknaden på ett genomgripande sätt.

Mer konkret finns det i dag ett antal *olika tillvägagångssätt* som i stor skala används för upphovsrättsintrång på nätet. Då förutsättningarna för att en viss rättslig strategi mot intrång ska vara effektiv och samtidigt rättsligt godtagbar skiljer sig mellan dessa tillvägagångssätt finns det anledning att helt kort beskriva deras särdrag.

1. Många intrång sker genom att användare utnyttjar olika typer av allmänt tillgängliga *lagringstjänster* (värdtjänster) för uppladdning av material som blir tillgängligt för andra användare. Typiskt sett är det fråga om generella kommunikationstjänster utan förhandsgranskning, som kan användas för alla typer av datafiler eller för alla filer av en viss typ, t.ex. film- eller ljudfiler. Exempel på lagringstjänster är tillhandahållande av en s.k. FTP-server eller mer moderna tjänster som Facebook, YouTube, Dropbox eller Flickr. I vissa fall är innehållet som laddas upp allmänt tillgängligt och sökbart via tjänsten. I andra fall är åtkomsten begränsad, t.ex. till den som har tillgång till en unik direktlänk till varje fil. Den senare konstruktionen är vanlig när det gäller s.k. cyberlockers och innebär normalt att den som laddar upp en fil får tillgång till länken, som sedan kan spridas t.ex. via e-post eller i ett diskussionsforum. Ibland handlar det om tjänster där den illegala användningen dominerar helt, men många gånger förekommer det en blandning av lagligt och intrångsgörande material i tjänsterna. Ofta är det möjligt att använda dessa lagringstjänster utan att behöva styrka sin identitet.
2. Intrång på nätet kan även ske genom *fildelning peer-to-peer,* dvs. kopiering och tillgängliggörande av filer direkt mellan enskilda användares datorer. Fildelningstekniken har i stor utsträckning förknippats med just upphovsrättsintrång, men den har flera tekniska egenskaper som göra att den också används för vissa typer av laglig distribution, även om den olagliga dominerar. Det finns olika generationer av fildelningsteknik och deras egenskaper variera i viss utsträckning. Utvecklingen startade med tjänsten Napster, och i dag dominerar BitTorrent-protokollet (som bl.a. används vid fildelning med hjälp av tjänsten The Pirate Bay). Drivkraften för att utveckla nya kommunikationsprotokoll och programvaror har inte

Ny Juridik 2:12 s 40

sällan varit att göra systemen mindre sårbara mot rättsliga strategier för att förhindra intrång. Många fildelningsnätverk försöker på olika sätt motverka att användare tar del av material utan att samtidigt göra något tillgängligt för andra användare. BitTorrent-program är t.ex. normalt konfigurerade så att en användare som laddar ner en viss fil samtidigt gör (delar av) denna fil tillgänglig för andra användare i nätverket. Även om tillgängliggörandet respektive nedladdningen av filer sker direkt mellan enskilda användare innehåller de flesta fildelningsnätverk någon form av central tjänst för sökning av filer och för sammankoppling av användare (index, trackers, hubbar etc.). Dessa tjänster kan vara öppet tillgängliga eller lösenordskyddade och därmed bara tillgängliga för vissa användare. Möjligheterna för någon som har tillgång till en sådan sök- eller sammankopplingstjänst, t.ex. en rättighetshavare eller polisen, att säkra bevisning om vem som gör vad i ett fildelningsnätverk varierar mellan de olika generationerna av fildelningsnätverk (i vart fall om användarna tilldelas sin IP-adress dynamiskt av sin internetleverantör). Exempelvis varierar möjligheterna att bevisa hur omfattande ett intrång är (t.ex. hur många filer som görs tillgängliga av en och samma användare) och hur många som har fått access till de tillgängliggjorda filerna. Eftersom dessa förhållanden är avgörande för hur allvarligt intrånget anses vara inverkar möjligheterna att i ett tidigt skede säkra bevisning om intrången även på vilka processuella utredningsåtgärder som rättighetshavare eller rättsvårdande myndigheter i ett senare stadium kan få använda sig av t.ex. för att identifiera den misstänkte intrångsgöraren eller för att säkra bevisning i dennes bostad (se nedan).

3. De senaste åren har intrång i viss omfattning skett genom tjänster placerade i länder utan upphovsrättsliga regler eller utan fungerande sanktioner mot intrång. Det handlar om rena pirattjänster som drivs kommer siellt och som inriktas mot användare i t.ex. Europa eller USA. Det intrångsgörande materialet tillhandahåll inte av användarna, utan av den som driver tjänsten genom nedladdning eller s.k. *streaming* (möjlighet att, som vid en vanlig radio- eller tv-sändning, lyssna eller titta utan framställning av permanenta kopior). När det gäller streaming är det tvek samt om svenska användare av dessa tjänster över huvud taget begår något intrång, men även om så är fallet är det i princip omöjligt att här i landet identifiera användarna utan att systematiskt avlyssna internettrafiken.

Sett över den senaste femtonårsperioden har fildelning peer-to-peer varit det dominerande tillvägagångssättet för intrång på nätet och därmed det fenomen som tilldragit sig mest intresse. Lagringstjänster har

Ny Juridik 2:12 s 41

använts för intrång långt innan internet slog igenom, då t.ex. i form av telefonuppkopplade s.k. BBS:er (Bulletin Board System). Denna form av intrång har på senare år fått en renässans, inte minst på grund av att tjänstetillhandahållarna i många fall har ansetts skyddade mot medverkansansvar, samtidigt som de rättsliga riskerna för användare som ägnar sig åt fildelning har ansetts öka. Piratstreaming och liknande centraliserade distributionstjänster förutsätter en relativt god bandbredd och har blivit populära först på senare år. En förklaring är också att de rättsliga riskerna för användarna med detta tillvägagångssätt är begränsade.

I *framtiden* kommer det finnas nya tekniska lösningar för kommunikation, vilka naturligtvis också kan användas för att begå upphovsrättsintrång. Det är t.ex. möjligt att tänka sig en utveckling mot att kommunikation i större utsträckning krypteras och därmed blir svårare att identifiera som otillåten och svårare att knyta till en viss person. Redan i dag finns det dessutom teknik för mer decentraliserad fildelning som inte kräver särskilda knutpunkter i form av trackers, hubbar etc. (vilka har visat sig sårbara för rättsliga åtgärder). Då det från rättsliga och policymässiga utgångspunkter knappast framstår som acceptabelt att förbjuda användningen av dessa tekniker helt tyder mycket på att den avgörande frågan blir hur starka drivkrafter användarna kommer att ha att ta dem i bruk för att begå upphovsrättsintrång.

Vissa av de faktiska förhållanden som har behandlats i detta avsnitt är konsekvenser av *datorteknikens grundläggande funktionssätt* och är därmed mycket svåra att påverka. Det gäller t.ex. möjligheterna att enkelt och billigt kopiera information. Möjligtvis kan en utveckling mot mer låst hårdvara (jfr t.ex. Apples kontroll över vilka program som en användare kan installera på företagets läsplattor och telefoner) i någon omfattning göra dessa egenskaper mindre påtagliga hos en normalanvändare.

Andra egenskaper kan hänföras till de *tidiga designval* som gjordes när internet skapades. Det gäller t.ex. det förhållandet att nätet är decentraliserat och bygger på den s.k. end-to-end-modellen (dvs. att själva nätverket är öppet för all typ av kommunikation som baserar sig på det s.k. TCP/IP-protokollet och att ”makten” över vad som kommuniceras - och hur - ligger hos användarna). Även den bristande spårbarheten kan hänföras till denna kategori. En förändring av denna grundläggande design är naturligtvis möjlig, men det kräver i princip internationellt samförstånd och att de privata kommunikationsoperatörer som tillsammans skapar internet är beredda att genomföra en

Ny Juridik 2:12 s 42

förändring. Eftersom många viktiga aktörer med inflytande över nätet anser att dessa designval är värda att slå vakt om (jfr nedan om ”öppet internet”) finns det ett relativt starkt motstånd mot sådana förändringar.

Ytterligare andra tekniska förhållanden skulle *enklare kunna påverkas*, t.ex. genom politiska beslut. Men det handlar i dessa fall om sådana egenskaper som inte kommer att ha en avgörande inverkan på intrångsmöjligheterna, eftersom det i huvudsak inte handlar om så grundläggande tekniska förhållanden.

