I

(Resolutioner, rekommendationer och yttranden)

YTTRANDEN

EUROPEISKA DATATILLSYNSMANNEN

Yttrande från Europeiska datatillsynsmannenöver EU:s pågående förhandlingar om ett handelsavtal om åtgärder mot varumärkesförfalskning (Acta-avtalet)

(2010/C 147/01)

EUROPEISKA DATATILLSYNSMANNEN HAR AVGETT DETTA YTTRANDE

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 16,

med beaktande av Europeiska unionens stadga om de grundläggande rättigheterna, särskilt artikel 8,

med beaktande av Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter, ([1])

med beaktande av Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation, ([2])

med beaktande av Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter, ([3]) särskilt artikel 41.

HÄRIGENOM FRAMFÖRS FÖLJANDE.

I. INLEDNING

1. EU deltar i förhandlingarna om att ta fram ett handelsavtal om åtgärder mot varumärkesförfalskning (Acta-avtalet). Förhandlingarna inleddes 2007 av en grupp intresserade parter och fortsatte sedan med en större grupp deltagare. I dag deltar bland annat Australien, Kanada, EU, Japan, Sydkorea, Mexiko, Marocko, Nya Zeeland, Singapore, Schweiz och Förenta staterna i förhandlingarna. Rådet gav kommissionen mandat att delta i förhandlingarna 2008.

2. Europeiska datatillsynsmannen inser att gränsöverskridande handel med förfalskade och piratkopierade varor är ett växande problem. Handeln bedrivs ofta av organiserade kriminella nätverk och det krävs lämpliga samarbetsmekanismer på internationell nivå för att bekämpa den här formen av brottslighet.

3. Europeiska datatillsynsmannen menar att EU:s förhandlingar om ett multilateralt avtal som framförallt är tänkt att säkerställa skyddet av immateriella rättigheter väcker väsentliga frågor om hur de åtgärder som vidtas för att bekämpa varumärkesförfalskning och piratkopiering påverkar enskilda personers grundläggande rättigheter, framförallt rätten till personlig integritet och dataskydd.

4. Här beklagar Europeiska datatillsynsmannen framförallt att kommissionen inte har rådfrågat honom om innehållet i avtalet. Europeiska datatillsynsmannen har därför på eget initiativ och på grundval av artikel 41.2 i förordning (EG) nr 45/2001 antagit detta yttrande för att ge kommissionen råd om de integritets- och dataskyddsaspekter som den bör ta hänsyn till vid förhandlingarna om Acta-avtalet.

II. FÖRHANDLINGSLÄGE OCH PRELIMINÄRT INNEHÅLL I ACTA-AVTALET

5. Den sjunde förhandlingsomgången ägde rum i Mexiko den 26–29 januari 2010, med målsättningen att ingå ett avtal under 2010. Hittills har det dock inte offentliggjorts något officiellt förslag till avtal.

([1]) EGT L 281, 23.11.1995, s. 31.
([2]) EGT L 201, 31.7.2002, s. 37.
([3]) EGT L 8, 12.1.2001, s. 1.

6. Målet med förhandlingarna är att anta ett nytt multilateralt avtal för att bättre säkerställa skyddet av immateriella rättigheter och bekämpa varumärkesförfalskning och piratkopiering. Om det nya avtalet antas skulle det innebära förbättrade internationella normer för hur man ska hantera storskaliga intrång i de immateriella rättigheterna. Kommissionens generaldirektorat för handel har särskilt förklarat att man avser att koncentrera sig på varumärkesförfalskning och piratkopiering som påverkar kommersiella intressen och inte på vanliga medborgares förehavanden ([4]).

7. När det gäller avtalets innehåll framgår det av *Summary of key elements under discussion* som kommissionens generaldirektorat för handel offentliggjorde i november 2009 att man framförallt kommer att arbeta för att uppnå Acta-avtalets mål att bekämpa varumärkesförfalskning och piratkopiering med hjälp av tre metoder: i) internationellt samarbete, ii) brottsbekämpande åtgärder och iii) fastställandet av en rättslig ram för att säkerställa skyddet av immateriella rättigheter på flera specifika områden, framförallt i den digitala miljön ([5]). De planerade åtgärderna kommer framförallt att handla om rättsliga förfaranden (till exempel föreläggande, tillfälliga åtgärder), Internetleverantörernas roll och ansvar för att förhindra intrång i upphovsrätten på Internet och gränsöverskridande samarbetsåtgärder för att förhindra att varor förs över gränserna. Den offentliggjorda informationen ger emellertid bara en inblick i huvuddragen i avtalet och inte i några detaljer om specifika och konkreta åtgärder.

8. Europeiska datatillsynsmannen konstaterar att även om Acta-avtalets syfte endast är att koncentrera sig på storskaliga intrång i immateriella rättigheter går det inte att utesluta att Acta-avtalet kan komma att drabba vanliga medborgare, särskilt med tanke på att verkställighetsåtgärderna äger rum i den digitala miljön. Europeiska datatillsynsmannen betonar att det därför kommer att krävas lämpliga garantier för att skydda enskilda personers grundläggande rättigheter. Dataskyddslagstiftningen gäller dessutom alla individer, inklusive dem som eventuellt är inblandade i varumärkesförfalskning och privatkopiering. Bekämpningen av storskaliga intrång kommer därför säkert också att innefatta behandling av personuppgifter.

9. Europeiska datatillsynsmannen uppmanar därför kommissionen att inleda en offentlig och öppen dialog om Acta-avtalet, eventuellt i form av ett offentligt samråd, som också skulle bidra till att se till att de åtgärder som ska antas är förenliga med EU:s integritets- och dataskyddslagstiftning.

III. EUROPEISKA DATATILLSYNSMANNENS SYNPUNKTER

10. Europeiska datatillsynsmannen uppmanar EU, framförallt kommissionen som fått mandat att ingå avtalet, att hitta rätt balans mellan å ena sida kraven på skydd av immateriella rättigheter och å andra sidan enskilda personers rätt till integritets- och dataskydd.

11. Europeiska datatillsynsmannen betonar att integritets- och dataskydd är några av EU:s kärnvärden. De erkänns i artikel 8 i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna och i artiklarna 7 och 8 i Europeiska unionens stadga om de grundläggande rättigheterna ([6]) och måste respekteras i all politik och all lagstiftning som EU antar i enlighet med artikel 16 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget).

12. Vidare betonar Europeiska datatillsynsmannen att alla avtal som EU ingår om åtgärder mot varumärkesförfalskning ska vara förenliga med de rättsliga förpliktelser som EU har enligt integritets- och dataskyddslagstiftningen, framförallt direktiv 95/46/EG och direktiv 2002/58/EG ([7]), samt Europadomstolens ([8]) och EU-domstolens ([9]) rättspraxis.

13. Integritets- och dataskyddet ska beaktas redan när förhandlingarna inleds, inte när man redan har fastställt och kommit överens om ordningar och förfaranden och det därför är för sent att hitta alternativa lösningar som uppfyller integritetskraven.

14. Europeiska datatillsynsmannen konstaterar att han, på grund av den knapphändiga information som offentliggjorts, inte kan analysera de enskilda bestämmelserna i Acta-avtalet. Europeiska datatillsynsmannen kommer i detta yttrande därför att koncentrera sig på att beskriva hur de möjliga konkreta åtgärder som beskrivs i avtalet kan komma att hota integritets- och dataskyddet på följande två områden: säkerställandet av skyddet av immateriella rättigheter (kapitel IV) och internationella samarbetsmekanismer (kapitel V).

([4]) Se http://trade.ec.europa.eu/doclib/docs/2009/november/tradoc_145271.pdf, s. 2.

([5]) Se fotnot 2 ovan.

([6]) Europeiska unionens stadga om de grundläggande rättigheterna, EUT C 303, 14.12.2007, s. 1.

([7]) Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation), EGT L 201, 31.7.2002, s. 37.

([8]) Vid en tolkning av tillämpliga delar av de huvudsakliga aspekterna och villkoren i artikel 8 i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna som antogs i Rom den 4 november 1950. Se särskilt hänvisningarna till rättspraxis på andra ställen i detta yttrande.

