

IRI PM

IRI Promemoria 3 / 2007

Daniel Westman

Förslag på nya civilrättsliga sanktioner i kampen mot olaglig fildelning - en kritisk granskning



Institutet för rättsinformatik
Juridiska fakulteten, Stockholms universitet

Förslag på nya civilrättsliga sanktioner i kampen mot olaglig fildelning – en kritisk granskning

Daniel Westman

1. Inledning

På kort tid har två uppmärksammade och kontroversiella lagförslag som skall underlätta rättighetshavarnas kamp mot olaglig fildelning på nätet presenterats. Det första förslaget innebär i korthet att en domstol skall kunna förelägga den som i kommersiell skala har tillhandahållit en elektronisk kommunikationstjänst (t.ex. access till Internet) att lämna ut information till en immaterialrättsinnehavare om t.ex. identiteten på de personer vars abonnemang har använts för att begå intrång (informationsföreläggande). Det andra förslaget innebär i korthet att en domstol på begäran av en upphovsrättsinnehavare skall kunna ålägga en accessleverantör att t.ex. säga upp avtalet med en abonnent om tjänsten upprepade gånger har utnyttjats för att göra skyddade prestationer tillgängliga för allmänheten i strid med upphovsrätten.

I denna artikel presenteras och kommenteras de båda förslagen. Framställningen begränsas till de föreslagna reglernas betydelse för accessleverantörer och enskilda användare som utnyttjar deras tjänster. Regler om informationsföreläggande förslås i alla de immaterialrättsliga lagarna, men här diskuteras endast reglernas innebörd och funktion vid intrång i upphovsrätten. De kritiska kommentarer som framförs utgår främst från förslagets förhållande till grundläggande fri- och rättigheter, t.ex. yttrande- och informationsfriheten och skyddet för den personliga integriteten, samt till kraven på rättsäkerhet.

Det bör noteras att båda förslagen läggs fram inom ramen för mer omfattande utredningsuppdrag. Förslaget om informationsföreläggande presenteras i departementspromemorian ”*Civilrättsliga sanktioner på immaterialrättens område – genomförande av direktiv 2004/48/EG*” (Ds 2007:19), som i ljuset av det s.k. sanktionsdirektivet behandlar civilprocessuella regler och sanktioner inom hela immaterialrätten. Ett informationsföreläggande skall enligt förslaget kunna meddelas i olika situationer och riktas mot olika subjekt. Förslaget om att införa möjligheter till domstolsföreläggande som ålägger accessleverantörer att säga upp avtalet med sina kunder presenteras i departementspromemorian ”*Musik och film på Internet - hot eller möjlighet?*” (Ds 2007:29). I promemorian görs en bred översyn av upphovsrätten på Internet. I promemorian avfärdar utredaren t.ex. möjligheten att ersätta ensamrätten till förfoganden online med någon form av ”bredbandsavgift”. Samtidigt föreslås att konsumentskyddet i samband med nedladdningar och s.k. streaming stärks och att en närmare utredning om hur detta kan ske görs. Film- och musikbranscherna uppmanas också att se över de avtalsvillkor som används vid utnyttjande av onlinetjänster och att göra eventuella tekniska skyddsåtgärder som används mer konsumentvänliga. Förslaget om föreläggande mot accessleverantörer är emellertid det enda konkreta lagstiftningsförslag som presenteras av utredningen.

2. Förslaget om informationsföreläggande

Om ett upphovsrättsintrång har begåtts skall en domstol vid vite få förelägga vissa personer att lämna information om ”ursprung och distributionsnät för den fysiska eller digitala vara med avseende på vilken intrånget eller överträdelsen har begåtts”. Det kan t.ex. handla om information om namn på och adress till den som tillhandahållit en vara eller tjänst online. Informationen skall syfta till att underlätta utredningen av intrånget. I den personkrets som skall kunna åläggas att lämna information ingår den som ”i kommersiell skala har tillhandahållit en tjänst, exempelvis en elektronisk kommunikationstjänst, som har använts vid intrånget eller överträdelsen”. Det innebär att ett informationsföreläggande skall kunna riktas mot t.ex. en person som i kommersiell skala tillhandahåller access till Internet. Med uttrycket kommersiell skala avses ”handlingar som utförs för att uppnå en direkt eller indirekt kommersiell eller ekonomisk fördel, vilket i allmänhet utesluter handlingar som utförs av slutkonsumenter i god tro” (Ds 2007:19 s. 323).

Beslut om informationsföreläggande skall endast kunna meddelas efter ansökan av rättighetsinnehavare eller den som på grund av upplåtelse har rätt att utnyttja verket. Den sökanden måste ha visat att ett intrång begåtts, men det skall inte krävas att den som har begått intrånget

är identifierad. Inte heller skall det krävas att intrånget har begåtts uppsåtligen eller av oaktsamhet. På samma sätt som när det gäller vitesförbud skall det vara tillräckligt att det i objektiv mening föreligger ett intrång (Ds 2007:19 s. 320).

Om ett informationsföreläggande utfärdas innebär det att en accessleverantörs tystnadsplikt enligt 6 kap. 20 § lagen om elektronisk kommunikation bryts (Ds 2007:19 s. 182 f.). Denna tystnadsplikt omfattar uppgifter om abonnemang, innehållet i ett elektroniskt meddelande och andra uppgifter som angår ett särskilt telemeddelande.

Ett informationsföreläggande får enligt förslaget endast meddelas om ”skälen för åtgärden uppväger den olägenhet eller det men i övrigt som åtgärden innebär för den som drabbas eller för något annat motstående intresse”. Ett informationsföreläggande måste annorlunda uttryckt vara proportionerligt. Ett föreläggande får inte innebära att någon blir skyldig att lämna information som skulle avslöja egen eller nära anhörigs brottslighet.

Ett informationsföreläggande kan enligt förslaget meddelas av den domstol där rättegång om intrånget pågår. Om rättegång om intrånget inte pågår kan informationsföreläggande ändå bli aktuellt. Förslaget går på denna punkt längre än vad artikel 8 i sanktionsdirektivet kräver. Skälen till att detta föreslås är att ett pågående mål annars lätt skulle kunna tyngas med sådant som inte är relevant för målets avgörande och att en sådan ordning skulle strida mot grundläggande principer i svensk processrätt (Ds 2007:19 s. 172 f.). Men effekten av att en pågående rättegång inte krävs blir också att det uppkommer en möjlighet för rättighetshavare att kräva informationsförelägganden riktade mot accessleverantörer, trots att det normalt saknas rättslig grund för att väcka talan om intrång eller medverkan till intrång mot dessa. Om ett informationsföreläggande begärs utan att en rättegång pågår skall motparten få rätt att yttra sig innan ett föreläggande beslutas. Muntlig förhandling skall hållas om det behövs med hänsyn till utredningen.