Kriterier för utvärdering av strategierna

I detta arbete utvärderas de olika strategiernas effektivitet och deras förenlighet med andra grundläggande rättigheter än upphovsrätten (yttrandefriheten, skyddet för den personliga integriteten och rättssäkerheten) samt strävan efter ett ”öppet internet”.

Effektivitet utgör ett naturligt utvärderingskriterium. Internationella konventioner och EU-rättsliga förpliktelser kräver att det ska finnas effektiva sanktioner. Omvänt är en strategi mot intrång som inte är effektiv av begränsat praktiskt intresse för såväl rättighetshavare som samhället i övrigt.

Effektivitet kan mätas på olika sätt och effektiviteten hos en viss rättslig reglering är inte sällan svårbedömd - särskilt på förhand. Strategier kan vara effektiva på lång eller kort sikt. Därtill kan läggas att de här analyserade strategierna har olika verkningssätt. Några avser att vara preventiva och antagandet är att den aktuella strategin på lång sikt ska främja respekten för ensamrätten (t.ex. strategin att hålla den egentliga intrångsgöraren ansvarig). Andra strävar efter att rent tekniskt hindra att intrång äger rum (t.ex. strategin med krav på avstängning, blockering och filtrering). Ytterligare andra strävar efter att bl.a. utbilda nätanvändarna (t.ex. strategin med varningsbrev). För att en strategi mot intrång som avser att verka preventivt långsiktigt ska vara effektiv krävs t.ex. att det är möjligt att säkra *bevisning* som gör det möjligt att i normalfallet vinna en civil- eller straffrättslig process mot en misstänkt intrångsgörare. På motsvararande sätt kräver en strategi vars syfte är att tekniskt förhindra eller försvåra intrång att de åtgärder som vidtas inte enkelt kan *kringgås* av användarna. Förutsättningarna i dessa hänseenden kommer att undersökas i följande avsnitt.

En strategi för att bekämpa brott eller civilrättsliga intrång behöver naturligtvis inte vara *helt* effektiv för att framstå som rättspolitiskt attraktiv.

Ny Juridik 2:12 s 43

Hur kostsam strategin är, vilka alternativ som finns (i form av andra strategier mot intrång eller andra upphovsrättsliga reformer) och hur väl strategin kan förenas med andra tungt vägande intressen påverkar givetvis bedömningen. Om en viss strategi anses ha en begränsad effektivitet påverkar detta t.ex. möjligheten att uppfatta eventuella begränsningar i yttrandefriheten och skyddet för den personliga integriteten som strategin medför som nödvändiga och proportionerliga. De faktiska förhållandena i en viss miljö måste sålunda i betydande utsträckning påverka vilken effektivitetsgrad som kan krävas.

I en nätmiljö är det ofta enkelt för en tekniskt kunnig användare att skriva en instruktion, skapa ett program eller utveckla en tjänst som kan användas för att göra en viss strategi mindre effektiv. Det kan t.ex. handla om att skapa en decentraliserad anonymiseringstjänst eller om att skriva ner en instruktion för hur av blockering av visst slag kan kringgås. Internets öppenhet och de låga distributionskostnaderna gör det sedan enkelt att sprida dessa lösningar till mindre kunniga användare. Detta förhållande påverkar på ett avgörande sätt flera av de här diskuterade strategiernas effektivitet. Alla användare kommer naturligtvis inte att använda dessa instruktioner, program eller tjänster, men om drivkraften att komma åt

visst material eller undgå identifiering finns blir det i många fall enkelt att göra det. Därmed blir det, något tillspetsat, drivkraften i användarkollektivet, och inte strategin i sig som avgör effektiviteten.

Flera strategier kräver *internationellt rättsligt samarbete* för att bli effektiva. Framför allt gäller detta strategin att hålla den egentliga intrångsgöraren ansvarig. Bristen på ett etablerat internationellt samarbete bidrar till att strategier som inriktar sig på att begränsa själva åtkomsten till intrångsgörande filer i det land där marknaden påverkas av intrånget (blockering och filtrering) policymässigt kan framstå som mer attraktiva.

För att vara godtagbara i ett demokratiskt samhälle måste strategier mot upphovsrättsintrång vara förenliga med vissa (andra) *grundläggande rättigheter* (enligt grundlagarna, Europakonventionen etc.).

Typiskt sett hanteras spänningar mellan *yttrandefrihet* och upphovsrätt inom upphovsrättslagstiftning, t.ex. genom regler om citat, nyhetsrapportering och parodier, men i atypiska situationer kan en domstol tillämpa en extern kontroll av upphovsrättens funktion genom att konstatera att en tillämpning av upphovsrättsliga regler skulle innebära en oproportionerlig begränsning av yttrandefriheten. Eftersom denna

Ny Juridik 2:12 s 44

undersökning är inriktad på strategier mot ren ”piratkopiering” diskuteras inte frågor av detta slag närmare.

Strategier med en sådan inriktning aktualiserar emellertid även and ra element i skyddet för yttrandefriheten. Rättsliga krav på avstängning, blockering eller filtrering för att förhindra spridning av visst innehåll kan t.ex. i många fall utgöra sådana *hindrande åtgärder* eller begränsningar av mottagarens *informationsfrihet* (frihet att ta emot material som har gjorts tillgängligt av andra) som är tillåtna endast under speciella omständigheter. Vidare kan proportionaliteten i beslut om sådana åtgärder ofta ifrågasättas eftersom inte bara intrångsgörande utan även *laglig kommunikation* i praktiken stoppas. *Avstängning* av enskilda användare från internet (som en sanktion för upphovsrättsintrång) har i flera sammanhang inte bedömts vara en rimlig och proportionerlig begränsning i yttrande- och informationsfriheten i den uppkopplade tid som vi lever i.

Regler om *mellanhänders straff- och skadeståndsansvar* kan, beroende på den närmare utformningen, aktualisera vissa yttrandefrihetsrättsliga frågeställningar. Att en stat utformar ansvarsregler på ett sätt som innebär att mellanhänderna ges bristande incitament att motsätta sig krav på t.ex. borttagning av visst material, trots att detta kanske är lagligt och att den som distribuerat materialet önskar en rättslig prövning, kan t.ex. framstå som problematiskt. En svårighet i detta sammanhang är att mellanhänder, t.ex. tillhandahållare av lagringstjänster, kan ha svårt att med säkerhet bedöma när ett intrång föreligger. Det kan både handla om osäkerhet beträffande faktiska förhållanden (kännedom om att en viss fil har lagts upp på tjänsten eller om rättighetshavaren har samtyckt till detta) och om bristande kompetensen att göra upphovsrättsliga bedömningar. Om t.ex. regler om medhjälp till brott trots detta ges en långtgående tillämpning kan det göra att mellanhänderna i syfte att minska sin riskexponering begränsar även lagligt tillgängliggörande.

En annan grundläggande rättighet som de olika strategierna mot intrång aktualiserar är *skyddet för den personliga integriteten*. Flera strategier förutsätter en tämligen omfattande behandling av personuppgifter. För att det ska vara möjligt att identifiera en intrångsgörare krävs t.ex. att rättighetshavare får *samla in och lagra personuppgifter* i form av t.ex. IP-adresser, från vilka intrångsgörande material har gjorts tillgängligt. I sammanhanget kan det noteras att privata aktörers behandling av uppgifter om lagöverträdelser behandlas särskilt restriktivt i personuppgiftslagstiftningen.

Ny Juridik 2:12 s 45

För att mer effektiv identifiering av intrångsgörare ska vara möjlig krävs det antagligen olika tjänstetillhandahållare, t.ex. tillhandahållare av lagringstjänster eller accessleverantörer, åläggs att *identifiera sina användare och att lagra information om deras användning av tjänsten*. Det är i många fall tveksamt om rättsliga krav på omfattande datalagring för att motverka upphovsrättsintrång kan förenas skyddet för den personliga integriteten. Det kan dock inte uteslutas att en identifierings- och datalagringsskyldighet skulle ses som proportionerlig när det gäller vissa bestämda typer av tjänster. Även tjänstetillhandahållares

rättigheter och skyldigheter att *lämna ut* de lagrade uppgifterna för utredning av upphovsrättsintrång aktualiserar integritetsrättsliga överväganden.