([9]) Se särskilt dom av den 29 januari 2008 i mål C-275/06, Productores de Música de España (Promusicae), REG 2008, s. I-271, och beslut av den 19 februari 2009 i mål C-557/07, LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten, REG 2009, s. I-1227.

IV. SÄKERSTÄLLANDET AV SKYDDET AV IMMATERIELLA RÄTTIGHETER I DEN DIGITALA MILJÖN

IV.1 Behovet av att analysera hur åtgärderna för att stänga av Internetanvändare efter tre varningar påverkar integritets- och dataskyddet

15. Enligt kommissionen kommer Acta-avtalet att skapa en rättslig ram för att bekämpa piratkopieringen i den digitala miljön ([10]). Denna ram kommer att fastställa på vilka villkor Internetleverantörer och andra mellanhänder på Internet ([11]) kan ställas till svars för intrång i upphovsskyddat material som passerar deras nät. Ramen kan även föreskriva korrigerande och rättsliga åtgärder mot Internetanvändare som laddat upp eller ned upphovsrättsskyddat material. Även om det officiellt inte har offentliggjorts några detaljer om denna ram framgår det av den information som finns att Internetleverantörer kan åläggas att stänga av Internetanvändare efter tre varningar, vilket även kallas *graduated response*. Detta kommer att ge upphovsrättsinnehavarna möjlighet att övervaka Internetanvändare och identifiera personer som misstänks ha gjort intrång i upphovsrätten. När den misstänkta intrångsgörarens Internetleverantör har informerats varnar leverantören den identifierade intrångsgöraren. Efter tre varningar stängs användaren av från Internet.

16. Samtidigt som förhandlingarna om Acta-avtalet pågår håller vissa medlemsstater, till exempel Frankrike, på att genomföra åtgärder för att stänga av Internetanvändare efter tre varningar. Dessa åtgärder diskuteras även i vissa EU-forum, till exempel i den dialog mellan berörda parter om olaglig upp – och nedladdning som generaldirektoratet för inre marknaden och tjänster har inlett, i samband med antagandet av kommissionens meddelande om att stärka säkerställandet av skydd för immateriella rättigheter på den inre marknaden ([12]). Frågan kommer även att diskuteras i Europaparlamentet i samband med debatten om förslaget till Europaparlamentets resolution om att stärka säkerställandet av skydd för immateriella rättigheter på den inre marknaden (nedan kallat *Marielle Gallos betänkande*).

17. Dessa förfaranden är mycket integritetskränkande. De består bland annat av en generell övervakning av alla Internetanvändares förehavanden på Internet, däribland helt lagliga sådana. De påverkar miljontals laglydiga Internetanvändare, däribland många barn och ungdomar. Åtgärderna vidtas av privata aktörer, inte av brottsbekämpande myndigheter. Vidare har Internet i dag en central roll i nästan alla delar av det moderna samhället. Att stänga av människor från Internet kan således få enorma konsekvenser och utestänga människor från arbete, kultur, e-förvaltningstjänster osv.

18. Mot bakgrund av detta är det relevant att granska om dessa åtgärder är förenliga med EU:s integritets- och dataskyddslagstiftning och framförallt om det är nödvändigt att stänga av Internetanvändare efter tre varningar för att säkerställa skyddet av de immateriella rättigheterna. Här bör man dessutom analysera om det finns andra, mindre integritetskränkande metoder.

19. Det är fortfarande oklart om Acta-avtalet kommer att innehålla åtgärder för att stänga av Internetanvändare efter tre varningar. Dessa åtgärder övervägs emellertid även på andra områden och kan – potentiellt – få stora konsekvenser för integritets- och dataskyddet. Av dessa skäl anser Europeiska datatillsynsmannen att det är nödvändigt att diskutera dem i detta yttrande. Innan Europeiska datatillsynsmannen går in på ovannämnda analys kommer han att kort beskriva den tillämpliga rättsliga ramen om integritet och dataskydd.

20. Observera att åtgärderna för att stänga av Internetanvändare efter tre varningar inte bara väcker frågor om integritet och dataskydd, utan även om andra värderingar som rättssäkerhet och yttrandefrihet. Detta yttrande kommer dock endast att ta upp frågor som rör skyddet av personuppgifter och personlig integritet.

IV.2 Avstängning av Internetanvändare efter tre varningar och tillämpningen av EU:s rättsliga ram för integritet och dataskydd

Utformning av åtgärder för att stänga av Internetanvändare efter tre varningar

21. I ett system där Internetanvändare stängs av efter tre varningar kan upphovsrättsinnehavaren med automatiserade tekniska hjälpmedel, som eventuellt tillhandahålls av tredje man, identifiera misstänkta intrång i upphovsrätten genom att övervaka Internetanvändarnas förehavanden. Upphovsrättsinnehavaren kan till exempel övervaka forum och

([10]) Se fotnot 2 ovan.

([11]) De olika mellanhänderna på Internet kan definieras utifrån sina olika funktioner. I praktiken fyller mellanhänderna dock i regel flera av dessa funktioner. Till mellanhänderna på Internet hör bland annat följande: a) *Internetleverantörer*: användarna ansluter till nätverket genom att ansluta till Internetleverantörens server, b) *nätverksleverantörer*: de tillhandhåller routern, dvs., den tekniska utrustning som krävs för att skicka uppgifterna, c) *webbhotell*: de hyr ut utrymme på sin server där användarna eller innehållsleverantörer kan ladda upp material. Användarna kan ladda upp och ned material till en Internettjänst, till exempel en anslagstavla eller ett fildelningsnätverk.

([12]) Meddelande från kommissionen till rådet, Europaparlamentet och Europeiska ekonomiska och sociala kommittén av den 11 september 2009 om att stärka säkerställandet av skydd för immateriella rättigheter på den inre marknaden, KOM(2009) 467 slutlig.

bloggar eller utge sig för att vara fildelare i fildelningsnätverk för att identifiera fildelare som misstänks utbyta upphovsrättsskyddat material ([13]).

22. När upphovsrättsinnehavarna har identifierat de Internetanvändare som misstänks göra intrång i upphovsrätten genom att samla in deras IP-adresser skickar de IP-adresserna till respektive Internetleverantör som varnar den berörda abonnenten om att han eller hon misstänks för upphovsrättsintrång. När Internetleverantören har varnat abonnenten ett visst antal gånger sägs abonnenten automatiskt upp eller stängs av från Internet ([14]).

Tillämplig EU-lagstiftning på integritets- och dataskyddsområdet

23. Åtgärderna för att stänga av Internetanvändare efter tre varningar måste uppfylla kraven om rätten till privatliv i artikel 8 i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna och artikel 7 i stadgan om de grundläggande rättigheterna. De måste även uppfylla kraven om rätten till skydd av personuppgifter i artikel 8 i stadgan om de grundläggande rättigheterna och artikel 16 FEUF, samt i direktiv 95/46/EG och direktiv 2002/58/EG.

24. Europeiska datatillsynsmannen anser att övervakningen av Internetanvändarnas beteende och insamlingen av deras IP-adresser utgör ett intrång i deras rätt till skydd för sitt privatliv och sin korrespondens. Åtgärderna utgör med andra ord ett ingrepp i deras rätt till privatliv. Denna ståndpunkt överensstämmer med Europadomstolens rättspraxis ([15]).

25. Direktiv 95/46/EG är tillämpligt ([16]) eftersom åtgärderna för att stänga av Internetanvändare efter tre varningar medför behandling av IP-adresser som – åtminstone i det aktuella fallet – bör anses vara personuppgifter. En IP-adress är en identifieringskod som ser ut som en nummerserie som åtskiljs av punkter, t.ex. 122.41.123.45. Ett abonnemang hos en Internetleverantör ger abonnenten tillgång till Internet. Abonnenten tilldelas en IP-adress varje gång han eller hon går in på Internet, via den utrustning som abonnenten använder för att ansluta till Internet (till exempel en dator) ([17]).