Den som efter ett föreläggande har lämnat information skall ha rätt till skälig ersättning för kostnad och besvär. Ersättningen skall betalas av den part som begärt informationen.

I förslaget om informationsföreläggande ingår även en särskild reglering om personuppgiftsbehandling hos rättighetshavare som utreder intrång. Bakgrunden är personuppgiftslagens restriktiva inställning till behandling av personuppgifter om lagöverträdelser och det faktum

att rättighetshavarna för att kunna begära ett informationsföreläggande måste kunna samla in uppgifter av detta slag för att styrka att intrång äger rum (jfr Westman, *Personuppgiftslagen och kampen mot piratkopiering*, Lov&Data nr. 84 2005, s. 7 ff.). Enligt förslaget införs ett särskilt undantag från förbudet i 21 § personuppgiftslagen som innebär att personuppgifter om lagöverträdelse som innefattar brott mot upphovsrättslagen får behandlas om detta är nödvändigt för att ett rättsligt anspråk skall kunna fastställas, göras gällande eller försvaras i ett enskilt fall. Övriga regler i personuppgiftslagen skall fortfarande tillämpas på behandlingen.

3. Förslaget om förbud mot fortsatt Internetaccess etc.

”En Internetleverantör som ägnar sig åt ren vidarebefordran” föreslås få en ”rätt och en skyldighet att med omedelbar verkan säga upp ett avtal om användning av sina tjänster, om den tjänst som avses med avtalet upprepade gånger har utnyttjats för att begå intrång” i rättighetshavarens ensamrätt att överföra verket till allmänheten eller att framföra verket offentligt och ”det är sannolikt att intrången kommer att fortsätta”. En sådan uppsägning skall dock inte få ske om det ”med hänsyn till omständigheterna skulle vara oskäligt”.

Den föreslagna bestämmelsen skall enligt författningskommentaren endast tillämpas när det gäller sådana Internetleverantörer som ”har avtal med bl.a. företag, enskilda och myndigheter om tillhandahållande av uppkoppling mot Internet” (Ds 2007:29 s. 366), dvs. endast accessleverantörer, inte tillhandahållare av rena överföringstjänster t.ex. överföringskapacitet inom ett företag.

En förutsättning för uppsägning är att ”intrång förekommit tidigare, vid upprepade tillfällen. Framförallt omfattas situationer där otillåtna tillgängliggöranden sker systematiskt och vane- mässigt. Enstaka tillgängliggöranden, eller tillgängliggöranden med en större tidsrymd emellan omfattas inte av bestämmelsen” (ibid).

För att skyldigheten att säga upp avtalet skall aktualiseras är det enligt förslaget tillräckligt att det i objektiv mening föreligger ett intrång. Uppsåt eller oaktsamhet hos den som gör intrång behöver inte styrkas. Inte heller intrångets eventuella skadeverkningar behöver styrkas. En förutsättning är emellertid att det är sannolikt att intrången kommer att fortsätta. När omfattande intrång förekommit kan det enligt utredning normalt förutsättas att också framtida intrång kommer att ske, men en motsatt bedömning kan göras om någon förändring i förhållanden som rör abonnenten har skett. Detsamma bör enligt utredningen gälla om Internetleve-

rantören har ”dragit ner uppkopplingshastigheten så att framtida omfattande intrång i praktiken omöjliggörs” (Ds 2007:29 s. 366 f.).

Uppsägning skall enligt förslaget inte få ske om det skulle vara oskäligt med hänsyn till omständigheterna. Vid en sådan bedömning är tanken att abonnentens intresse av fortsatt uppkoppling skall kunna beaktas. Normalt torde en bedömning av om uppsägningen är oskälig förutsätta att abonnenten informeras om att en uppsägning kan bli aktuell på grund av att uppkopplingen använts för att begå upphovsrättsintrång. Abonnenten har då getts en möjlighet att vidta åtgärder för att förhindra framtida intrång (Ds 2007:29 s. 367).

Fullgörs inte den ovan beskrivna skyldigheten föreslås som enda sanktionen att en domstol, på talan av rättighetsinnehavaren eller den som på grund av upplåtelse har rätt att utnyttja verket, skall kunna förelägga den som tillhandahåller tjänsten att ”vidta de åtgärder som skäligen kan begäras” för att denne skall uppfylla dessa skyldigheter (ibid). Enligt författningskommentaren skall ett föreläggande även kunna avse mindre ingripande åtgärder, t.ex. nedsättning av uppkopplingshastigheten (Ds 2007:29 s. 367 f.).

Vid bedömningen av det skett ett omfattande och systematiskt intrång kan enligt utredningen alla intrång som skett i de rättigheter som tillkommer en rättighetshavare i den taleberättigade kretsen beaktas, dvs. även sådana rättigheter som tillkommer någon annan än den som för talan (ibid). Hur en sådan prövning skall kunna ske utan att någon styrker att verket är skyddat och att rättighetshavaren motsätter sig utnyttjandet etc. framgår inte närmare av förslaget.

En Internetleverantör skall vara skyldig att underrätta innehavaren av accessavtalet om att en talan om föreläggande har väckts.

4. Allmänna kommentarer

De ovan beskrivna förslagen skall ses mot bakgrund av att upphovsrättsinnehavare har stora och i många fall växande svårigheter att komma tillrätta med intrång som sker genom fildelning mellan enskilda användare på Internet. Den straffrättsliga vägen med polisanmälningar mot anonyma användare som begär intrång har visat sig svårframkomlig. En förklaring till detta är att polis och åklagare har bristande resurser och inte kan prioritera denna typ av brott. En annan förklaring är att det har visat sig svårt att få fällande domar i denna typ av mål. Detta beror i sin tur på att straffvärdet för intrång som rättighetshavarna, när moderna fildelnings-

tekniker används, kan koppla till en viss abonnent anses vara lågt. Följden blir att de straffprocessuella tvångsmedel som skulle behöva användas för att säkra den bevisning som krävs för en fällande dom inte kan tillgripas (se Westman, *Bevisfrågor vid upphovsrättsintrång genom fildelning m.m.*, Lov&Data nr. 88, 2006, s. 36 ff.).