Rättsliga krav på *filtrering* av internettrafik i syfte att stoppa överföring av upphovsrättsligt skyddat material aktualiserar också integritetsrättsliga överväganden. Ingripanden av detta slag bör normalt betraktas som en form av avlyssning, eftersom privat datatrafik (visserligen automatiskt) granskas i syfte att identifiera (och stoppa) visst innehåll. Ett sådant ingrepp i skyddet för post- och telehemligheten i syfte att förhindra upphovsrättsintrång torde sällan kunna anses vara proportionerligt.

Strategierna måste även vara *rättssäkra* för alla inblandade aktörer, dvs. internetanvändare, rättighetshavare och tjänstetillhandahållare. Sanktionsregler måste bygga på en *oskuldspresumtion*, vilket t.ex. innebär att regler om strikt ansvar för en innehavare av ett internetabonnemang kan ifrågasättas. Processer som leder fram till ett ingripande beslut måste även i övrigt uppfylla de krav som följer av *rätten till en rättvis rättegång*, t.ex. rätt till domstolsprövning i brottmål eller mål som rör ingrepp i civila rättigheter. Det innebär bl.a. att summarisk masshantering av intrångsärenden inte kan införas i effektivitetens intresse och att normala beviskrav måste tillämpas även beträffande misstänkta intrång på nätet. Kraven på en rättvis rättegång torde även styra utformningen av regler om mellanhänders ställning, framför allt i relation till en enskild användares rätt att få sitt yttrande prövat på ett godtagbart sätt.

Detta arbete syftar inte till att fastställa de exakta gränserna för det skydd som de grundläggande rättigheterna (enligt t.ex. Europakonventionen, regeringsformen eller yttrandefrihetsgrundlagen) erbjuder i en nätmiljö. Det ovan sagda innebär emellertid att det är möjligt att göra en övergripande bedömning av förhållandet mellan dessa rättigheter

Ny Juridik 2:12 s 46

och strävan efter effektivitet vid utformningen av strategier mot intrång i denna miljö.

Vid sidan av de här behandlade grundläggande rättigheterna har strategier mot intrång på nätet också kommit att ställas mot värdet av ett ”*öppet internet*”. Innebörden av detta begrepp låter sig inte enkelt definieras och det är uppenbart att olika personer använder uttrycket med delvis olika betydelser. I kärnområdet ligger emellertid - som framhållits ovan - en positiv syn på de designval som har format internets grundläggande tekniska arkitektur. Att slå vakt om ett öppet internet innebär t.ex. värnande av en decentraliserad kommunikationsstruktur och den s.k. end-to-end-modellen. I synsättet ligger även en skepsis mot att lösa ”innehålls- eller tjänsterelaterade problem”, t.ex. spridning av oönskat innehåll eller användning av oönskade tjänster, genom tekniska begränsningar på den grundläggande kommunikationsnivån. Det framhålls t.ex. att förändringar i domännamnssystemet (DNS) i syfte att försöka blockera åtkomsten till en viss utrustning eller ett visst innehåll riskerar att få allvarliga bieffekter på nätets funktion eller att skada förtroendet för nätet som kommunikationsplattform.

Det synsätt på internet som beskrivits här kan också sägas ligga till grund för de rättspolitiska kraven på *nätneutralitet,* dvs. krav på att nätoperatörer inte utan sakliga skäl ska få behandla trafik i deras nät på skilda sätt, t.ex. diskriminera beroende på mottagare eller innehåll. En operatör av accesstjänster eller överföringstjänster på nätet uppfattas i båda dessa sammanhang som en neutral aktör som på ett lojalt sätt ska vidareförmedla användarnas kommunikation.

Utöver det sagda menar vissa debattörer att kravet på ett öppet internet innefattar krav på att kunna kommunicera *krypterat* och utan att behöva vara identifierad. De praktiska möjligheterna att kommunicera på detta sätt i dag följer av att användarna kan använda vilken programvara de önskar (t.ex. krypteringsprogramvara) och skicka vilken typ av trafik som helst genom näten (t.ex. krypterad trafik). Ett anspråk att få kommunicera krypterat etc. torde dock inte ta sikte på vilka åtgärder t.ex. rättsvårdande myndigheter får vidta i syfte att identifiera en misstänkt person. Krav på ett öppet internet kan inte heller anses omfatta anspråk på total frihet att kommunicera vilken information som helst utan rättsligt ansvar.

Kraven på att internets öppenhet ska värnas kom tidigare mest från den tekniska världen och avsåg i huvudsak att slå vakt om nätets tekniska fördelar. På senare tid har värdet av ett öppet internet även

Ny Juridik 2:12 s 47

betonats i politiska sammanhang. Det är inte ovanligt att det i sådana sammanhang hänvisas både till de ovan behandlade grundläggande rättigheterna och ett öppet internet under rubriken (”friheten på nätet”).

Identifiering av och ansvar för den egentliga intrångsgöraren

En naturlig utgångpunkt är att åtgärder för att motverka upphovsrättsintrång även i en nätmiljö i första hand bör inriktas mot den egentliga intrångsgöraren. I praktiken handlar det främst om personer som gör skyddade verk *tillgängliga för allmänheten* i strid med ensamrätten, t.ex. den enskilde fildelaren, den som laddar upp ett verk på en lagringstjänst där det är tillgänglig för allmänheten eller den som tillhandahåller en streamingtjänst eller nedladdningstjänst med material som han eller hon själv har låtit föra in i tjänsten. Den som endast tillhandahåller en tjänst som möjliggör kommunikation, t.ex. lagringstjänster eller sök- och indexeringstjänster som möjliggör fildelning, anses normalt inte därigenom själv göra de verk som användarna för in tjänsten tillgängliga för allmänheten. Däremot kan en tjänstetillhandahållare, som diskuteras närmare i följande avsnitt, i vissa fall anses medverka till användarnas intrång på ett otillåtet sätt.

Frågor om tillgång till *bevisning* och vilka beviskrav som ska tillämpas hamnar i fokus när denna strategis effektivitet utvärderas. Därutöver kräv att de sanktioner (straff eller skadestånd) som tillämpas har en *avskräckande effekt* på andra potentiella intrångsgörare. När det handlar om att motverka intrång i de breda användargrupperna torde risken för att över huvud taget bli föremål för en rättslig process normalt vara tillräckligt. För att få t.ex. mer ideologiskt drivna intrångsgörare eller personer med ett ekonomiskt syfte att avstå från intrång torde det krävas en mer påtaglig upptäcktsrisk och mer kraftfulla sanktioner.

Såväl faktiska förhållanden som rättsregler påverkar möjligheterna att säkra den bevisning som krävs för att strategin ska vara framgångsrik. Förutsättningarna för bevisinsamling varierar i viss grad beroende på miljön för intrånget (lagringtjänst, fildelningsnätverk etc.). Vilken styrka som krävs på bevisningen bestäms av om det är fråga om en civilrättslig eller en straffrättslig process. I en straffrättslig process måste åklagaren av rättssäkerhetsskäl visa att det är ställt utom allt rimligt tvivel att den åtalade har begått den brottsliga handlingen. I en civilrättslig process tillämpas det lägre beviskravet att intrånget är styrkt.

Ny Juridik 2:12 s 48

För att en person ska kunna bindas vid ett otillåtet tillgängliggörande i ett fildelningsnätverk krävs i princip bevisning i tre steg.

För det första måste rättighetshavaren i fildelningsnätverket säkra bevisning om att hans eller hennes skyddade verk vid en viss tidpunkt har funnits tillgängligt för en krets som utgör allmänheten och kunnat laddas ner från en viss IP-adress. I princip måste den tillgängliggjorda filens faktiska innehåll kontrolleras och dokumenteras.

För det andra måste den IP-adress som används vid tillgängliggörande kunna kopplas till en viss identifierbar internetabonnent. Då många internetabonnenter inte har tillgång till en statisk IP-adress, utan dynamiskt tilldelas en adress av sin accessleverantör i samband med att de ansluter sig till internet förutsätter insamling av sådan bevisning dels att accessleverantören har en logg över tilldelningen av IP-adresser, dels att leverantören har en rättslig skyldighet att lämna ut uppgiften om abonnemangsinnehavaren till rättsvårdande myndigheter och - om en civilrättslig process om intrånget ska vara möjlig - direkt till rättighetsinnehavare. Slutligen krävs att abonnemangsinnehavaren är identifierad, dvs. att det inte handlar om t.ex. ett anonymt kontantkort.