26. Om en användare utför en viss aktivitet, till exempel laddar upp material på Internet, kan användaren identifieras av tredje man via användarens IP-adress. En användare med IP-adress 122.41.123.45 misstänks till exempel ha laddat upp upphovsskyddat material till en fildelningstjänst kl. 15.00 den 1 januari 2010. Internetleverantören kommer då att kunna koppla IP-adressen till namnet på den abonnent som tilldelats denna adress och därmed identifiera abonnenten.

27. Med *personuppgifter* avses i artikel 2 i direktiv 95/46/EG ”varje upplysning som avser en identifierad eller identifierbar fysisk person (den registrerade). En identifierbar person är en person som kan identifieras, direkt eller indirekt, framför allt genom hänvisning till ett identifikationsnummer” ([18]). Mot bakgrund av denna definition måste slutsatsen dras att IP-adresser och upplysningar om aktiviteter som är kopplade till sådana adresser utgör personuppgifter i alla här relevanta fall. En IP-adress fungerar som ett identifikationsnummer som gör det möjligt att ta reda på namnet på den abonnent som tilldelats IP-adressen. De upplysningar som samlats in om abonnenten (”abonnenten laddade upp visst material till webbplatsen ZS kl. 15.00 den 1 januari 2010”) *avser*, dvs. handlar uppenbarligen om en identifierbar persons förehavanden (innehavaren av IP-adressen), och måste därför också anses utgöra personuppgifter.

([13]) Fildelningsteknik (P2P) är en distribuerad programvarulösning som används för att koppla samman olika datorer och kommunicera direkt med andra datorer.

([14]) Andra påföljder kan till exempel vara att begränsa vissa Internetfunktioner, till exempel hastigheten, mängden datatrafik osv.

([15]) Se framförallt Europadomstolens dom av den 26 juni 2006, Weber och Saravia mot Tyskland (dec), mål nr 54934/00, punkt 77, och Europadomstolens dom av den 1 juli 2008, Liberty m.fl. mot Förenade kungariket, mål nr 58243/00.

([16]) EU-domstolen gör en bred tolkning av tillämpligheten av direktiv 95/46/EG, vars bestämmelser måste tolkas mot bakgrund av artikel 8 i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna. Domstolen förklarade i sin dom av den 20 maj 2003 i de förenade målen C-465/00, C-138/01 och C-139/01, Rundfunk, REG 2003, s. I-4989, punkt 68, att ”bestämmelserna i direktiv 95/46 reglerar behandling av personuppgifter som kan innebära intrång i de grundläggande friheterna och då särskilt i rätten till privatliv, måste bestämmelserna i fråga med nödvändighet tolkas mot bakgrund av de grundläggande rättigheterna, vilka enligt fast rättspraxis utgör en integrerad del av de allmänna rättsprinciper som domstolen skall säkerställa iakttagandet av”.

([17]) Den IP-adress som Internetleverantören tilldelar en individ kan vara densamma varje gång individen surfar på Internet (så kallad statisk IP-adress). Den kan också vara dynamisk, vilket innebär att Internetleverantören tilldelar sina kunder en ny IP-adress varje gång de ansluter till Internet. Internetleverantören kan naturligtvis få fram vilken abonnent som har tilldelats en viss IP-adress (dynamisk eller statisk).

([18]) I skäl 26 kompletteras denna definition: ”Principerna för skyddet måste gälla all information som rör en identifierad eller identifierbar person. För att avgöra om en person är identifierbar skall härvid beaktas alla hjälpmedel som i syfte att identifiera vederbörande rimligen kan komma att användas antingen av den registeransvarige eller av någon annan person. Skyddsprinciperna gäller inte för uppgifter som gjorts anonyma på ett sådant sätt att den registrerade inte längre är identifierbar.”

28. Dessa ståndpunkter delas helt och hållet av artikel 29-gruppen som i ett dokument om dataskyddsfrågor och immateriella rättigheter förklarade att IP-adresser, som samlas in för att säkerställa skyddet av immateriella rättigheter, dvs. för att identifiera Internetanvändare som misstänks ha gjort intrång i de immateriella rättigheterna, är personuppgifter i den mån de används mot en viss person för att säkerställa skyddet av dessa rättigheter ([19]).

29. Direktiv 2002/58/EG är också tillämpligt eftersom åtgärderna för att stänga av Internetanvändare efter tre varningar medför insamling av trafik- och kommunikationsuppgifter. Direktiv 2002/58/EG reglerar användningen av sådana uppgifter och föreskriver att principen om konfidentialitet ska tillämpas på kommunikation via allmänna kommunikationsnät och på de uppgifter som kommuniceras.

IV.3 **Nödvändigheten av att stänga av Internetanvändare efter tre varningar**

30. I artikel 8 i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna fastställs principen om nödvändighet. Enligt denna är det endast tillåtet att ingripa i rätten till privatliv om det är nödvändigt för att uppnå legitima mål i ett demokratiskt samhälle ([20]). Principen om nödvändighet återfinns även i artiklarna 7 och 13 i direktiv 95/46/EG och i artikel 15 i direktiv 2002/58/EG ([21]). Enligt denna princip krävs det en analys av om åtgärden är proportionerlig, där inblandade intressen vägs mot varandra, sett till hela det demokratiska samhället ([22]). Det ska vidare göras en bedömning av om det finns andra, mindre integritetskränkande åtgärder.

31. Även om Europeiska datatillsynsmannen inser att det är viktigt att säkerställa skyddet av immateriella rättigheter anser han att åtgärderna för att stänga av Internetanvändare efter tre varningar, så som de framstår i dagsläget – med ett visst mått av generell tillämpning – är oproportionerliga och därför inte kan anses vara nödvändiga åtgärder. Europeiska datatillsynsmannen är vidare övertygad om att det finns andra, mindre integritetskränkande lösningar eller att de planerade åtgärderna kan utföras på ett mindre integritetskränkande sätt eller i mer begränsad omfattning. Systemet med avstängning efter tre varningar medför även problem på ett mer ingående juridiskt plan. Dessa slutsatser kommer att förklaras nedan.

Åtgärderna för att stänga av Internetanvändare efter tre varningar är oproportionerliga

32. Europeiska datatillsynsmannen vill betona att åtgärderna är långtgående. Följande aspekter måste nämnas i det avseendet:

i) Den (obemärkta) övervakningen skulle påverka miljontals personer och *alla* användare, oavsett om de är misstänkta eller ej.

ii) Övervakningen skulle innebära en systematisk registrering av uppgifter. Vissa av dessa skulle kunna medföra civilrättsliga eller straffrättsliga påföljder för människor. En del av de insamlade upplysningarna skulle därför räknas som känsliga uppgifter enligt artikel 8 i direktiv 95/46/EG som kräver kraftfullare garantier.

iii) Övervakningen skulle troligtvis innebära att många oskyldiga blir felaktigt misstänkta. Det är inte alltid helt enkelt att avgöra om det rör sig om upphovsrättsintrång. Ofta måste domstolarna granska mycket stora mängder tekniska och juridiska detaljer och mycket text för att avgöra om intrång föreligger ([23]).

([19]) Artikel 29-gruppens arbetsdokument om dataskyddsfrågor och immateriella rättigheter, *Working Document on data protection issues related to intellectual property rights*, (WP 104) (ej översatt till svenska), antaget den 18 januari 2005. Gruppen inrättades enligt artikel 29 i direktiv 95/46/EG. Den är ett europeiskt oberoende rådgivande organ i frågor om integritet och dataskydd. Dess uppdrag beskrivs i artikel 30 i direktiv 95/46/EG och artikel 15 i direktiv 2002/58/EG. Se även gruppens yttrande 4/2007 om begreppet personuppgifter (WP 136), antaget den 20 juni 2007, särskilt s. 16–17.

([20]) I artikel 8 i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna finns ett uttryckligt krav på att ingrepp eller restriktioner endast får förekomma om det ”i ett demokratiskt samhälle är nödvändigt”.