Företrädare för film- och skivbolag framhåller mot denna bakgrund att det är naturligt att accessleverantörer ”tar ett större ansvar”. Vad som menas med detta är inte alltid helt klart, men vid sidan av regler av det slag som har beskrivits ovan, kan det handla om att ändra reglerna om accessleverantörernas frihet från straff- och skadeståndansvar (de s.k. ansvarsfrihetsreglerna i e-handelsdirektivet, 2000/31/EG). Som skäl för att ålägga accessleverantörer nya skyldigheter anförs främst att dessa har *faktiska möjligheter* att stoppa pågående intrång och att identifiera abonnenter vars uppkopplingar används för att begå intrång. Ibland anges även att accessleverantörerna *tjänar pengar* på de pågående intrången genom att de säljer bredbandsuppkopplingar med höga överföringskapaciteter som behövs för att ladda ner och sprida skyddade verk. Accessleverantörerna brukar å sin sida påpeka att de inte kan och av integritetsskäl inte får övervaka om deras användare begår upphovsrättsintrång. Leverantörerna brukar också invända att de inte har kompetens eller legitimitet att ta ställning till kvalificerade bedömningsfrågor när det gäller vad som utgör upphovsrättsintrång. De framhåller vidare att höga överföringskapaciteter även behövs för att utnyttja legala film- och musiktjänster och att de själva ofta driver sådana tjänster som de vill att deras kunder i första hand skall använda.

Med utgångspunkt i det befintliga upphovsrättssystemet kan det te sig naturligt att införa de regler som föreslås i departementspromemoriorna. Sveriges internationella åtagande kan även tala för att förslagen genomförs. Artikel 1 i sanktionsdirektivet kräver t.ex. att medlemsstaterna tillhandahåller ”de åtgärder, förfaranden och sanktioner” som är nödvändiga för att säkerställa skyddet för immateriella rättigheter. När det gäller föreläggande mot Internetoperatörer som går ut på att stoppa en användares pågående intrång finns det en skyldighet för medlemsstaterna enligt artikel 8.3 i infosoc-direktivet att införa regler som gör det möjligt för rättighetshavare ”att begära ett föreläggande gentemot mellanhänder vars tjänster utnyttjas av en tredje part för att begå intrång” i upphovsrätten. Lagrådet har ifrågasatt om Sverige fullgjort sina åtaganden i detta hänseende (prop. 2004/05:110 s. 563 ff.).

Vid prövningen av om de här behandlade förslagen bör genomföras är det emellertid inte tillräckligt att konstatera att rättighetshavarnas har ett *behov* av att på något sätt komma till rätta

med pågående intrång som sker genom olaglig fildelning. Inte heller är det tillräckligt att konstatera att accessleverantörer *kan* blockera Internettrafik och ofta har information som kan användas för att identifiera den som har begått intrång online. Förslagen aktualiserar förhållandet till grundläggande anspråk på rättssäkerhet och rätten till yttrandefrihet och till privat- och familjeliv enligt t.ex. Europakonventionen. Ett krav på uppsägning av ett Internetabonnemang innebär exempelvis att en eller flera personers möjlighet att kommunicera begränsas genom myndighetsingripande. Ett informationsföreläggande mot en accessleverantör innebär att tredje man ges möjlighet att kartlägga användares kommunikation på nätet på ett sätt som anses utgöra intrång i dennes privatliv. Detta innebär bl.a. att det måste prövas om de föreslagna reglerna är *nödvändiga* i ett demokratiskt samhälle för att uppnå vissa godtagbara syften. Eftersom skydd för upphovsrätten kan utgöra ett sådant godtagbart syfte kommer fokus i detta sammanhang främst att riktas mot frågan om ingreppen är proportionerliga. En proportionalitetsbedömning måste göras både när de begränsande reglerna utformas och när de tillämpas.

Det kan påpekas att de internationella åtagandena inom immaterialrätten inte ger anledning till en annan bedömning. Reglerna om informationsföreläggande i artikel 8 sanktionsdirektivet är till skillnad från de föreslagna svenska reglerna begränsande till krav på information i en pågående process. Dessutom anges att regler om informationsföreläggande inte påverkar andra lagbestämmelser, t.ex. sådana som ”reglerar sekretesskydd för informationskällor eller behandling av personuppgifter”. Enligt artikel 1 skall åtgärder, förfaranden och sanktioner som medlemsstaterna inför vara ”rättvisa och skäligen, inte onödigt komplicerade eller kostsamma och inte medföra oskäligen tidsfrister eller omotiverade dröjsmål”. De skall också vara ”effektiva, proportionella och avskräckande” och ”tillämpas så att hinder för lagenlig handel inte uppkommer och så att missbruk inte sker”. På samma sätt kan det framhållas att artikel 8.3 i infosoc-direktivet inte kräver att regler om föreläggande mot accessleverantörer av just det här föreslagna slaget införs. I detta direktivs ingress (p. 59) anges t.ex. att villkoren och bestämmelserna för föreläggande mot mellanhänder bör bestämmas av medlemsstaterna själva. Rent allmänt gäller att krav i EG-direktiv måste vara förenliga med grundläggande fri- och rättigheter. Detsamma gäller för de regler som genomför direktivet i nationell rätt.

Frågan om de föreslagna reglerna utgör nödvändiga begränsningar i t.ex. rätten till privatliv eller yttrandefriheten kan inte besvaras fullständigt här. Denna fråga är i grunden politisk, även om den i slutänden kan komma under en domstols prövning. Syftet med den fortsatta framställningen är främst att uppmärksamma de praktiska konsekvenserna av de föreslagna

reglerna och att bedöma dessa konsekvenser med utgångspunkt i kraven på rättssäkerhet, skydd för yttrandefriheten och skyddet för privat- och familjelivet (inklusive skyddet för personuppgifter). Därmed ges ett förbättrat underlag för den politiska och rättsliga bedömningen av om reglerna är proportionerliga. I sammanhanget finns det anledning att erinra om Integritetsskyddskommittén kritik mot att effekterna för den personliga integriteten sällan utreds och redovisas när ny lagstiftning föreslås (se SOU 2007:22, *Skyddet för den personliga integriteten*, s. 445 ff.).

Innan jag kommenterar de aktuella förslagen var och en för sig finns det anledning att framföra två övergripande synpunkter.

Den första är att de problem som utredningarna försöker lösa genom sina förslag *inte är speciella för immaterialrätten*. Även den som t.ex. har blivit lurad av en anonym säljare på nätet har ett behov av att kunna identifiera denne för att kräva tillbaka sina pengar i domstol. På samma sätt kan den som utsatts för förtal på nätet ha ett intresse av att den användare som gjort sig skyldig till förtålet får sin uppkoppling blockerad. Dessa möjligheter finns inte idag. Varför skall lagstiftaren tillmötesgå bara upphovsrättsinnehavarnas intressen av nya sanktioner? (Jfr E.I.P.R. 2003, 25(10), 447-449, där ett antal akademiker med immaterialrätt som specialitet riktar kritik mot det då föreliggande förslaget till sanktionsdirektiv bl.a. på denna grund.)