För det tredje krävs det normalt någon form av bevisning som knyter intrånget till den person som har åtalats eller stämts i en civilrättslig process. Det är inte givet att den som är abonnent har utfört eller ens känner till det aktuella intrånget. Flera personer i ett hushåll kan t.ex. ofta använda ett och samma abonnemang. Abonnenten kan även ha valt att låta utomstående personer använda uppkopplingen, t.ex. genom att tillhandahålla ett trådlöst nätverk, till vilket andra personer har kunnat ansluta.

Den svenska regleringen på området innebär i korthet följande: Uppgifter om misstänkta intrångsgörares IP-adresser får, med vissa begränsningar, samlas in och användas av rättighetshavarna (se 53 g § upphovsrättslagen samt personuppgiftslagen). Leverantörer av internetaccess är enligt de regler som genomför

EU:s datalagringsdirektiv skyldiga att lagra uppgifter bl.a. om vilken abonnent som vid en viss tidpunkt tilldelats en viss IP-adress (6 kap. 16 a § lagen om elektronisk kommunikation). Dessa uppgifter kan från och med den 1 juli 2012 begäras ut av polis och åklagare vid misstanke om brott, oavsett vilken påföljd som brottet bedöms kunna leda till i det enskilda fallet (6 kap. 22 § första stycket punkt 2). Däremot kan sådana tvångslagrade uppgifter inte lämnas ut direkt till en rättighetshavare så att denne t.ex. kan

Ny Juridik 2:12 s 49

skicka varningsbrev eller inleda en civilrättslig process. Har accessleverantören emellertid frivilligt lagrat uppgifterna om tilldelad IP-adress även för interna ändamål, t.ex. säkerhetsändamål (vilket torde vara vanligt) kan en domstol, efter begäran från en rättighetshavare som visat sannolika skäl för att ett intrång har begåtts, genom ett s.k. informationsföreläggande, besluta om att uppgifterna ska lämnas ut till rättighetshavaren (53 c § upphovsrättslagen). EU-domstolen har funnit att en sådan ordning innebär en korrekt avvägning mellan intresset av effektiva sanktioner och intresset av att skydda internetanvändares personuppgifter. Ett krav är emellertid att den nationella domstolen ska göra en avvägning mellan de olika intressena som aktualiseras innan den beslutar om utlämnandet (C-461/10, jfr även C-275/06). Enligt de svenska förarbetena till bestämmelserna ska ett informationsföreläggande i princip kunna utfärdas även om bevisning bara presenteras om otillåtet tillgängliggörande av *ett* verk. Huruvida den av EU-domstolen anvisade proportionalitetsbedömningen också måste utfalla på samma sätt är oklart.

För att en viss fysisk person ska kunna hållas ansvarig för intrånget (steg 3) krävs i ett straffrättsligt mål typiskt sett en undersökning av användarens utrustning eller annan bevisning som visar att det är ställt utom allt rimligt tvivel att det är den tilltalade som är gärningsmannen. För att en undersökning av användarens utrustning ska kunna genomföras krävs i praktiken en husrannsakan. Grundläggande krav på proportionalitet innebär emellertid att husrannsakan normalt inte kan ske vid misstanke om brott som endast antas kunna leda till böter. Samtidigt visar underrättspraxis att straffvärdet för tillgängliggörande genom fildelning av upp till ett antal tiotal verk i icke kommersiellt syfte normalt är dagsböter. Det är när fildelning sker med hjälp av BitTorrent-tekniken dessutom svårt att styrka att ett och samma abonnemang har varit inblandat i ett mer omfattande tillgängliggörande, även om så kanske faktiskt är fallet. Sålunda är det när det gäller fildelning i denna miljö många gånger svårt att säkra tillräckligt med bevisning för att det ska vara möjligt att vinna ett straffrättsligt mål mot en abonnent som nekar och som påstår att andra har kunnat använda abonnemanget.

Vilken bevisning som krävs för att en civilrättslig intrångstalan ska anses vara styrkt är mer osäkert. Vägledande svensk praxis saknas, men i vissa andra länder, t.ex. Danmark, har en spårning till ett visst abonnemang inte ansetts vara tillräckligt för att abonnemangsinnehavaren ska kunna åläggas skadeståndsrättsligt ansvar för intrånget. I dessa fall

Ny Juridik 2:12 s 50

har det ofta handlat om att svarande har påstått sig ha ett öppet trådlöst nätverk, något som inte har kunnat motbevisas. En möjlighet att få tillstånd en civilrättslig s.k. intrångsundersökning för att säkra bevisning om abonnentens utrustning torde bara finnas i vissa speciella fall. I Frankrike har abonnenter i lag i stället ålagts ett visst ansvar för de handlingar som utförs med hjälp av deras uppkoppling. Endast genom att använda en av staten särskilt anvisad teknisk lösning för att skydda sin uppkoppling mot obehörigt utnyttjande kan abonnenten undgå detta ansvar. En sådan ordning stärker naturligtvis strategins effektivitet, med det kan diskuteras om den uppfyller kraven på rättssäkerhet och om ett strikt ansvar av detta slag verkligen är rättspolitiskt önskvärt, t.ex. blir det i praktiken mycket riskabelt att erbjuda andra användare tillgång till internetanslutningen genom ett öppet trådlöst nätverk.

I dag finns det i svensk rätt inte något förbud mot att tillhanda kommunikationstjänster till användare som inte är identifierade. Det är t.ex. möjligt att använda s.k. *kontantkort* för att ansluta till nätet. På senare tid har det också blivit vanligare att svenska nätanvändare utnyttjar s.k. *anonymiseringstjänster*. Dessa tjänster innebär att användaren får en IP-adress av en tjänsteleverantör, som sedan typiskt sett inte lagrar någon information om vem som har använt tjänsten. Det är ännu så länge osäkert om en fristående anonymiseringstjänst (dvs. en tjänst som tillhandahålls av någon annan än den som tillhandahåller själva internetaccessen) omfattas av den nya datalagringsskyldigheten. Leverantörer av anonymiseringstjänster kan under alla förhållanden enkelt etablera sig i länder där de inte omfattas av en eventuell europeisk datalagringsskyldighet och där de inte kan tvingas att lämna ut uppgifter till ett svenskt rättssubjekt.

Den kortfattade beskrivningen av faktiska förhållanden och den rättsliga regleringen på området visar att det finns vissa brister i den här diskuterade strategins *effektivitet,* åtminstone när det gäller intrång som sker genom fildelning i moderna fildelningsnätverk. Intrångsgörare med starka drivkrafter att fortsätta med sin verksamhet kan antas vara svåra att lagföra och avskräcka så länge inte anonymiseringstjänster förbjuds och effektivt blockeras av svenska accessleverantörer och så länge som en abonnent inte åläggs något form av presumtionsansvar för de handlingar som utförs med hjälp av hans eller hennes abonnemang. En sådan lagstiftning kan emellertid ifrågasättas, bl.a. i ett integritets- och rättssäkerhetsperspektiv. I relation till nätanvändare som inte har

Ny Juridik 2:12 s 51

en lika tydlig drivkraft att begå intrång kan strategin troligen vara mer effektiv. I denna grupp kan redan risken för att kallas till polisförhör med anledning av ett misstänkt intrång ha en viss avskräckande effekt. Om strategin kombineras med åtgärder för att minska drivkraften att begå intrång har den potential att bli framgångsrik i bredare användargrupper och därmed tillräckligt effektiv att skydda en legal marknad. Även en användning av varningsbrev (se nedan) kan utgöra ett inslag i en sådan strategi.

När intrång sker genom uppladdning till en allmänt tillgänglig *lagringstjänst* är ett effektivitetsproblem ofta att användarna inte är identifierade för andra som använder tjänsten. Lagringstjänster omfattas inte heller av datalagringsskyldigheten, så någon absolut skyldighet att lagra uppgifter om t.ex. IP-nummer finns inte. Därtill kommer att många populära lagringstjänster är etablerade i andra länder och därmed mindre benägna att tillmötesgå en begäran om information som kommer från ett svenskt rättssubjekt. I vissa fall är det ändå - t.ex. med hjälp av annan information - möjligt att identifiera den som tillgängliggjort ett verk i dessa tjänster. Men för att en strategi som inriktar sig mot den egentliga intrångsgöraren ska vara effektiv i denna tekniska miljö krävs troligen utökade skyldigheter för tillhandahållaren av lagringstjänsten att logga uppgift om användarnas IP-nummer m.m. En sådan skyldighet skulle eventuellt kunna kopplas till förutsättningarna för att leverantören själv ska vara ansvarsfri (se nästa avsnitt).