([21]) Enligt artikel 13 i direktiv 95/46/EG är en begränsning endast tillåten när den utgör ”en nödvändig åtgärd med hänsyn till a) statens säkerhet, b) försvaret, c) allmän säkerhet, d) förebyggande, undersökning, avslöjande av brott eller åtal för brott eller av överträdelser av etiska regler som gäller för lagreglerade yrken, e) ett viktigt ekonomiskt eller finansiellt intresse hos en medlemsstat eller hos Europeiska unionen, inklusive monetära frågor, budgetfrågor och skattefrågor, f) en tillsyns-, inspektions- eller regleringsfunktion som, även om den är av övergående karaktär, är förbunden med myndighetsutövning i de under punkterna c), d) och e) nämnda fallen, g) skydd av den registrerades eller andras fri- och rättigheter”. Enligt artikel 15 i direktiv 2002/58/EG ska ”en sådan begränsning i ett demokratiskt samhälle [vara] nödvändig, lämplig och proportionell för att skydda nationell säkerhet (dvs. statens säkerhet), försvaret och allmän säkerhet samt för förebyggande, undersökning, avslöjande av och åtal för brott eller vid obehörig användning av ett elektroniskt kommunikationssystem enligt artikel 13.1 i direktiv 95/46/EG”.

([22]) Se även Europadomstolens dom av den 2 augusti 1984, Malone mot Förenade kungariket, serie A nr 82, s. 32, punkt 81 f., och Europadomstolens dom av den 4 december 2008, Marper mot Förenade kungariket (GC), nr 30562/04 och 30566/04, punkt 101 f.

([23]) Domstolarna kan behöva ta ställning till om materialet faktiskt är upphovsrättskyddat, vilka rättigheter som kränkts, om användningen kan anses utgöra rättmätig användning, tillämplig lagstiftning, skadestånd osv.

iv) Hänsyn måste tas till de potentiella *effekterna* av övervakningen, som kan leda till att användaren stängs av från Internet. Detta skulle inskränka den enskildes rätt till yttrandefrihet, informationsfrihet och tillgång till kultur, e-förvaltningstjänster, marknadsplatser, e-post och i vissa fall arbetsrelaterade aktiviteter. Här är det särskilt viktigt att inse att effekterna inte bara blir kännbara för den misstänkta intrångsgöraren utan för alla familjemedlemmar som använder samma Internetanslutning, inklusive skolbarn som använder Internet i sitt skolarbete.

v) Det kommer i regel att vara privata företag (dvs. upphovsrättsinnehavare eller Internetleverantörer) som gör bedömningen och fattar beslutet. Europeiska datatillsynsmannen uttryckte redan i ett tidigare yttrande oro över att den privata sektorn (dvs. Internetleverantörer eller upphovsrättsinnehavare) ska övervaka enskilda personer på områden som i princip omfattas av de brottsbekämpande myndigheternas behörighet ([24]).

33. Europeiska datatillsynsmannen är inte övertygad om att fördelarna med åtgärderna väger tyngre än konsekvenserna för enskilda personers grundläggande rättigheter. Upphovsrättsskyddet ligger i upphovsrättsinnehavarnas och samhällets intresse. Inskränkningarna av de grundläggande rättigheterna förefaller emellertid inte motiverade, om man väger hur allvarlig integritetskränkningen är, dvs. hur stort ingrepp i privatlivet det rör sig om enligt ovan, mot de förväntade fördelarna, nämligen att förhindra intrång i de immateriella rättigheterna som – till stor del – utgörs av småskaliga intrång. Som generaladvokat Kokott förklarade i sitt förslag till avgörande i målet Promusicae: ”Det är […] inte säkert att privat fildelning utgör ett tillräckligt allvarligt hot mot skyddet av upphovsrätten, särskilt när den sker utan vinstsyfte, för att motivera tillämpning av detta undantag. Det är nämligen omtvistat huruvida privat fildelning medför en verklig skada.” ([25])

34. Här är det även värt att påminna om hur Europaparlamentet reagerade på förslaget att stänga av Internetanvändare efter tre varningar vid översynen av telekompaketet, särskilt ändringsförslag 138 till ramdirektivet ([26]). I ändringsförslaget fastställdes att åtgärder som inskränker grundläggande fri- och rättigheter endast får införas om de är lämpliga, proportionella och nödvändiga i ett demokratiskt samhälle, och att genomförandet av dem ska vara föremål för tillräckliga rättssäkerhetsgarantier i enlighet med den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna och med de allmänna principerna i gemenskapsrätten, inbegripet verksamt rättsligt skydd och korrekt rättsförfarande ([27]).

35. Mot bakgrund av detta understryker Europeiska datatillsynsmannen vidare att alla åtgärder som inskränker grundläggande rättigheter kommer att bli föremål för noggrann granskning både på EU-nivå och på nationell nivå. Här kan en parallell dras till direktiv 2006/24/EG ([28]) om lagring av uppgifter som avviker från den allmänna dataskyddsprincipen om att uppgifter ska raderas när de inte längre behövs för de ändamål som de samlades in. Enligt direktivet ska trafikuppgifter lagras för att bekämpa allvarliga brott. Notera att uppgifter endast får lagras vid ”allvarliga brott”, att det endast är ”trafikuppgifter” som får lagras, vilket i princip utesluter information om kommunikationens innehåll, och att det finns stränga garantier. Trots det har det ifrågasatts om det är förenligt med grundläggande rättigheter. Rumäniens författningsdomstol har beslutat att lagring av massuppgifter är oförenligt med grundläggande rättigheter ([29]) och det pågår för närvarande ett mål i Tysklands författningsdomstol ([30]).

Förekomsten av andra, mindre integritetskränkande åtgärder

36. Iakttagelserna ovan stärks av att det finns mindre integritetskränkande sätt att nå samma mål. Europeiska datatillsynsmannen vidhåller att mindre integritetskränkande modeller bör undersökas och provas.

([24]) Yttrande från Europeiska datatillsynsmannen av den 23 juni 2008 om förslaget till Europaparlamentets och rådets beslut om inrättande av ett flerårigt gemenskapsprogram för att skydda barn som använder Internet och annan kommunikationsteknik, EUT C 2, 7.1.2009, s. 2.

([25]) Se det mål som avses i fotnot 8, punkt 106.

([26]) Se Europaparlamentets och rådets direktiv 2009/140/EG av den 25 november 2009, EUT L 337, 18.12.2009, s. 37.

([27]) Det så kallade ändringsförslag 138 till artikel 1 i ramdirektivet lyder i sin slutliga form som följer: ”3a. Åtgärder som vidtas av medlemsstaterna angående slutanvändarnas tillträde till eller användning av tjänster och applikationer genom elektroniska kommunikationsnät ska respektera fysiska personers grundläggande fri- och rättigheter som garanteras genom den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna och de allmänna principerna i gemenskapsrätten. Alla dessa åtgärder angående slutanvändares tillgång till eller användning av tjänster och tillämpningar genom elektroniska kommunikationsnät som kan medföra en inskränkning av dessa grundläggande fri- och rättigheter får därför införas endast om de är lämpliga, proportionella och nödvändiga i ett demokratiskt samhälle, och genomförandet av dem ska vara föremål för tillräckliga rättssäkerhetsgarantier i enlighet med den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna och med de allmänna principerna i gemenskapsrätten, inbegripet verksamt rättsligt skydd och korrekt rättsförfarande. Följaktligen får dessa åtgärder vidtas endast med vederbörlig respekt för principen om presumtion för oskuld och rätten till integritet. Ett föregående, rättvist och opartiskt förfarande ska garanteras, inbegripet den eller de berörda personernas rätt att höras, med förbehåll för behovet av lämpliga förutsättningar och processuella arrangemang i vederbörligen underbyggda brådskande fall i enlighet med den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna. Rätten till effektiv och snabb domstolsprövning ska garanteras.”

([28]) Europaparlamentets och rådets direktiv 2006/24/EG av den 15 mars 2006, EUT L 105, 13.4.2006, s. 54.