Jag menar att frågan om undantag från accessleverantörers tystnadsplikt och frågan om skyldigheterna att avbryta eller filtrera en Internetuppkoppling åtminstone bör övervägas i ett bredare sammanhang. Jag tror att dessa komplexa frågor, som aktualiserar flera olika intressen och grundläggande rättigheter, skulle få en mer allsidigt belysning ur såväl faktisk som rättslig synpunkt om de hanterades som något annat än rent immaterialrättsliga frågor. Varför inte överväga om dessa frågor bör få en mer generell lösning i lagen om elektronisk kommunikation eller möjligtvis i rättegångsbalken? Personligen är jag inte säker på att ett lagstiftningsärende i en sådan kontext hade lett fram till samma förslag, bl.a. av det skälet att avvägningen mellan intressena tenderar att skifta beroende på sammanhanget de görs i.

Det finns för det andra problem förknippade med användningen av civilrättsliga sanktioner mot en tillhandahållare av accesstjänster i syfte att *komma tillrätta med tredje mans olagliga kommunikation*. Det förhållandet att ett eventuellt föreläggandena prövas i en rättegång där

rättighetshavaren och accessleverantören är parter leder till vissa rättssäkerhetsproblem för den enskilda användaren som i huvudsak får vidkännas konsekvenserna av ett föreläggande (jfr Ds 2007:29 s. 356). Det blir t.ex. svårt för domstolen att göra en korrekt prövning av om ett intrång – ens i objektiv mening – verkligen har skett och av om ett föreläggande är proportionerligt i det enskilda fallet. I allmänhet har accessleverantörerna inte kunskap om alla förhållanden som är relevanta för en prövning. Det går inte heller att räkna med att leverantören alltid har en vilja att i abonnentens intresse argumentera emot ett föreläggande. Att vara part i en domstolsprocess är som bekant inte billigt. Detta kan sammantaget leda till att tillämpliga inskränkningar i ensamrätten, avtalsförhållanden som gör tillgängliggörandet tillåtet, försök till vilseledande om rättigheter eller faktorer som gör föreläggande i det enskilda fallet oproportionerligt inte blir kända för domstolen. Även om problem av detta slag bara är aktuella i enstaka situationer är det viktigt att en ordning med föreläggande mot accessleverantörer innehåller tillräckliga garantier för användarens rättssäkerhet (se vidare nedan för konkreta exempel).

Ett visst skydd skapas genom att en enskild användare kan ha rätt att *intervenera* i en process som rör en begäran om föreläggande. Förslaget till förelägganden om uppsägning av abonnemangsavtalet etc. innehåller som nämnts en uttrycklig skyldighet för accessleverantören att underrätta abonnenten om att talan om föreläggande har väckts. Att intervenera i ett ärende är emellertid inte helt okomplicerat för en privatperson. En intervention innebär dessutom att personen förlorar det skydd som tystnadsplikten i lagen om elektronisk kommunikation är tänkt att ge. En intervention i ett ärende om informationsföreläggande blir av förklariga skäl tämligen meningslös, eftersom intervenientens identitet då blir känd. Men även en intervention för att få behålla sin uppkoppling kan vara mindre tilltalande, eftersom detta innebär beteenden som registrerats på nätet därmed kommer att kunna hänföras till intervenienten. Man kan hävda att detta inte är något problem ”om man inte har något att dölja”, men det är som bekant inte det synsätt som ligger bakom regler som skyddar privatlivet i allmänheten och personuppgifter i synnerhet.

Ingripande mot tredjeman för att komma tillrätta med olaglig kommunikation kan även resa *principiella betänkligheter* sett i ett yttrandefrihetsperspektiv. En jämförelse kan göras med det synsätt som ligger till grund för den svenska tryck- och yttrandefrihetsregleringen, där ingripanden mot distributörer av det skyddade yttrandet i princip är förbjudna. Detta gäller trots att distributörerna i dessa fall medverkar till intrånget i objektiv (och kanske även sub-

jektiv) mening. Upphovsrätten är visserligen uttryckligen undantagen från tryckfrihetsförordningens (TF) och yttrandefrihetsgrundlagens (YGL) exklusiva tillämpningsområde (1 kap. 8 § TF och 1 kap. 12 § YGL), men det innebär inte att de yttrandefrihetsintressen som motiverat regleringen i grundlagarna är helt frånvarande i dessa sammanhang. Dessutom är det oklart hur långtgående begränsningar i yttrandefriheten som kan accepteras med hänvisning till undantaget för upphovsrätten i grundlagarna. Ett föreläggande om att en uppkoppling till internet skall avbrytas begränsar ju alla typer av yttranden, inte bara sådana som utgör upphovsrättsintrång. Även informationsfriheten, dvs. friheten att utan hinder från det allmänna inhämta information, begränsas genom ett sådant föreläggande. Det måste alltså även prövas om denna begränsning är proportionerlig.

5. Särskilt om informationsföreläggande

Ett informationsföreläggande skulle, i det sammanhang som här diskuteras, innebära att personuppgifter om en abonnent skulle lämnas ut till en rättighetshavare. Därmed aktualiseras framförallt reglernas förhållande till skyddet för den personliga integriteten. En fråga som berör detta förhållande är om reglerna om informationsföreläggande är förenliga med framför allt skyddet för privatlivet i Europakonventionen och regler om personuppgiftsskydd i dataskyddsdirektivet (1995/46/EG) och direktivet om integritet och elektronisk kommunikation (2002/58/EG). En annan fråga är mer rättspolitisk och handlar om hur intresset av en effektiv upphovsrättslig ensamrätt skall vägas mot det ingrepp i privatlivet som sker genom föreläggandet. Om informationsförelägganden mot accessleverantörer principiellt anses godtagbara återstår frågorna kring hur reglerna skall utformas för att säkerställa att ingreppet i den personliga integriteten blir proportionerligt i det enskilda fallet.

Av betydelse för förhållandet till integritetsskyddet är hur de uppgifter som skulle kunna bli föremål för ett utlämnande betraktas. Personuppgifter som är hänförliga till elektronisk kommunikation är olika känsliga ur integritetssynpunkt. Känsligast anses ofta uppgifter om kommunikationens innehåll vara. Men även s.k. trafikuppgifter, dvs. sådana uppgifter som behandlas i syfte att överföra ett meddelande, t.ex. uppgifter om sändare, mottagare och tidpunkt, anses känsliga. Detta bl.a. eftersom de kan användas för att spåra kommunikation och kartlägga kommunikationsmönster. Minst känsliga anses abonnentförteckningar vara, men även sådana aktualiserar vissa integritetsaspekter.