När det gäller utländska *pirattjänster för streaming eller nedladdning* är det största problemet inte identifieringen (som t.ex. ofta skulle kunna ske genom spårning av betalningar etc.) utan bristen på adekvat lagstiftning och aktivitet från rättsvårdande myndigheter i det aktuella landet. För att strategin ska bli framgångsrik i förhållande till denna typ av tjänster krävs alltså ett mer utvecklat internationellt rättsligt samarbete.

Straff- och skadeståndsansvar för tjänstetillhandahållare

En tydlig strategi i en digital miljö har alltid varit att förhindra intrång med hjälp av rättsliga ageranden mot olika leverantörer av kommunikationstjänster som användarna utnyttjar för att begå intrången. Om mellanhänder riskerar straff- eller skadeståndsansvar kan de tvingas att anpassa sina tjänster så att det generellt blir svårare att begå intrång (t.ex. genom filtrering eller blockering av sådant innehåll som förmedlas)

Ny Juridik 2:12 s 52

eller att vidta åtgärder mot intrång i enskilda fall (t.ex. avstängning av användarkonton som upprepade gånger används för att begå intrång). Leverantörer kan också göra bedömningen att hon eller han helt måste upphöra med tillhandahållandet av tjänsten i syfte att med säkerhet undvika ansvar.

De åtgärder som vidtas kan sålunda förhindra eller försvåra intrång på ett mer eller mindre effektivt sätt, men alla åtgärder utom att upphöra helt med tillhandahållandet innebär fortsatt risk för nya intrång. På samma sätt kan olika åtgärder vara mer eller mindre precisa när det gäller att förhindra just intrång. De flesta åtgärder medför en påtaglig risk för att även laglig kommunikation förhindras. Därmed står det klart att utformningen och tillämpningen av straff- och skadeståndsregler för mellanhänder aktualiserar en delikat avvägning mellan effektivitet och andra viktiga intressen, t.ex. användarnas yttrandefrihet och rättssäkerhet. Reglernas utformning aktualiserar också frågan om hur kostsamma granskning- och bedömningsåtgärder som en tjänstetillhandahållare rimligen kan förväntas utföra för att inte anses medverka till ett intrång.

Modaliteter i straff- och skadeståndsansvarets utformning som påverkar dess effektivitet är bl.a. om tjänstetillhandahållaren är *skyldig att övervaka tjänsten* i syfte att upptäcka intrång, vilken *grad av kännedom* om ett intrång som krävs för ansvaret ska aktualiseras och vilka åtgärder som anses vara tillräckliga för

att *befria från ansvar* när det har konstaterats att intrång i viss omfattning föreligger. Då de faktiska och rättsliga förutsättningarna för att agera effektivt och samtidigt proportionerligt mot intrång i praktiken ser olika ut för olika typer av kommunikationstjänster (internetaccess, lagringstjänster etc.) är det naturligt att dessa i ansvarshänseende behandlas på lite olika sätt. För en tjänstetillhandahållare - men indirekt även för användarna av tjänsten - är det, trots de många intressen som är involverade, viktigt att förutsättningarna för ansvarsfrihet är tydliga. En alltför stor osäkerhet riskerar att leda till att oönskade begränsningar i möjligheterna att kommunicera vidtas.

Det svenska (inklusive det EU-rättsliga) regelverket på området är komplext. Det straff- och skadeståndsrättsliga ansvaret för tillhandahållare av kommunikationstjänster bestäms i grunden av *brottsbalkens* allmänna regler om medverkan till brott, särskilt medhjälp. Vid en straffrättslig prövning av en tjänstetillhandahållares ansvar enligt dessa regler aktualiseras framför allt *teorier om bristande gärningsculpa och*

Ny Juridik 2:12 s 53

socialadekvans. I praktiken blir det vid en sådan prövning nödvändigt för domstolen att göra normativa (rättspolitiska) bedömningar av vad som ska anses vara ett tillåtet risktagande i samband med tillhandahållande av en kommunikationstjänst. Avgörande för utgången av en sådan prövning kommer typiskt sett att vara vilka olika intressen som inkluderas i bedömningen och hur dessa vägs mot varandra. Eftersom det handlar om kommunikation är det naturligt att yttrandefrihetsrättsliga principer tillmäts särskild vikt i detta sammanhang. Därutöver aktualiserar frågan hur kravet på *subjektiv täckning* (t.ex. uppsåt) ska bedömas. Alla kommunikationstjänster som tillhandahålls allmänheten kommer i varierande utsträckning att användas för att begå brott. Frågan blir därför vilken grad av insikt, kännedom etc. som krävs för att uppsåtlig eller grovt oaktsam medverkan ska anses föreligga.

Brottsbalkens reglering kompletteras när det gäller s.k. *elektroniska anslagstavlor* (i praktiken främst lagringstjänster där användarna kan lägga upp material) med en straffsanktionerad skyldighet för tillhandahållaren att ta bort sådant material som en användare har skickat in till tjänsten om denne därigenom uppenbart har gjort sig skyldig till upphovsrättsintrång (och vissa andra uppräknade brott). Denna reglering finns i lagen om ansvar för elektroniska anslagstavlor (BBS-lagen).

Dessa regler med ett rent svenskt ursprung kompletteras av de EU-rättsliga *ansvarsfrihetsreglerna* i EU:s direktiv om elektronisk handel (2000/31/EG). Dessa bestämmelser sätter den yttre gränsen för det nationella straff- och skadeståndsansvaret genom att ange relativt tydliga förutsättningarna för när tillhandahållare av tre olika kategorier av kommunikationstjänster, nämligen enbart vidarebefordran (access och ren överföring), cachning och värdtjänster (lagringstjänster), är ansvarsfria. Förutsättningarna för ansvarsfrihet varierar mellan de olika typerna av tjänster. Ansvarsfriheten för enbart vidarebefordran är t.ex. tämligen heltäckande, medan ansvarsfriheten för en tillhandahållare av värdtjänster går förlorad när denne erhåller en viss grad av kännedom om ett intrång eller om de omständigheter som konstituerar ett intrång.

Medverkansansvaret närmare gränser vid tillhandahållande av kommunikationstjänster får än så länge betecknas som relativt oklart. Strategin kan vara *effektiv* mot det som kan beskrivas som ”rena pirattjänster”, dvs. tjänster som helt undviker att ta bort intrångsgörande material, trots att de har fått konkret kännedom om att sådant material görs tillgängligt via tjänsten, och som i praktiken uppmanar sina

Ny Juridik 2:12 s 54

användare till att fortsätta att begå intrång. Problemet när det gäller denna typ av tjänster kan i stället vara att identifiera vilka personer som faktiskt är involverade i tillhandahållandet av tjänsten

Troligen är ansvaret betydligt mer begränsat när en tjänst i inte obetydlig utsträckning används för laglig verksamhet och det finns rimligt fungerande rutiner för att ta bort intrångsgörande material när tillhandahållaren underrättas om sådant. Även beträffande denna typ av tjänster kan rättighetshavare utnyttja hotet om ansvar, t.ex. enligt BBS-lagen, till att få utpekat intrångsgörande material borttaget från tjänsten. Även denna strategi kan vara effektiv, om än relativt arbetskrävande. Fler och fler rättighetshavare (och leverantörer av lagringstjänster) utnyttjar emellertid nu automatiska system för identifiering av skyddade verk som har laddats upp på öppna lagringstjänster. Den ökande användningen av cyberlockers (jfr ovan) för att begå intrång gör det emellertid svårare för rättighetshavare att identifiera intrångsgörande filer. Utvecklingen aktualiserar i förlängningen frågan om leverantörer av lagringstjänster i framtiden

bör åläggas en skyldighet att installera programvara som automatiskt söker igenom den egna tjänsten i jakt på intrång.

Ansvarsfrihetsregeln för *accessleverantörer* i EU-rätten (till skillnad från den svenska implementeringen av denna regel) är i princip utformad så att ett medverkansansvar är uteslutet i andra situationer än när accessleverantören agerar i maskopi med den egentliga intrångsgöraren.