([29]) http://www.legi-internet.ro/english/jurisprudenta-it-romania/decizii-it/romanian-constitutional-court-decision-regarding-data-retention.html

([30]) http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg09-124.html

37. Europeiska datatillsynsmannen erinrar om att det ändrade direktiv 2002/22/EG om samhällsomfattande tjänster och användares rättigheter avseende elektroniska kommunikationsnät och kommunikationstjänster (nedan kallat *direktivet om samhällsomfattande tjänster*), som ingår i det nyligen ändrade telekompaketet, innehåller vissa regler och förfaranden för att bekämpa småskaliga upphovsrättsintrång bland konsumenter ([31]). Till dessa förfaranden hör bland annat att medlemsstaterna är skyldiga att ta fram standardiserad information av allmänintresse om olika ämnen. Intrång i upphovsrätten och närstående rättigheter, och de rättsliga följderna av detta, nämns särskilt ([32]). Medlemsstaterna kan sedan uppmana Internetleverantörerna att sprida informationen till alla sina kunder och inkludera den i sina avtal.

38. Tanken med systemet är att informera människor och få dem att inte göra intrång i upphovsrätten och sprida upphovsrättsskyddad information, samtidigt som man undviker att övervaka Internetanvändningen och därmed slipper de integritets- och dataskyddsproblem som kan vara förknippade med en sådan övervakning. Medborgarrättsdirektivet ska genomföras i maj 2011. Dessa förfaranden har således inte införts ännu. Det har därför ännu inte funnits någon möjlighet att testa fördelarna med dem. Det verkar således vara för tidigt att redan nu bortse från de nya förfarandenas potentiella positiva resultat och i stället införa åtgärder för att stänga av Internetanvändare efter tre varningar, som innebär en betydligt större inskränkning av de grundläggande rättigheterna.

39. Dessutom bör man komma ihåg att direktiv 2004/48/EG av den 28 april 2004 om säkerställande av skyddet för immateriella rättigheter innehåller en rad olika verktyg för att säkerställa skyddet av immateriella rättigheter i domstolarna (diskuteras nedan i punkt 43 och framåt) ([33]).

40. Ipred har först nyligen införlivats i medlemsstaternas lagstiftning. Man har således inte hunnit utvärdera om bestämmelserna är lämpliga för att säkerställa skyddet av immateriella rättigheter. Av det skälet är det åtminstone tveksamt om det nuvarande systemet som bygger på domstolsförfaranden, och som inte har testats ännu, behöver ersättas. Detta föranleder oundvikligen frågan om varför befintliga intrång inte kan åtgärdas med befintliga civil- och straffrättsliga påföljder för upphovsrättsintrång. Innan kommissionen föreslår sådana åtgärder bör den således ta fram tillförlitlig information som visar att det nuvarande regelverket inte har gett avsedd effekt.

41. Vidare är det oklart om man allvarligt har funderat över alternativa ekonomiska affärsmodeller som inte innebär systematisk övervakning av enskilda personer. Om upphovsrättsinnehavarna till exempel visar vilka förluster de har gjort till följd av fildelning skulle upphovsrättsinnehavarna och Internetleverantörerna kanske kunna prova Internetabonnemang där en del av abonnemangsavgiften för obegränsad användning av Internet går till upphovsrättsinnehavarna.

Möjligheten att bedriva målinriktad övervakning på ett mindre integritetskränkande sätt

42. Om man bortser från möjligheten att använda helt andra modeller, vilka som sagt bör undersökas och testas, kan målinriktad övervakning i vilket fall som helst bedrivas på ett mindre integritetskränkande sätt.

43. Målet att säkerställa skyddet av immateriella rättigheter kan även nås genom att endast övervaka ett begränsat antal personer som misstänks göra allvarliga intrång i upphovsrätten. Ipred ger viss vägledning i det avseendet. I direktivet fastställs på vilka villkor myndigheterna kan beordra Internetleverantörer att lämna ut personuppgifter för att säkerställa skyddet av immateriella rättigheter. Enligt artikel 8 får de behöriga rättsliga myndigheterna beordra Internetleverantörer att lämna ut personuppgifter om misstänkta intrångsgörare (t.ex. information om ursprung och distributionsnät för de intrångsgörande varorna eller tjänsterna) som svar på en berättigad och proportionell begäran vid intrång i *kommersiell skala* ([34]).

44. Kriteriet ”kommersiell skala” är således avgörande. Enligt detta kriterium kan övervakning vara proportionell i avgränsade, specifika, tillfälliga situationer där det föreligger

([31]) Se Europaparlamentets och rådets direktiv 2009/136/EG av den 25 november 2009, EUT L 337, 18.12.2009, s. 11.

([32]) I artikel 21.4 i direktiv 2009/136/EG anges till exempel följande: ”Medlemsstaterna får kräva att de företag som avses i punkt 3 vid behov sprider kostnadsfri information av allmänintresse till befintliga och nya abonnenter, med hjälp av samma metoder som företagen normalt använder för att kommunicera med abonnenterna. I så fall ska informationen tillhandahållas av de berörda offentliga myndigheterna i ett standardiserat format och ska bland annat omfatta följande: a) De vanligaste användningssätten för elektroniska kommunikationstjänster för att bedriva olaglig verksamhet eller sprida skadligt innehåll, särskilt när det kan skada respekten för andras fri- och rättigheter, inklusive intrång i upphovsrätt och närstående rättigheter, och de rättsliga följderna av detta.” Vidare anges följande i artikel 20.2: ”Medlemsstaterna får också kräva att avtalet ska innehålla sådan information som avses i artikel 21.4 och som är relevant för den tillhandahållna tjänsten, vilken tillhandahålls av de berörda offentliga myndigheterna för detta ändamål avseende användningen av elektroniska kommunikationsnät och kommunikationstjänster för att bedriva olaglig verksamhet eller för att sprida skadligt innehåll samt om metoderna för att skydda sig mot risker för personlig säkerhet, integritet och personuppgifter.”

([33]) EUT L 157, 30.4.2004, s. 45. (nedan kallat *Ipred*).

([34]) Detta bekräftas också i skäl 14 i Ipred.

välgrundade misstankar om upphovsrättsintrång i kommersiell skala. Kriteriet skulle kunna omfatta situationer där privatpersoner gör uppenbara intrång i upphovsrätten i syfte att erhålla direkta eller indirekta ekonomiska kommersiella fördelar.

45. För att ovanstående ska vara effektivt kan upphovsrättsinnehavarna i praktiken rikta in sig på att övervaka vissa IP-adresser för att kontrollera hur omfattande intrånget är. Detta skulle innebära att upphovsrättsinnehavarna för samma ändamål även skulle få lov att kontrollera rapporter om misstänkta intrång. Sådana uppgifter bör endast användas efter att man har kontrollerat hur allvarligt intrånget är, till exempel uppenbara fall av omfattande intrång och mindre men upprepade intrång under en viss tidsperiod för att skaffa sig kommersiella fördelar eller finansiella vinster. Kravet på upprepade intrång under vissa tidsperioder betonas och förklaras närmare nedan i diskussionen om bevarandeprincipen.

46. Detta skulle innebära att insamlingen av information för att bevisa misstänkt missbruk på Internet i dessa fall kan anses vara proportionerlig och nödvändig för att förbereda rättsliga förfaranden, bland annat en rättstvist.

47. Europeiska datatillsynsmannen anser att databehandling för att samla in den här typen av bevis som en ytterligare garanti först bör kontrolleras och godkännas av nationella dataskyddsmyndigheter. Datatillsynsmannen baserar sin uppfattning på att databehandlingen medför specifika risker för enskilda personers fri- och rättigheter med tanke på ändamålet, dvs. att vidta åtgärder som skulle kunna leda till åtal och med tanke på att de insamlade uppgifterna är känsliga. Det faktum att databehandlingen medför övervakning av elektronisk kommunikation är ytterligare ett skäl för ökad tillsyn.

48. Europeiska datatillsynsmannen anser att ”kommersiell skala” i Ipred är ett mycket lämpligt kriterium för att fastsälla gränserna för övervakningen för att respektera proportionalitetsprincipen. Vidare tycks det inte finnas några tillförlitliga bevis för att effektiva rättsliga åtgärder mot upphovsrättsintrång enligt kriterierna i Ipred skulle vara omöjliga eller ineffektiva. Till exempel kommer det rapporter från bland annat Tyskland som tyder på motsatsen. Där har man efter genomförandet av Ipred haft ca 3 000 rättsliga avgöranden som har lett till att Internetleverantörer har lämnat ut uppgifter om 300 000 abonnenter.