I en traditionell telefonmiljö är gränsdragningar mellan dessa kategorier tämligen klara. Men hur skall uppgiften om vem som vid en given tidpunkt var innehavare av en viss IP-adress betraktas? Ett möjligt synsätt är att det rör sig om samma låga känslighetsgrad som en uppgift om vem som innehar ett visst telefonnummer. Enligt min mening haltar en sådan liknelse, bl.a. eftersom de båda kommunikationsmiljöerna i övrigt är så olika. Internetkommunikation är så mycket mer än överföring av tal mellan två personer. Därtill kan lägga att en abonnent när det gäller traditionell telefoni enkelt kan välja att dölja sitt nummer för den uppringde, medan detta är mycket komplicerat eller omöjligt i en Internetmiljö. Synen på de här aktuella uppgifterna bör mot denna bakgrund inte göras med utgångspunkt i enkla liknelser från telefonivärden, kombinerat med en analys av befintliga rättsliga begrepp, utan med utgångspunkt i en mer allmän bedömning av vad de aktuella uppgifterna skapar för möjligheter att kartlägga den aktuella personen. En sådan analys visar tydligt att tillgång till uppgifter om vem som vid en viss tidpunkt innehade ett visst IP-nummer kan användas för att omfattande kartläggningar av personens beteenden. I sammanhanget kan det även vara betydelsefullt att ta hänsyn till användarnas förväntningar om anonymiteten och spårbarheten är i denna miljö, eftersom detta påverkar deras beteenden. En närmare undersökning av detta slag skulle enligt min mening visa att skyddsbehovet när det gäller den här diskuterade typen av personuppgifter är stort.

(Jfr nedan om generaladvokatens klassificering av denna typ av uppgifter som trafikuppgifter i personuppgiftsdirektivens mening. Se även Ds 2005:6, *Brott och brottsutredningar i IT-miljö*, s. 322 ff., om hur denna typ av uppgifter bör klassificeras enligt lagen om elektronisk kommunikation, men jfr för en avvikande uppfattning i detta hänseende SOU 2005:38, *Tillgång till elektronisk kommunikation i brottsutredningar m.m.*, s. 131.)

När det gäller Sveriges möjligheter att införa regler om informationsföreläggande riktat mot accessleverantörer är en kommande dom från EG-domstolen av avgörande betydelse (se mål C-275/06).

Generaladvokaten har i ett omfattande förslag till dom funnit att en överföring av personrelaterade trafikuppgifter till andra än behöriga myndigheter skulle stå i strid gemenskapsrättsliga bestämmelser om personuppgiftsskydd, framförallt direktivet om integritet och elektronisk kommunikation. Generaladvokaten konstaterar att de immaterialrättsliga direktiven, t.ex. sanktionsdirektivet, inte påverkar lagstiftningen om personuppgiftsskydd (p. 42-49). Ett utlämnande av uppgifter direkt till rättighetshavare träffas av direktivet om integritet och elek-

tronisk kommunikations regler om konfidentialitet och förbud mot behandling av *trafikuppgifter* (p. 57-64). Inga av de befintliga undantagen från dessa regler och förbud anses heller vara tillämpliga (p. 67-121).

Även om EG-domstolens gör en annan bedömning än vad generaladvokaten gjort innebär det inte automatiskt att det svenska förslaget om informationsförelägganden mot accessleverantörer är förenligt med EG-rätten.

För det första går det svenska förslaget om informationsföreläggande längre än vad sanktionsdirektivet kräver, vilket har betydelse om EG-domstolen skulle finna att sanktionsdirektivet har företräde framför direktivet om integritet och elektronisk kommunikation.

För det andra innehåller det s.k. datalagringsdirektivet (2006/24/EG), som inte var gällande vid tidpunkten för talans väckande i det aktuella målet, i artikel 4 en bestämmelse som innebär att medlemsstaterna skall tillse att trafikuppgifter som lagras i enlighet med direktivet ”endast görs tillgängliga för behöriga nationella myndigheter, i närmare angivna fall och i enlighet med nationell lagstiftning”. Denna bestämmelse synes hindra informationsföreläggande av det föreslagna slaget (jfr dock diskussionen ovan om vad som utgör en ”trafikuppgift”).

För det tredje återstår den övergripande frågan om de föreslagna reglerna är förenliga med det grundläggande skyddet för privat- och familjelivet i artikel 8 i Europakonventionen. Ett utlämnande av uppgifter om enskilda personers kommunikation till tredje man utgör i enlighet med Europadomstolens praxis utan tvekan ett ingrepp i rätten till privatliv enligt artikel 8 första stycket. Ett sådant ingrepp får enligt artikel 8 andra stycket bara ske ”med stöd av lag och om det i ett demokratiskt samhälle är nödvändigt med hänsyn till den nationella säkerheten, den allmänna säkerheten eller landets ekonomiska välstånd, till förebyggande av oordning eller brott, till skydd för hälsa eller moral eller till skydd för andra personers fri- och rättigheter”. En prövning av dessa förhållanden är som framhållits ovan i hög grad rättspolitisk och kräver mer utrymme än vad som här står till buds. Jag skall därför nöja mig med att peka på ett resonemang som generaladvokaten för i det ovan nämnda förslaget till dom som är relevant när en sådan prövning skall göras (p. 112-115). Där framhålls att utlämnande av personrelaterade trafikuppgifter till myndigheter för att möjliggöra såväl civilrättsliga som straffrättsliga åtgärder mot intrång i upphovsrätten är ett mildare ingrepp, som samtidigt säkerställer att ut-

lämnande är rimligt i förhållande till de skyddade rättigheterna. Statliga myndigheter är bundna av de grundläggande rättigheterna och måste särskilt beakta processuella garantier. Därutöver beaktar de normalt även omständigheter som befriar den användare som har anklagats för intrång i upphovsrätten från ansvar. Som exempel nämns att det faktum att ett intrång har skett från ett visst abonnemang inte med nödvändighet innebär att det är abonnemangsinnehavaren som har begått intrånget. Det kan t.ex. finnas ett öppet trådlöst nätverk som gör att tredje man kan använda uppkopplingen. Upphovsrättsinnehavaren har, enligt generaladvokaten, till skillnad från statliga myndigheter inte något intresse av att beakta eller reda ut sådana omständigheter.