Föreläggande om blockering, filtrering och avstängning

Under senare tid har det internationellt blivit vanligare med domstolsbeslut som innebär att framför allt accessleverantörer föreläggs att vidta vissa åtgärder för att avbryta ett pågående intrång eller att hindra framtida intrång av samma slag. Enligt EU-rätten ska det i princip finnas möjlighet att utverka ett föreläggande mot mellanhänder vars tjänster utnyttjas för att begå intrång i större omfattning, men de närmare formerna för föreläggandet lämnas till medlemsstaterna att besluta om. Sett i ett internationellt perspektiv är det emellertid långtifrån självklart att accessleverantörer ska kunna föreläggas att ingripa mot kommunikation i sina nät. I grund och botten handlar det om synen på dessa kommunikationstjänster och deras roll i samhället.

Beroende på föreläggandets närmare utformning är det möjligt att tala om krav på *avstängning* (skyldighet att upphöra med att leverera

Ny Juridik 2:12 s 55

access till en intrångsgörare), *blockering* (skyldighet att förhindra att leverantörens kunder från att nå viss adress etc.) och *filtrering* (skyldighet att automatiskt granska information som passerar genom nätet och hindra kommunikation som utgör upphovsrättsintrång från att nå sin mottagare).

En fördel från *effektivitetssynpunkt* är att förelägganden av dessa slag kan utverkas relativt fort. Normalt prövas frågan om ett eventuellt föreläggande i en interimistisk process där rättighetshavare och accessleverantör är parter. En annan fördel är att det normalt sett blir relativt tydlig för accessleverantören vad denne måste göra, eftersom det är domstolen som utformar det konkreta föreläggandet. Genom att ett föreläggande i praktiken syftar till att helt begränsa olika användares möjlighet att få tillgång till eller att kommunicera viss (intrångsgörande) information kan föreläggandet många gånger framstå som effektivt när det gäller att förhindra framtida intrång. Om den egentliga intrångsgöraren inte kan förmås att upphöra med sin verksamhet kan åtgärder som i praktiken tar sikte på att minska intrångets negativa effekter framstå som attraktiva.

Sett i ett internationellt perspektiv utgör föreläggande om *blockering* av en viss tjänst den mest förekommande formen av föreläggande. Sådan blockering kan rent tekniskt utformas på olika sätt, t.ex. kan blockeringen ta sikte på vissa IP-adresser eller på vissa domännamn. Blockeringen har alltså rent tekniskt nästan alltid en utformning som är vidare än det intrång som motiverar den. Detta aktualiserar som nämnts i avsnitt 5 bl.a. frågor om proportionalitet. Åtminstone i situationer när intrången sker med hjälp av tjänster som till väsentlig del innehåller annat än intrångsgörande material kommer föreläggande om blockering därför troligen inte att kunna utverkas. Därtill kan läggas att användare som har en drivkraft att begå intrång (t.ex. med hjälp av sådana tjänster som har blockerats av deras accessleverantör) kan utnyttja enkelt tillgängliga instruktioner eller tjänster för att kringgå blockeringen. Sådan drivkraft finns typiskt sett just när det gäller de tjänster som kan vara aktuella för blockering, t.ex. The Pirate Bay. Användarna av dessa tjänster är redan medvetna om att de (typiskt sett) begår ett intrång när det fildelar upphovsrättsligt skyddat material, men har valt att strunta i det.

För att ett föreläggande på ett mer effektivt sätt ska förhindra intrång krävs alltså i princip att själva innehållet i användarnas kommunikation granskas och blockeras (dvs. filtrering). Grundläggande

Ny Juridik 2:12 s 56

rättigheter och andra motstående intressen gör emellertid att förelägganden av detta slag knappast är möjliga (jfr t.ex. EU-domstolens dom i C-70/10). Därtill kan läggas att även filtrering kan kringgås, t.ex. genom krypterad kommunikation. En ökad effektivitet i systemet med föreläggande tycks sålunda kräva förändringar av internets grundläggande öppna infrastruktur.

I den utsträckning som ett föreläggande om *avstängning* kan förhindra att intrångsgörande material ens finns åtkomligt på nätet är effektiviteten naturligtvis högre. Ofta finns det emellertid alternativa leverantörer av internetaccess för den som verkligen vill nå ut med material på nätet. En nackdel med att ett föreläggande om avstängning är vidare att det normalt måste utverkas i det land där den intrångsgörande tjänsten bedrivs. Detta gör att strategin att utverka ett sådant föreläggande blir mindre effektiv när det gäller rena pirattjänster som agerar i länder utan ett effektivt upphovsrättsskydd.

En principiell invändning mot en strategi som går ut på att utverka förelägganden mot olika typer av mellanhänder är att de som egentligen berörs av beslutet, dvs. leverantören av den server etc. som ska blockeras och de användare vars kommunikationsmöjligheter begränsas, typiskt sett inte har partsställning i dessa processer. Samtidigt har accessleverantören inte alltid resurser och incitament att gå i svaromål i dessa typer av mål. Därigenom skapas ofta en viss obalans i processer om denna typ av förelägganden.

Andra särskilda arrangemang anpassade för internetmiljön

Det framhålls ibland att nätmiljön - framför allt den omfattande olagliga användningen av fildelningstekniken - kräver specialanpassade rättsliga lösningar som kan motverka intrång på ett sätt som samtidigt är både effektivt och förenligt med motstående intressen. Ett argument för specialanpassade lösningar är också att det krävs att det allmänna tar ett större ansvar för att motverka även småskaliga intrång som sammantaget anses skada rättighetshavare på ett allvarligt sätt. En strategi mot denna typ av intrång kräver, framhålls det, ett moment av utbildning av nätanvändarna och att dessa ges tillfälle att förändra sitt beteende innan de drabbas av en mer kännbar sanktion.

Detta synsätt ligger till grund för den berömda *Hadopi-lagen* i Frankrike. Den franska lösningen, som ofta beskrivs i termer av ”graduated

Ny Juridik 2:12 s 57

response” eller ”three strikes and you’re out” tar främst sikte på tillgängliggörande i fildelningsnätverk genom att introducera ett statligt system för att sända *varningsbrev* till abonnenter vars uppkoppling har utnyttjats för otillåtet tillgängliggörande för allmänheten av skyddade verk. Efter tre varningar kan accessleverantören föreläggas att avsluta ett abonnemang. Abonnemangsinnehavarens namn förs samtidigt upp på en spärrlista, vilket gör det otillåtet för andra leverantörer att låta denna person teckna abonnemang under en viss tid.

En statlig myndighet (Hadopi) har i uppdrag att ta emot anmälningar om intrång från rättighetshavare och skicka ut varningsbrev i olika former. Beslut om avstängning av en abonnent fattas av domstol efter begäran av myndigheten. Hela processen är i hög grad automatiserad och förutsätter en omfattande informationsbehandling. Systemet bygger på tanken att en abonnent är ansvarig för hur uppkopplingen används och att rättighetshavarens uppgifter i anmälan om intrånget i stor utsträckning tas för goda. Det har därför bl.a. ifrågasatts om systemet uppfyller grundläggande rättssäkerhetskrav (t.ex. oskuldspresumtionen). Det enda sättet för en abonnent att slippa avstängning för ett intrång som han eller hon kanske inte själv har utfört är att installera en särskild säkerhetsprogramvara som myndigheten anvisar. Precis som när det gäller strategier som fokuserar på den egentliga intrångsgöraren blir denna strategis effektivitet bristande om intrångsgöraren använder sig av en anonymiseringstjänst.

Det element i Hadopi-systemet som har kritiserats mest är själva möjligheten att besluta om *avstängning* av ett abonnemang. Utgångspunkten för lagstiftningen var som sagt att systemet skulle vara mindre ingripande för den enskilde än en normal straff- eller skadeståndsrättslig process, men en avstängning från internet kan tvärtom uppfattas som en alltför ingripande sanktion, ett kännbart straff som utdöms utan tillgång till normala straffrättsliga rättssäkerhetsgarantier. Frågan om skydd mot avstängning från internet var bl.a. föremål för diskussion under förhandlingarna om det s.k. Telekompaketet år 2009, dvs. EU:s översyn av ett antal direktiv på telekommunikationsområdet. Resultatet av dessa förhandlingar blev att det i artikel 1.3 i direktivet om samhällsomfattande tjänster (2002/22/EG) numera anges att nationella bestämmelser om slutanvändares tillgång till eller användning av tjänster och tillämpningar av elektroniska kommunikationsnät måste vara förenliga med grundläggande rättigheter i Europakonventionen,

Ny Juridik 2:12 s 58

bl.a. rätten till en rättvis rättegång och rätten till personlig integritet. Det kan diskuteras om Hadopi-lagens system för avstängning skulle klara en prövning enligt Europakonventionen.