49. Sammanfattningsvis är det, med tanke på att Ipred endast har varit i kraft i två år, svårt att förstå varför lagstiftarna skulle överge kriterierna i direktivet för mer integritetskränkande metoder när EU precis är i färd med att börja testa dem som nyligen har antagits. Av samma skäl är det även svårt att förstå behovet av att ersätta det nuvarande domstolsbaserade systemet med andra typer av åtgärder (som dessutom väcker frågor om rättsäkerheten, som inte tas upp här).

IV.4 **Huruvida åtgärderna för att stänga av Internetanvändare efter tre varningar är förenliga med mer detaljerade dataskyddsbestämmelser**

50. Det finns andra mer specifika juridiska skäl till varför åtgärderna för att stänga av Internetanvändare efter tre varningar är problematiska ur ett dataskyddsperspektiv. Europeiska datatillsynsmannen betonar att det i direktiv 95/46/EG ställs krav på rättslig grund för databehandlingen, något som är tveksamt i det här fallet, och att det i direktiv 2002/58/EG föreskrivs en skyldighet att radera loggfiler.

Rättslig grund för behandling

51. Åtgärder för att stänga av Internetanvändare efter tre varningar medför behandling av personuppgifter. Vissa av dessa kommer att användas i rättsliga eller administrativa förfaranden för att stänga av upprepade intrångsgörare från Internet. Ur detta perspektiv räknas sådana uppgifter som känsliga uppgifter enligt artikel 8 i direktiv 95/46/EG. I artikel 8.5 anges följande: ”Behandling av uppgifter om lagöverträdelser, brottmålsdomar eller säkerhetsåtgärder får utföras endast under kontroll av en myndighet eller – om lämpliga skyddsåtgärder finns i nationell lag […]”.

52. Här är det relevant att påminna om artikel 29-gruppens dokument som nämndes ovan och som tar upp frågan om behandling av rättsliga uppgifter ([35]). Artikel 29-gruppen uppger att enskilda personer naturligtvis har rätt att behandla rättsliga uppgifter som part i ett rättsligt förfarande, men att principen inte är tillräckligt omfattande för att tredje man ska få utföra närmare utredningar, insamling och centralisering av personuppgifter, vilket i synnerhet gäller systematiska och generella efterforskningar, t.ex. genomsökningar av Internet ([36]). För denna typ av utredningar, framhåller man, är det de rättsliga myndigheterna som har behörighet. Även om det kan vara nödvändigt med målinriktad insamling av specifika bevis för att belägga och pröva rättsliga krav, särskilt i fall som rör allvarligt intrång, delar Europeiska datatillsynsmannen helt artikel 29-gruppens uppfattning att det inte är befogat med storskaliga utredningar som medför behandling av stora mängder uppgifter om Internetanvändare.

53. Diskussionen om ovannämnda proportionalitetsprincip och kriteriet om ”kommersiell skala” är relevanta för att avgöra under vilka förutsättningar det är befogat att samla in IP-adresser och därmed förknippad information.

([35]) Se punkt 28 i detta yttrande.
([36]) Min understrykning.

54. Internetleverantörerna kan försöka legitimera upphovsrättsinnehavarnas behandling av uppgifter genom att infoga klausuler i kundernas avtal som gör det möjligt att övervaka deras uppgifter och säga upp deras abonnemang. Kunderna skulle samtycka till övervakningen genom att ingå sådana avtal. Förfarandet väcker för det första den grundläggande frågan om huruvida enskilda personer kan ge Internetleverantören sitt samtycke till att tredje man, som inte lyder under Internetleverantörens ”ansvar”, behandlar uppgifter om dem.

55. För det andra har vi frågan om samtyckets giltighet. I artikel 2 h i direktiv 95/46/EG avses med samtycke ”varje slag av frivillig, särskild och informerad viljeyttring genom vilken den registrerade godtar behandling av personuppgifter som rör honom”. En viktig poäng är att samtycket för att vara giltigt, oavsett omständigheterna, måste vara den registrerades frivilliga, särskilda och informerade viljeyttring enligt artikel 2 h i direktivet. Europeiska datatillsynsmannen är mycket tveksam till om privatpersoner som ombeds ge sitt samtycke till övervakning av deras förehavanden på Internet verkligen kommer att ha något val – särskilt med tanke på att alternativet blir att inte ha tillgång till Internet alls, vilket skulle kunna äventyra många andra områden i livet.

56. För det tredje är det högst tveksamt om en sådan övervakning skulle kunna anses vara *nödvändig* för att fullgöra ett avtal i vilket den registrerade är part, vilket krävs enligt artikel 7 b i direktiv 95/46/EG, eftersom övervakningen uppenbarligen inte hör till syftet med det avtal som ingåtts med den registrerade utan endast är ett sätt för Internetleverantören att tillgodose andra intressen.

Radering av loggfiler

57. Enligt direktiv 2002/58/EG, särskilt artikel 6, får trafikuppgifter som IP-adresser endast samlas in och lagras för ändamål som är direkt förenade med själva kommunikationen, inklusive fakturering, trafikhantering och bedrägeribekämpning. Därefter måste uppgifterna raderas. Detta påverkar inte skyldigheterna enligt direktivet om lagring av uppgifter där det som sagt krävs att trafikuppgifter bevaras och lämnas ut till polis och åklagare **endast** för att underlätta utredningen av **allvarliga brott** ([37]).

58. I enlighet med ovanstående bör Internetleverantörer radera alla loggfiler som avslöjar Internetanvändarnas förehavanden som inte längre behövs för ovannämnda ändamål. Med tanke på att loggfiler inte behövs vid fakturering borde tre eller fyra veckor räcka för Internetleverantörens trafikhantering ([38]).

59. Det innebär att Internetleverantören, när den kontaktas av upphovsrättsinnehavaren, inte bör ha de loggfiler som kopplar IP-adresserna till abonnenterna, såvida denna kontakt inte tas inom den begränsade period som anges ovan. Internetleverantören bör endast lagra loggfilerna utöver denna period av berättigade skäl för de ändamål som föreskrivs i lagstiftningen.

60. Det innebär i praktiken att Internetleverantörerna helt enkelt inte kommer att kunna uppfylla upphovsrättsinnehavarens begäran, om denne inte handlar mycket snabbt, eftersom de inte längre har dessa uppgifter. Detta sätter i sig gränserna för vad som avses med acceptabla övervakningsförfaranden ovan.

Risk för följdverkningar

61. Europeiska datatillsynsmannen är vidare inte bara oroad över hur åtgärderna för att stänga av Internetleverantörer efter tre varningar påverkar integritets- och dataskyddet utan även över vilka följdverkningar åtgärderna får på andra områden. Om man tillåter dessa åtgärder riskerar detta senare att legitimera ännu mer omfattande övervakning av Internetanvändarnas förehavanden på andra områden och för andra ändamål.

62. Europeiska datatillsynsmannen uppmanar kommissionen att se till att Acta-avtalet inte går längre än eller strider mot EU:s gällande regler för att säkerställa skyddet av immateriella rättigheter, som respekterar grundläggande rättigheter och medborgerliga friheter, såsom skyddet av personuppgifter.

V. **DATASKYDDSFRÅGOR I INTERNATIONELLA SAMARBETSMEKANISMER**

63. En av de metoder som parterna i Acta-avtalet föreslår för att säkerställa skyddet av immateriella rättigheter är att öka det internationella samarbetet med ett antal åtgärder som

([37]) Se punkt 35 i detta yttrande.

([38]) Trafikhantering består bland annat av att analysera trafik i datornätverk för att optimera eller garantera prestandan, öka hastigheten och/eller öka den användbara bandbredden.

skulle göra det möjligt att effektivt säkerställa skyddet av immateriella rättigheter inom Acta-ländernas jurisdiktion.