Utan att föregripa en fullständig proportionalitetsprövning och EG-domstolens slutliga dom kan det konstateras att det snarare verkar vara så att de befintliga nationella reglerna om edition och intrångsundersökning behöver analyseras närmare (och kanske omprövas) i ljuset av Europakonventionens skydd för privatlivet och EG:s personuppgiftsdirektiv, än att dessa regler kan tas till intäkt för att informationsföreläggande vad avser personuppgifter kan införas utan problem i svensk rätt.

Finns det något alternativ till informationsföreläggande som säkerställer att rättighetshavare kan försvara sina rättigheter civilrättsligt vid intrång genom fildelning och som är samtidigt förenligt med de ovan behandlade reglerna och intressena? En *möjlig* lösning, som tillämpas i Förenta staterna, är att rättighetshavarna stämmer en anonym användare. Uppgifterna från accessleverantören överlämnas till domstol, som efter att bevisning framlagts och den tilltalade svarat anonymt, kan besluta om anonymiteten skall hävas. En fördel med en sådan ordning är att den som innehar abonnemanget blir part i målet och kan argumentera emot ett utlämnande. Inte heller en sådan ordning är emellertid problemfri. I Förenta staterna finns det kritik mot att organisationer som företräder rättighetshavarna utnyttjar discovery-institutet för att identifiera användaren innan denne har hunnit inkomma med svaromål i tvistemålet. För svensk del skulle en ordning av detta slag ställa krav på vissa processrättsliga nyordningar. Ett problem sett i rättighetshavarnas perspektiv är vidare att den abonnent som får veta att han eller hon är stämd kan undanskaffa sådan bevisning i sin dator som kan behövas för att intrång skall kunna styrkas (se vidare nedan).

En möjlig rättspolitisk ståndpunkt är naturligtvis också att integritetsintresset och risken för missbruk gör det olämpligt att över huvudtaget tillhandahålla civilrättsliga instrument för att identifiera Internetanvändare.

Jag övergår nu till att uppmärksamma några mer *konkreta* problem med förslaget om informationsföreläggande mot accessleverantörer.

Föreläggande mot tredje man kan som framhållits ovan vara problematiska ur rättsäkerhets-synpunkt. Det finns t.ex. en risk för att reglerna om informationsföreläggande *missbrukas* i syfte att identifiera och kartlägga en anonym meningsmotståndare som yttrat sig på nätet eller en skyddad uppgiftslämnare. Detta kan göras genom att dokument som visar att upphovsrättsligt skyddade verk gjorts tillgänglig från en IP-adress fabriceras. För en domstol kan vilseledandet vara svårt att upptäcka och i efterhand kan det vara omöjligt att styrka att en sådan bevisning beträffande aktuella aktiviteter på nätet vid en viss tidpunkt är förfalskade. Ett sätt att i någon mån minska riskerna för denna typ av missbruk är givetvis att kräva att bevisningen om ett intrång måste se ut på visst sätt, t.ex. komma från en oberoende tredje part. Man också tänka sig att krav på att sökande ställer säkerhet för att ett informationsföreläggande skall kunna meddelas.

Ett annat förhållande som det finns anledning att uppmärksamma är att det enligt förslaget krävs att intrånget är *styrkt* för att ett informationsföreläggande skall kunna meddelas. Kravet är tänkt som en rättssäkerhetsgaranti. Att styrka ett intrång – ens i objektiv mening – utan att den som tillgängliggör verket är identifierad är emellertid normalt sett omöjligt. Hur kan domstolen t.ex. veta att den som tillgängliggör verket inte har rätt att göra det enligt en inskränkning i ensamrätten eller enligt ett avtal? Skall rättighetshavarens påstående om generell frånvaro av licenser innebära att intrånget är styrkt? Min slutsats är att beviskravet för att reglerna överhuvudtaget skall kunna tillämpas skulle behöva sänkas, men då aktualiseras återigen frågan om rättssäkerhet och proportionalitet.

Jag har i andra sammanhang framhållit att det är rimligt att immaterialrättsinnehavare – i enlighet med allmänna regler för *personuppgiftsbehandling* – har rätt att behandla personuppgifter i syfte att beivra intrång i sina rättigheter (se Westman, *Personuppgiftslagen och kampen mot piratkopiering*, Lov&Data nr. 84 2005, s. 7 ff.). Mot denna bakgrund kan det föreslagna undantaget från 21 § personuppgiftslagen te sig rimligt. Det framstår som naturligt att rättig-

hetshavare som på ett mer omfattande och systematiskt sätt bedriver spaning, t.ex. för att göra polisanmälningar, inte alltid skall vara beroende av ett individuellt undantag från Datainspektionen. Samtidigt menar jag att det hade varit lämpligare med en mer generell lösning av privata subjekts rätt att behandla uppgifter om lagöverträdelse i syfte att tillvara ta sina rättigheter. Även här aktualiseras alltså frågan om varför just immaterialrättsinnehavare skall särbehandlas i jämförelse med andra subjekt som också har ett behov att kunna behandla denna typ av uppgifter. En allmän översyn av 21 § personuppgiftslagen eller åtminstone Datainspektionens föreskrifter med undantag från 21 § är av detta skäl mer tilltalande lösningar (jfr dock Personuppgiftslagsutredningens bedömningar i detta hänseende i SOU 2004:6, *Översyn av personuppgiftslagen*, s. 173 ff.).

I departementspromemorian görs bedömningen att inga särskilda regler om *ansvar för missbruk* av sådan information som en rättighetshavare skall kunna erhålla med stöd av ett informationsföreläggande behövs. Skälet för denna slutsats är att reglerna i personuppgiftslagen anses ge ett tillfredsställande skydd för uppgifterna (Ds 2007:19 s. 196 ff.). I sammanhanget skall dock påpekas att personuppgiftslagen endast gäller behandling av personuppgifter som sker i viss form (jfr 5 §). Det är därför inte givet att lagen *alltid* är tillämplig på rättighetshavarens hantering av uppgifterna. Detta förhållande bör beaktas när fråga om särskilda regler om ansvar för missbruk av informationen övervägs.

Det är, som har framhållits i andra sammanhang, långt ifrån säkert att den information som skulle erhållas genom ett informationsföreläggande är tillräcklig för att en rättighetshavare ska kunna vinna bifall till en skadeståndsrättslig talan mot den abonnent som identifierats (se Westman, *Bevisfrågor vid upphovsrättrinrång genom fildelning m.m.*, Lov&Data nr. 88 2006, s. 39). Uppgifterna om abonnenten kan emellertid komma att användas för att sända varningsbrev, eventuellt i kombination med krav på ersättning för de intrång som har begåtts genom den aktuella anslutningen.