Samtidigt innehåller systemet vissa moment som framstår som tilltalande, både när det handlar om att skapa mer effektiva sanktioner och när det gäller att förbättra skyddet för grundläggande rättigheter. Varningsfunktionen har, som framhållits, flera fördelar för den som blir varnad. Exempelvis kan denne vidta åtgärder för att motverka framtida intrång. Men ett system med varningsbrev och registrering av vilka abonnenter som tidigare har tagit emot varningar har även andra fördelar. För det första framstår det från ett rättspolitiskt perspektiv som önskvärt att sanktioner först och främst riktas mot stora eller återkommande intrångsgörare. För det andra kan möjligheten att vinna en civilrättslig process eventuellt förbättras om en rättighetshavare kan visa att en abonnemangsinnehavare tidigare har varnats, men inte vidtagit tillfredsställande åtgärder för att säkerställa kontrollen över uppkopplingen.

Ett möjligt alternativ till det franska systemet skulle därmed t.ex. kunna vara ”three strikes and you’re identified”. Internetoperatörer skulle i ett sådant system ges en rättslig skyldighet att under vissa förhållanden vidarebefordra varningsbrev från rättighetshavare och föra en förteckning över dem som varnats. Om samma abonnent varnas igen inom viss tid skulle operatören vara skyldig att lämna uppgift om detta förhållande till rättighetshavaren. Denne kan baserat på egna bevis och med uppgifterna från operatören begära ett informationsföreläggande avseende abonnemangsinnehavarens identitet. Domstolen har, när information om tidigare varningar finns tillgänglig, ett bättre underlag för att göra sin proportionalitetsbedömning.

Även andra specialanpassade lösningar för att motverka intrång på nätet har föreslagits. I Australien och UK har särskilda statliga spärrlistor, som utan domstolsbeslut i det enskilda fallet ska implementeras av accessleverantörerna i landet, diskuterats. I USA rasade nyligen en omfattande debatt om de två lagförslagen *SOPA och PIPA* som lades fram i den amerikanska kongressen och representanthuset. Förslagen innebar bl.a. att rättighetshavare eller riksåklagaren kunde utverka ett domstolsbeslut om blockering av vissa utländska webbplatser som i huvudsak var ägnade att främja intrång i amerikanska verk. Blockeringen skulle sedan implementeras av amerikanska accessleverantörer. Förslaget innehöll även regler som innebar att domännamn som

Ny Juridik 2:12 s 59

användes i intrångsgörande verksamhet skulle kunna beslagtas av den amerikanska staten. Förslagen kritiserades för att innebära ett hot mot användarnas grundläggande rättigheter samt ett ”öppet internet” och drogs (tillfälligt) tillbaka.

”Självreglering” och ”frivilliga åtgärder”

En strategi som ofta förespråkas från rättighetshavarsida är att tillhandahållare av kommunikationstjänster ska uppställa särskilda regler för användning av tjänsten som syftar till att motverka upphovsrättsintrång (”självreglering”) och vidta olika praktiska åtgärder för att upprätthålla dessa regler (”frivilliga åtgärder”). Frivilliga arrangemang uppmuntras också i vissa internationella regelverk (t.ex. EU:s direktiv om elektronisk handel 2000/31/EU och det s.k. ACTA-avtalet). Politiskt kan det framstå som tilltalande att förorda självreglering som ett uttryck för en marknadslösning, men lika ofta ses nog denna lösning som ett sätt att undvika lagstiftning på ett politiskt känsligt område.

Den enskilde tjänsteleverantörens ambitionsnivå avgör hur effektiva frivilliga åtgärder mot upphovsrättsintrång blir. Häri ligger naturligtvis strategins effektivitetsproblem. Om det verkligen handlar om frivillighet kan det vara svårt att få aktörer som verkar på en konkurrensutsatt marknad att vidta ingripande åtgärder som kunderna kan uppfatta som försämringar, utan försäkringar från alla betydelsefulla konkurrenter om att de också vidtar motsvarande åtgärder. Av detta skäl görs ofta försök att få tillstånd frivilliga åtgärder genom olika former av ”branschsamtal”. Sådana samtal har förts såväl på EU-nivå som i många medlemsstater, bl.a. Sverige, under senare år. I vissa sammanhang är det i praktiken fråga om frivillighet under galgen, där de inblandade aktörerna hotas med lagstiftning om de inte ”frivilligt” kommer fram till en lösning. Problemet med denna typ av hot är att tjänsteleverantörer normalt, av såväl förutsebarhetsskäl som pr-skäl, föredrar att deras skyldigheter preciseras i lagstiftning och att någon annan gör bedömningen av vad som är lagligt och olagligt.

När det gäller förhållandet till de ovan behandlade grundläggande rättigheterna kan frivilliga lösningar framstå som effektiva. Yttrandefrihetsregleringen och regler om rättssäkerhet begränsar t.ex. inte på samma sätt vilka åtgärder som privata företag på eget initiativ kan vidta mot sina kunder. Därmed är inte sagt att det inte finns situationer där en stat enligt Europakonventionens horisontella skydd för yttrandefriheten

Ny Juridik 2:12 s 60

kan vara skyldig att ingripa mot kommunikationsoperatörers begränsning av enskilda medborgares möjlighet att yttra sig. Regler om personuppgiftsbehandling och skydd för post- och telehemligheten är i princip tillämpliga fullt ut vid ”frivilliga åtgärder”. Detta innebär i praktiken att självreglering ofta kan vara svårare att tillämpa för accessleverantörer än för t.ex. tillhandahållare av lagringstjänster. Även försvaret av ett ”öppet internet” kan sägas tala emot frivilliga åtgärder på accessnivå (t.ex. blockering, filtrering och avstängning). Eftersom dessa frivilliga åtgärder kan ses som en avvikelse från principen om nätneutralitet uppfattas de många gånger som minst lika problematiska som lagstiftning med motsvarande innehåll. Tjänstetillhandahållare bör, enligt detta synsätt, inte ges makt att bestämma om och hur olika typer av trafik på nätet ska förmedlas eftersom detta på sikt bl.a. kommer leda till en fragmentisering av nätet och att dess positiva egenskaper går förlorade.

Mot ”självreglering” och ”frivilliga åtgärder” som strategi mot intrång kan även andra principiella invändningar resas. Själva begreppet *självreglering* är missvisande eftersom det ytterst är de som kommunicerar på nätet som påverkas. Att uppfatta intrång på nätet som en fråga som ska lösas i diskussioner mellan rättighetshavare och tillhandahållare av olika typer av kommunikationstjänster framstår därmed som problematiskt. De som ytterst berörs av den reglering som tas fram - användarna - är sällan representerade på ett godtagbart sätt. På samma sätt har en användare ofta rätt att kräva rättssäkra processer för t.ex. borttagning av hans eller hennes material även om tjänstetillhandahållaren gör detta av eget initiativ. Därigenom finns det i praktiken ofta ett *legitimitetsproblem* förknippat med denna strategi. Eftersom så många principiella intressen aktualiseras när möjligheterna att kommunicera ska begränsas i syfte att lösa ett visst samhällsproblem talar mycket för att detta i huvudsak bör ske genom lagstiftning. Därmed inte sagt att det inte i vissa fall, framför allt i samband med *lagringstjänster*, finns ett utrymme för en tjänstetillhandahållare att konkretisera den rättsliga regleringen med egna villkor eller att utforma effektiva processer för nedtagning av intrångsgörande material.

Val av strategi/er

Analysen av de olika strategierna har inte gjorts så djupgående att den tillåter några helt entydiga slutsatser om vilken eller vilka strategier som

Ny Juridik 2:12 s 61

bör väljas. Det tycks som om intrång i olika miljöer delvis kan kräva olika strategier. Samtidigt har det konstaterats att alla de behandlade strategierna har tydliga effektivitetsbrister. Dessa brister kan inte bara utnyttjas av tekniskt kunniga användare, utan även andra användare som har drivkraften att komma åt skyddade verk etc. Det kan t.ex. handla om att använda anonymiseringstjänster eller lösningar för att kringgå blockering av vissa domännamn.