64. Mot bakgrund av den information som finns kan slutsatsen dras att flera av de åtgärder som planeras för att säkerställa skyddet av immateriella rättigheter kommer att medföra internationella utbyten av information om misstänkta upphovsrättsintrång mellan myndigheter (t.ex. tullmyndigheter, polis och rättsväsende) och mellan offentliga och privata aktörer (t.ex. Internetleverantörer och upphovsrättsorganisationer). Ett sådant utbyte av information väcker en rad frågor ur dataskyddssynpunkt.

V.1 **Är datautbytet enligt Acta-avtalet legitimt, nödvändigt och proportionerligt?**

65. I det nuvarande läget i förhandlingarna, när ett antal konkreta aspekter av databehandlingen fortfarande är antingen odefinierade eller okända, är det omöjligt att kontrollera om de föreslagna åtgärderna är förenliga med grundläggande dataskyddsprinciper och EU:s dataskyddslagstiftning.

66. För det första kan det ifrågasättas om det är legitimt att överföra uppgifter till tredjeländer inom ramen för Acta-avtalet. Det kan ifrågasättas om det är relevant att anta åtgärder på internationell nivå på området så länge EU:s medlemsstater inte är överens om harmoniseringen av åtgärder för att säkerställa skyddet i den digitala miljön och om vilka straffrättsliga påföljder som ska tillämpas ([39]).

67. Mot bakgrund av ovanstående verkar det som om det skulle vara lättare att uppfylla principerna om nödvändighet och proportionalitet vid utbyte av uppgifter enligt Acta-avtalet om avtalet uttryckligen var begränsat till de allvarligaste intrången i de immateriella rättigheterna i stället för att tillåta utbyte av stora mängder uppgifter om varje misstänkt intrång. Detta kommer att kräva att man exakt definierar vad som utgör de ”allvarligaste intrången i de immateriella rättigheterna”, vilka medför att uppgifter får utbytas.

68. Vidare bör särskild uppmärksamhet ägnas åt de personer som är inblandade i uppgiftsutbytet och åt frågan om uppgifter endast kommer att utbytas mellan myndigheter eller även mellan privata aktörer och myndigheter. Som beskrivits tidigare i detta yttrande väcks ett antal frågor när privata aktörer är inblandade på ett område som i princip omfattas av de brottsbekämpande myndigheternas behörighet ([40]). Privata aktörers inblandning i insamling av personuppgifter om intrång i immateriella rättigheter och utbyte av dessa uppgifter med myndigheter bör vara strikt begränsad till vissa specifika omständigheter med lämpliga garantier.

V.2 **Tillämplig dataskyddslagstiftning för överföring av uppgifter inom ramen för Acta-avtalet**

Allmän ram för överföring av uppgifter

69. Den allmänna ramen för dataskydd i EU anges i direktiv 95/46/EG. I artiklarna 25 och 26 beskrivs vad som gäller vid överföring av uppgifter till tredjeländer. Enligt artikel 25 får överföring av personuppgifter endast ske till länder som säkerställer en adekvat skyddsnivå. I annat fall är en sådan överföring i princip förbjuden.

70. Kommissionen avgör från fall till fall om skyddsnivån i ett tredjeland är adekvat och har efter en grundlig analys av artikel 29-gruppen i flera fall fattat beslut om att ett antal länder har en adekvat skyddsnivå ([41]).

71. Europeiska datatillsynsmannen noterar att de flesta av parterna i Acta-avtalet inte finns med på den lista som kommissionen har upprättat över länder som har ett adekvat dataskydd. Med undantag för Schweiz och – i vissa specifika fall – Kanada och Förenta staterna, har inga andra parter i Acta-avtalet erkänts ha en adekvat skyddsnivå. Det innebär att ett av villkoren i artikel 26.1 i direktiv 95/46/EG måste vara uppfyllt, eller så måste parterna ställa tillräckliga garantier, för att uppgifter ska få överföras från EU till dessa länder enligt artikel 26.2 i direktivet.

Specifik ram för överföring av uppgifter för att bekämpa brott

72. Även om direktiv 95/46/EG utgör den viktigaste dataskyddsrättsakten i EU är dess tillämpningsområde för närvarande begränsat eftersom det uttryckligen utesluter vissa verksamheter, bland annat statens verksamhet på straffrättens område (artikel 3). Utbyte av uppgifter för att bekämpa brott ingår således inte i tillämpningsområdet för direktiv 95/46/EG utan omfattas av de allmänna dataskyddsprinciperna i Europarådets konvention nr 108 och dess

([39]) Rådet håller för närvarande på att diskutera ett förslag om straffrättsliga påföljder, KOM(2006) 168 av den 26 april 2006.

([40]) Se punkterna 32 och 52 i detta yttrande. Se även yttrandet från Europeiska datatillsynsmannen av den 11 november 2008 om slutrapporten från EU–USA-kontaktgruppen på hög nivå för informationsutbyte, integritetsskydd och skydd av personuppgifter, EUT C 128, 6.6.2009, s. 1.

([41]) Se Europeiska kommissionens beslut om adekvat skydd för personuppgifter i Argentina, Kanada, Schweiz, Förenta staterna (safe harbour och passageraruppgifter (PNR)), Guernsey, Isle of Man och Jersey. Beslutet finns på följande webbplats: http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm

tilläggsprotokoll som alla EU:s medlemsstater har skrivit under ([42]). Dessutom gäller de regler som EU har antagit om polissamarbete och straffrättsligt samarbete på straffrättens område som anges i rådets rambeslut 2008/877/RIF ([43]).

73. Enligt dessa rättsakter ska det i princip finnas en adekvat skyddsnivå i det tredjeland till vilket uppgifterna ska överföras. Det finns dock ett antal undantag, framförallt när ett tredjeland har adekvata garantier. Precis som vid utbyte av uppgifter enligt direktiv 95/46/EG krävs det vid utbyte av uppgifter för att bekämpa brott adekvata garantier mellan parterna för att uppgifterna ska överföras.

Mot en ny ram för överföring av uppgifter

74. EU väntas inom en snar framtid anta nya gemensamma dataskyddsregler enligt artikel 16 i EUF-fördraget som ska gälla alla verksamhetsområden i EU. Det innebär att EU om några år kan komma att få en heltäckande dataskyddsram med enhetliga regler för dataskydd för alla verksamhetsområden i EU, vilket innebär samma skyddsnivå och garantier för all databehandling. Som kommissionsledamoten med ansvar för rättvisa, grundläggande rättigheter och medborgarskap, Viviane Reding ([44]), förklarat bör denna nya ram fungera som en gemensam, modern och heltäckande rättsakt för dataskydd i EU. En sådan ram är särskilt välkommen eftersom den skulle skapa större klarhet och konsekvens om vilka dataskyddsregler som gäller i EU.

75. I ett internationellt sammanhang pekar Europeiska datatillsynsmannen även på dataskyddsmyndigheternas nyligen antagna resolution *International standards on the protection of personal data and privacy* som är ett första steg mot att upprätta globala dataskyddsnormer ([45]). De internationella normerna innehåller ett antal dataskyddsgarantier som liknar dem som anges i direktiv 95/46/EG och konvention nr 108. Även om de internationella normerna ännu inte har någon bindande kraft ger de fortfarande viss vägledning om vilka dataskyddsprinciper som tredjeländer frivilligt kan tillämpa så att deras rättsliga ram är förenlig med EU:s normer. Europeiska datatillsynsmannen anser att de länder som undertecknar Acta-avtalet även bör ta hänsyn till principerna i de internationella normerna när de behandlar personuppgifter från EU.

V.3 **Nödvändigheten av att genomföra lämpliga garantier för att skydda uppgifter som överförs från EU till tredjeländer**

Vilka former av garantier bör det finnas för att effektivt skydda uppgifter som överförs till tredjeländer?

76. Europeiska datatillsynsmannen betonar att om man kan visa att det är nödvändigt att överföra personuppgifter till tredjeländer bör EU – utöver själva Acta-avtalet – förhandla fram specifika avtal med mottagarländerna som innehåller lämpliga dataskyddsgarantier som ska reglera utbytet av personuppgifter.