6. Särskilt om föreläggande om uppsägning av Internetabonnemang etc.

Förslaget som syftar till att förhindra intrång som sker genom användande av en accessleverantörens tjänster består av två delar. För det första ges accessleverantörerna ”en rätt och en skyldighet” att under vissa betingelser ”med omedelbar verkan säga upp ett avtal om användning av sina tjänster”. Denna skyldighet sanktioneras för det andra genom att en domstol kan utfärda ett föreläggande mot accessleverantören.

Det finns mot denna bakgrund anledning att inledningsvis överväga om det är lämpligt att ålägga accessleverantörer en skyldighet att agera mot sina kunder redan *utan ett domstolsföreläggande*. Problemet med en sådan ordning är, enligt min mening, att accessleverantören i praktiken blir helt utlämnad till information som tillhandahålls av någon som påstår sig ha blivit utsatt för ett intrång. Accessleverantören har nämligen själv stora *faktiska svårigheter* att kontrollera vad tjänsten används till, samtidigt som *rättsregler* om personuppgiftsbehandling och regler om konfidentialitet i kommunikationen i stor utsträckning gör en sådan kontroll olaglig. Avlyssning är naturligtvis uteslutet både av praktiska och rättsliga skäl. Den enda kontroll som accessleverantören rent faktiskt kan utföra utan avlyssning är en ”bakvägssökning” efter IP-nummer som man själv administrerar i publika tjänster som kan användas för tillgängliggörande i strid med upphovsrätten. Antalet sådana tjänster är emellertid mycket stort och en sådan övervakning skulle kräva mycket avancerad personuppgiftsbehandling vars laglighet kan ifrågasättas. Dessutom är det svårt för accessleverantörerna att veta vad de skall leta efter. Huruvida en fil som påträffas utgör intrång i en tredjemans upphovsrätt framgår inte alltid, vare sig för en människa eller för ett automatiskt system. Det är dessutom ofta svårt att i efterhand kontrollera en anmälares påstående om att vissa filer vid en viss tidpunkt har gjorts tillgängliga i strid med upphovsrätten via moderna fildelningsnätverk av BitTorrent-typ.

Det skall i sammanhanget noteras att accesstjänster när det gäller de faktiska och rättsliga förutsättningarna för kontroll helt skiljer sig från värdtjänster eller elektroniska anslagstavlor (t.ex. webbhotell eller forum). Sådana tjänster innebär att användarna ges möjlighet att ladda upp material som blir omedelbart tillgängligt för andra användare, inklusive tjänstetillhandahållaren. I dessa situationer kan alltså tjänstetillhandahållaren, efter en underrättelse från en rättighetshavare, kontrollera och avlägsna det om det bedöms vara olagligt utan några större faktiska eller rättsliga problem (även här finns det emellertid problem med själva bedömningen av om material som har skickats in till tjänsten verkligen utgör intrång i någons upphovsrätt).

Det tycks inte vara utredningens avsikt att införa några nya rättigheter eller skyldigheter för accessleverantören att övervaka sina kunder skall införas. Sådana skyldigheter skulle i de flesta fall strida mot artikel 15 i e-handelsdirektivet, som förskriver en frånvaro av övervaknings-skyldighet för t.ex. accessleverantörer. Åtminstone i de fall där det handlar om fildelning mellan enskilda användare blir konsekvensen därmed att en accessleverantör antingen kan välja

att agera baserat på den information som erhålls från påstådda rättighetshavare eller välja att avvakta ett eventuellt domstolsföreläggande. I det första fallet finns det stora rättssäkerhetsproblem för accessleverantörens kunder. I det andra fallet är inte mycket vunnet på att införa skyldigheten att agera även utan ett domstolsföreläggande. Förslaget tycks bygga på en vag förhoppning om att accessleverantörerna "frivilligt skall göra något", men frågan är vad de rättsligt och faktisk kan göra. Att införa generella skyldigheter agera mot användarna av tjänsten, utan att det finns praktiska och rättsliga möjligheter att fullgöra dem i en bråkdel av alla fall där skyldigheten aktualiseras, är inte ägnat att stärka förtroendet för lagstiftningen som instrument för att motverka upphovsrättsintrång.

Den enda rättssäkra åtgärden, som jag för närvarande ser, att accessleverantörer skulle kunna vidta utan ett föreläggande i det enskilda fallet, kanske efter en justering av reglerna om behandling av personuppgifter om lagöverträdelse, är att vidarebefordra "varningsbrev" som rättighetshavare skickar. Om lagstiftaren önskar att detta skall ske bör istället en uttrycklig vidarebefordringsskyldighet införas. Införs ett sådant krav bör det övervägas vem som skall bära kostnaderna för hanteringen.

Ett argument för att ålägga accessleverantörer att agera även utan ett föreläggande utfärdats har varit att accessleverantören, oavsett det individuella abonnemangsavtalets innehåll, därmed erhåller en sådan rättslig rådighet som enligt allmänna principer är ett krav för att vite skall kunna föreläggas. En sådan rådighet borde emellertid, som jag ser det, kunna åstadkommas även på andra sätt, t.ex. genom en uttrycklig regel som säger att accessleverantören har en rätt och en skyldighet att bryta avtalet om en domstol utfärdar ett föreläggande. Det är svårt att se att de grundläggande principerna om viten skulle vara av den karaktären att de hindrar lagstiftaren från en sådan lösning.

När det gäller den andra delen av förslaget, dvs. möjligheterna för en domstol att besluta om *förelägganden mot accessleverantörerna*, aktualiseras frågan om proportionalitet mellan intrånget och föreläggandets effekt. Utredningen är väl medveten om att förslaget är känsligt i detta hänseende och har därför som framgått ovan på olika sätt försökt begränsa förslagets tillämpningsområde och effekt. Detta framgår t.ex. genom förslagets begränsning till tillgängliggörande för allmänheten i strid med upphovsrätten, genom kravet på upprepade intrång, genom kravet på att intrånget kan antas fortsätta och genom att situationen hos mottagaren skall beaktas vid föreläggandets utformning.