Även om vissa rättsliga förutsättningar kan förändras i syfte att göra strategierna mer effektiva är det knappast möjligt att åstadkomma väsentligt högre effektivitet. En viktig förklaring till detta är att effektiva sanktioner och skyddet för användarnas (andra) grundläggande rättigheter ofta utgör två kommunicerande kärl. Riktigt effektiva sanktioner kräver, med de grundläggande tekniska förutsättningar som finns, i princip rättsliga lösningar som inte är godtagbara i ett demokratiskt samhälle. När ansvars- och sanktionsregler samt processuella regler utformas och tillämpas måste nämligen en avvägning mellan flera grundläggande rättigheter göras (se t.ex. EU-domstolens domar C-275/06 och C-70/10). Detta resulterar i att de mest effektiva rättsliga strategierna inte kommer anses vara godtagbara.

Alternativet att i grunden förändra internetarkitekturer i syfte att skapa en ”säkrare” miljö återstår naturligtvis. En sådan strategi är emellertid svår att förena med de tekniska, ekonomiska och politiska intressena förknippade med ett ”öppet internet”. Det är tveksamt om upphovsrätten i dag har en sådan ställning att den kan anses rättfärdiga krav på fundamentala förändringar av detta slag. Däremot finns det andra starka krafter, främst i form av totalitära stater, men också inom ”säkerhetsindustrin”, som av helt andra

skäl är intresserade av motsvarande förändringar, t.ex. att göra det lättare att spåra kommunikation på internet och svårare att kring blockering och filtreringsåtgärder som vidtas av staten. Motståndet mot en sådan utveckling är, under parollen ”friheten på nätet”, emellertid stort och växande, inte bara i den tekniska världen utan även på politiska arenor.

För egen del drar jag slutsatsen att *strategier som inriktar sig mot den egentliga intrångsgöraren* bör vara huvudstrategin även när intrång sker på nätet. Det faktum att det i denna miljö är fråga om många intrångsgörare, som står för relativt begränsade intrång, bör inte ändra på detta förhållande. Det finns flera skäl till att jag har kommit till denna slutsats.

Ny Juridik 2:12 s 62

Ett viktigt skäl är att strategin är viktig för att medborgarnas *respekt för upphovsrätten* inte ska urholkas. Strategier som i stället är inriktade på att minska effekterna av de intrång som sker (avstängning, blockering och filtrering) riskerar att leda till uppfattningen att det är fråga om en teknisk kamp mellan dem som vill kommunicera och dem som vill förhindra det. Detta bidrar till att användarnas intrång i sig uppfattas som mindre allvarliga, vilket i sin tur kan leda till att fler användare får drivkraften att utnyttja de tillgängliga metoderna för kringgående av t.ex. blockeringar, med följd att strategin som sådan blir mindre effektiv. Till detta bidrar också att uppmärksamheten kring vilka tjänster som blockeras alltid blir stor på nätet.

Den politiska utgångspunkten, ”att man inte kan kriminalisera en hel ungdomsgeneration”, borde därför rimligen leda till slutsatsen att den lagliga tillgången till skyddat material måste förbättras och att åtgärder för att stärka upphovsrättens legitimitet bland gemene man bör vidtas, inte till att huvudstrategin att hålla den enskilde intrångsgöraren ansvarig bör överges.

Ett sätt att stärka den här diskuterade strategin är, som framhållits i avsnitt 9, att införa ett system med *varningsbrev*. Varningsbreven kan ha en både preventiv och utbildande funktion. Ett sådant system dock är främst relevant om intrången på nätet i väsentlig utsträckning sker genom fildelning. Effekten av upprepade intrång bör inte som i Frankrike vara avstängning, utan att uppgifter om abonnenten kan bli tillgängliga för rättighetshavare. Huruvida särskilda regler om en abonnentens civilrättsliga ansvar för uppkopplingens användning behövs i denna situation är osäkert.

Denna strategi kräver ett ökat fokus på *internationellt rättsligt samarbete*. Det är därför något av en paradox att många debattörer som starkt förespråkar att ”ett öppet internet” samtidigt motsätter sig internationella avtal om sådant samarbete. Bristande möjligheter att stoppa utländska pirattjänster ”vid källan” leder nämligen i de flesta fall till krav på blockering och filtrering.

Strategin att hålla den enskilda intrångsgöraren ansvarig kan i förekommande fall *kompletteras* med övriga strategier, givetvis under förutsättning att dessa i det enskilda fallet är förenliga med de krav som följer av en tillämpning av de grundläggande rättigheterna.

Det *straff- och skadeståndsrättsliga ansvaret för tillhandahållare* av kommunikationstjänster, främst olika typer av lagringstjänster och andra tjänster som underlättar olovlig fildelning, spelar en relativt viktig

Ny Juridik 2:12 s 63

roll, men i princip endast för sådana tjänster som drivs med kvalificerat ont uppsåt och där den lagliga användningen är av helt underordnad betydelse. När det gäller andra tjänster av dessa slag bör ansvar i princip främst kunna komma i fråga i samband med försumlighet att ingripa mot uppenbara intrång som tillhandahållaren har kännedom om. I detta sammanhang kan även egna regelverk och rutiner vara en framkomlig väg för att nå resultat. Accessleverantörer bör inte, annat än i de undantagsfall som har beskrivits ovan, kunnat hållas straff- och skadeståndsansvariga.

Den nuvarande tillämpningen av regler om föreläggande som leder till *avstängning eller blockering*, framför allt i andra länder, inger enligt min mening betänkligheter, dels därför att strategin, som framhållits ovan, i viss utsträckning framstår som kontraproduktiv, dels därför att den avvägning i förhållanden till andra intressen som gjorts i många fall kan ifrågasättas. Därmed är inte sagt att dessa metoder aldrig bör vara tillåtna. En rimlig utgångspunkt är dock att dessa åtgärder uppfattas som en sista utväg när andra metoder

har uttömts. Vidare bör förändringar av processen som leder fram till ett beslut göras så att allmänhetens intressen bättre tillgodose.

Förelägganden om införande av *filtrering* är typiskt sett uteslutna när det gäller accesstjänster, men kan emellertid spela en viss roll beträffande vissa typer av lagringstjänster. En förutsättning är då givetvis att föreläggandet kan implementeras på ett godtagbart sätt.

Slutsatser om sanktionernas roll

Analysen föranleder även vissa övergripande slutsatser om vilken roll som strategier mot intrång spelar för att lösa de utmaningar som upphovsrätten står inför i dag. Alldeles oberoende av det värde som anses finnas i den upphovsrättsliga ensamrätten och den rätt till effektiva sanktioner som en rättighetshavare har rätt till enligt internationella regler är det viktigt att ha en realistisk bild av vad som faktiskt är möjligt att uppnå genom sådana strategier. Framställningen har visat att strategiernas effektivitet i en nätmiljö i hög grad är beroende av vilka drivkrafter som användarna har att kringgå dem.

Detta bör mana till viss eftertanke. Givetvis har sanktioner en viktig roll att fylla även när intrång begås på nätet, men behovet av att dessa sanktioner uppfattas som legitima blir mycket större i denna miljö. De senare åren tycks misstron mot det upphovsrättsliga systemet snarare

Ny Juridik 2:12 s 64

ha stärkts. En förklaring kan vara att upphovsrätten som sådan inte har uppfattats som tillräckligt balanserad (jfr punkt B i avsnitt 1 ovan). En annan förklaring är att den upphovsrättsliga avtalsmarknaden inte har fungerat och förmått möta den efterfrågan som har funnits (jfr punkt c i avsnitt 1 ovan). Ett för stort fokus på sanktioner, när många upplever att upphovsrätten inte förmår leverera det verksinnehåll som efterfrågas i rätt form, rätt tid och till rätt pris, riskerar att utsätta upphovsrätten för stora påfrestningar. Om medborgarna inte uppfattar att systemet ”levererar”, kan respekten för systemet inte upprätthållas med hjälp av sanktioner. Diskussionerna som redovisas under punkt B och C ovan är därför helt centrala för upphovsrättens framtid.