Utredningens ambitioner i dessa delar är lovvärda, men enligt min mening kvarstår betydande problem. Ett föreläggande inom immaterialrätten innebär normalt ett förbud mot att fortsätta med ett intrångsgörande utnyttjande av vissa utpekade skyddade prestationer. Det aktuella förslaget innebär emellertid att tredje man kan föreläggas att avbryta eller begränsa en generell kommunikationstjänst på ett sätt som inte alls är kopplat till fortsatt förfogande över just de skyddade prestationerna som utgör själva grunden för förelägandet. Genom att kopplingen mellan den intrångsgörande handlingen och sanktionen är så vag får den föreslagna regleringen karaktären av *straff eller särskild rättsverkan med anledning av brott*. Ett grundkrav skulle därmed vara att normala rättsäkerhetsgarantier t.ex. när det gäller krav på bevisningen och när det gäller processuella rättigheter tillämpas, något som inte är fallet enligt förslaget.

Accesstjänster får allt mer karaktären av grundläggande tjänster som medborgarna behöver för att kunna utföra en mängd olika aktiviteter i sin vardag. Flera användare i ett hushåll kan dessutom vara beroende av en fungerande uppkoppling till Internet. Dessa förhållande skall enligt utredning beaktas vid bedömningen av om ett föreläggande skall utfärdas. Frågan är emellertid om inte lagstiftaren vid en mer abstrakt proportionalitetsbedömning borde kunna konstatera att utrymmet för att meddela föreläganden när det gäller denna typ av tjänster är så begränsat att regleringen av principiella skäl är tveksam.

I sammanhanget bör det särskilt beaktas att accesstjänst i de allra flesta fall, åtminstone till någon del, används för att sprida yttranden som omfattas av skyddet för yttrandefriheten. Ett domstolsföreläggande som har innebörden att en viss kanal för sådana yttrande skall stängas utgör en begränsning av yttrandefriheten. Europakonventionen kräver att nationella regler som begränsar yttrandefriheten skall stå i rimlig proportion till det godtagbara syfte som finns med att begränsa yttrandefriheten. Med hänvisning till vad som ovan anförts om kopplingen mellan intrånget i upphovsrätten till vissa skyddade verk och begränsningen i möjligheten att kommunicera är det tveksamt om så är fallet (jfr även ovan under 4).

En förutsättning för att ett föreläggande skall kunna meddelas är enligt förslaget att uppkopplingen ”*upprepade gånger har utnyttjats för att begå intrång*”. I samband med den olagliga fildelning mellan enskilda användare med t.ex. BitTorrent-teknik, mot vilket förslaget främst riktar sig, är det emellertid normalt svårt för rättighetshavarna att styrka att intrång vid två olika tidpunkter utförs av en och samma användare. Detta sammanhänger med att en användare

re kan få olika IP-adresser vid olika uppkopplingstillfällen. Resultatet blir därmed antingen att reglerna inte kommer att kunna tillämpas i de fall som utredningen förutsatt eller att domstolarna måste ställa kraven på återkommande intrång lägre än vad utredningen anger i promemorian, med de effekter detta får i proportionalitetshänseende.

Innan diskussionen om detta förslag avslutas finns det anledning att uppmärksamma att förelägganden mot accessleverantörer på ett principiellt plan även kan utformas på andra sätt. Accessleverantören skulle t.ex. kunna föreläggas att *hindra tillgängliggörandet av ett visst verk*. Detta ligger mer i linje med hur förbud inom immaterialrätten normalt utformas. Problemet är att en sådan lösning skulle kräva en enorm trafikövervakning, med påföljande kostnader och integritetsförluster. Samtidigt skulle riskerna vara stora för att verket skulle kunna ta sig igenom de filter som skulle införas, med påföljd att vitet skulle kunna dömas ut. För en accessleverantör skulle det vara enklare att istället säga upp abonnemanget. En annan lösning som har diskuterats är om accessleverantörer direkt skulle kunna åläggas att *använda viss filtreringsteknik*. I denna situation skulle accessleverantören kunna slippa bära risken för att filtreringen inte fungerar på ett tillfredställande sätt. Hur ett krav i ett enskilt fall på användningen av generella filter av detta slag skulle förhålla sig till frånvaron av övervakningsskyldighet i artikel 15 i e-handelsdirektivet är minst sagt oklart. Dessutom kan filtrering som bygger på en (teknisk) granskning av innehållet ses som en form av avlyssning. Den tekniska effektiviteten i dessa filtreringssystem skulle vidare innebära att inte alla intrång skulle blockeras. Samtidigt – och det är mer betänkligt – skulle systemen kunna innebära en ”överfiltrering” i förhållande till upphovsrätten. Exempelvis skulle systemen antagligen blockera filer som skickas mellan vänner som enligt upphovsrätten har rätt att göra verk tillgänglig för varandra och kopiera dessa för privat bruk. Generella filtreringssystem kan även innebära att trafik med vissa kommunikationsprotokoll som ofta används för fildelning direkt mellan enskilda användare blockeras. Även i sådana fall finns det naturligtvis ett proportionalitetsproblem eftersom fildelning i sig inte är olagligt. Denna korta utblick visar sammanfattningsvis att även andra typer av föreläggande är förknippade med betydande praktiska och rättsliga problem. Därmed inte sagt att dessa lösningar inte förtjänar att studeras närmare i syfte att försöka hitta acceptabla lösningar för att hindra fortsatta upphovsrättsintrång.

7. Avslutning

I det föregående har jag på flera punkter kritiserat de föreslagna reglerna för att de inte i tillräcklig utsträckning har utformats med beaktande av grundläggande regler om t.ex. rättssä-

kerhet, integritet och yttrandefrihet. Jag vill emellertid avslutningsvis framhålla att jag inte utesluter att det kan vara nödvändigt att på något sätt skärpa de civilprocessuella reglerna för att stärka rättighetshavarnas ställning i en digital miljö. Ett förslag om nya civilprocessuella regler måste dock placeras i ett vidare rättsligt och sakligt sammanhang än vad som gjorts i de nu aktuella utredningarna. Det krävs särskilt noggrannare utredning av möjligheterna att i praktiken tillämpa sådana regler utan att grundläggande fri- och rättigheter hotas (jfr Integritetsskyddskommitténs kritik mot att integritetseffekterna sällan behandlas närmare när ny lagstiftning föreslås, SOU 2007:22 s. 445 ff.).

Samtidigt skall det påpekas att Internetmiljön tenderar att skärpa motsättningen mellan olika intressen på ett sätt som inte sällan tvingar fram rättpolitiska val beträffande vilka intressen och värden som skall ges prioritet. Innan det konstateras att så är fallet när det gäller de här aktuella frågorna bör emellertid en djupare undersökning göras av om det finns lösningar som samtidigt beaktar alla de olika intressen som gör sig gällande. Det skulle t.ex. kunna handla om att tydligare integrera tekniska och rättsliga lösningar på de problem som finns.