77. Lämpliga dataskyddsgarantier bör i regel anges i ett bindande avtal mellan EU och mottagaren i tredjeland där den mottagande parten åtar sig att iaktta EU:s dataskyddslagstiftning och att ge enskilda personer samma rättigheter och rättsmedel som ges enligt EU:s lagstiftning. Behovet av ett bindande avtal härrör från artikel 26.2 i direktiv 95/46/EG och artikel 13.3 b i rambeslutet och stöds även av EU:s gällande praxis att ingå specifika avtal för att tillåta att specifika uppgifter överförs till tredjeländer ([46]).

78. På samma sätt kan mottagaren enligt förslaget till internationella normer vara tvungen att garantera att den ställer en adekvat skyddsnivå för att uppgifterna ska överföras. Dessa garantier kan även lämnas i ett avtal.

Innebörden av de garantier som Acta-länderna ska ställa vid överföring av personuppgifter

79. Europeiska datatillsynsmannen betonar särskilt att internationella informationsutbyten för att bekämpa brott är särskilt känsliga ur dataskyddssynpunkt, eftersom det skulle kunna legitimera att stora mängder uppgifter överförs på

([42]) Europarådets konvention om skydd för enskilda vid automatisk databehandling av personuppgifter som antogs i Strasbourg den 28 januari 1981 och tilläggsprotokollet till konventionen beträffande tillsynsmyndigheter och internationella flöden av uppgifter som antogs i Strasbourg den 8 november 2001.

([43]) Rådets rambeslut 2008/977/RIF av den 27 november 2008 om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete, EUT L 350, 30.12.2008, s. 60.

([44]) Se svaren på Europaparlamentets frågor till kommissionsledamotskandidat Viviane Reding, s. 5 på följande webbplats: http://www.europarl.europa.eu/hearings/static/commissioners/answers/reding_replies_en.pdf

([45]) Resolutionen antogs i Madrid i november 2009.

([46]) Till exempel Europols och Eurojusts avtal med Förenta staterna, PNR-avtalet och Swiftavtalet, samt avtalet mellan EU och Australien om lufttrafikföretags behandling av passageraruppgifter (PNR) från Europeiska unionen och överföring av dessa till Australiens tullmyndighet.

ett område där konsekvenserna för den enskilde är särskilt allvarliga och där det är särskilt viktigt med strikta och tillförlitliga garantier.

80. Europeiska datatillsynsmannen påpekar att specifika villkor och garantier endast kan fastställas från fall till fall i ljuset av alla aspekter av uppgiftsutbytet. I vägledande syfte framhåller Europeiska datatillsynsmannen nedan emellertid några av de principer och garantier som de mottagande tredjeländerna måste upprätthålla för att uppgifterna ska kunna överföras:

— Det måste kontrolleras att det finns en rättslig grund för att behandla uppgifterna (dvs. behandlingen måste bygga på en juridisk skyldighet, på de registrerades samtycke eller på något annat giltigt skäl) och att överföringen är förenlig med datainsamlingens ursprungliga syfte. Inga uppgifter bör överföras som faller utanför det angivna syftet.

— Mängden och typen av personuppgifter som ska utbytas bör tydligt anges och inte överstiga det som är strikt nödvändigt för att uppnå syftet med överföringen. De personuppgifter som samlas in och överförs får till exempel innehålla Internetanvändarnas IP-adresser, datum och tidpunkt för det misstänkta brottet och typen av brott. Europeiska datatillsynsmannen rekommenderar att uppgifterna inte kopplas till någon specifik individ under utredningsfasen och erinrar om att en misstänkt person endast får identifieras i enlighet med lagstiftningen och efter ett domstolsbeslut. Europeiska datatillsynsmannen påpekar att uppgifter som rör intrång och misstankar om intrång i immateriella rättigheter tillhör en särskild kategori av uppgifter, som i regel endast får behandlas av brottsbekämpande myndigheter och som i regel kräver extra garantier. Det måste därför särskilt anges vilka personer som är behöriga att behandla uppgifter som rör intrång och misstankar om intrång i immateriella rättigheter och vilka villkor som gäller för att behandla uppgifterna i enlighet med gällande dataskyddslagstiftning.

— Det måste tydligt anges vilka personer som får utbyta uppgifter med varandra och det bör i princip vara förbjudet att sprida uppgifterna vidare, såvida detta inte är nödvändigt för en specifik utredning. Denna begränsning är särskilt viktig eftersom de utsedda mottagarna inte otillbörligen ska lämna ut uppgifter till obehöriga.

— Europeiska datatillsynsmannen utgår från att Acta-avtalet inte bara kommer att leda till att myndigheter samarbetar med varandra, utan även till att privata organisationer (t.ex. Internetleverantörer och upphovsrättsorganisationer) får i uppgift att se till att lagstiftningen följs. I det senare fallet måste man noggrant se över villkoren för och de privata organisationernas inblandning i att säkerställa skyddet av immateriella rättigheter, i den mening att Acta-avtalet i praktiken inte får ge Internetleverantörer och upphovsrättsorganisationer rätt att övervaka användarnas beteende på Internet. Vidare bör privata organisationer endast behandla personuppgifter för att bekämpa brott om det finns en lämplig rättslig grund. Det är även viktigt att klargöra om privata organisationer ska tvingas samarbeta med polisen och hur omfattande detta samarbete i så fall ska vara. Detta bör i vilket fall som helst vara begränsat till ”allvarliga brott”, vilka dessutom exakt måste definieras eftersom inte alla intrång i de immateriella rättigheterna ska anses utgöra allvarliga brott.

— Det måste tydligt anges vilken metod som ska användas vid utbyte av uppgifter. Det bör särskilt anges om utbytet ska ske i form av ett ”push system” – där t.ex. Internetleverantörer och upphovsrättsorganisationer under sin tillsyn lämnar ut uppgifter till tredje man, till exempel polis eller brottsbekämpande myndigheter, i utlandet – eller ett ”pull system” – där t.ex. polis och brottsbekämpande myndigeter får direkt tillgång till privata aktörers databaser eller till centrala databaser där uppgifterna finns samlade. Som redan har beskrivits i samband med PNR är ett ”push system” det enda alternativ som är förenligt med EU:s dataskyddsprinciper, eftersom det ger avsändaren i EU, som sannolikt är den registeransvarige, rätt att kontrollera överföringen av uppgifter ([47]).

— Det måste anges hur länge mottagaren får lagra uppgifterna samt för vilka ändamål det är nödvändigt att lagra dem. Denna tid bör vara proportionerlig i förhållande till det ändamål som ska uppnås, vilket innebär att uppgifterna ska tas bort eller raderas när de inte längre behövs för detta ändamål.

— Det bör tydligt anges vilka krav som ska ställas på registeransvariga i tredjeländer. Det måste finnas mekanismer för att utöva tillsyn och/eller utkräva ansvar så att det finns effektiva åtgärder och påföljder att ta till mot registeransvariga vid otillbörlig behandling eller andra relevanta incidenter. Vidare bör prövningsmöjligheter införas så att enskilda personer kan klaga hos en

([47]) Se artikel 29-gruppens yttrande 4/2003 om skyddsnivån i USA för överföring av passageraruppgifter, WP 78, av den 13 juni 2003.

oberoende dataskyddsmyndighet och ansöka om kompensation hos en oberoende och opartisk domstol ([48]).

— Det avtal som parterna ingår bör tydligt ange vilka rättigheter de registrerade har när deras personuppgifter behandlas av en mottagande tredjepart för att garantera att de har effektiva verktyg för att göra gällande sina rättigheter om deras personuppgifter behandlas utomlands.

— Det är dessutom viktigt med öppenhet och parterna i dataskyddsavtalet måste komma överens om hur de ska informera de registrerade om vilka uppgifter som behandlas, vilka rättigheter de har och hur de ska göra gällande dem.

VI. **SLUTSATSER**

81. Europeiska datatillsynsmannen uppmanar kommissionen att inleda en offentlig och öppen dialog om Acta-avtalet, eventuellt genom ett offentligt samråd, som också skulle bidra till att se till att de åtgärder som ska antas är förenliga med EU:s integritets- och dataskyddslagstiftning.

82. Europeiska datatillsynsmannen uppmanar kommissionen att i de pågående förhandlingarna om Acta-avtalet hitta rätt balans mellan å ena sida kraven på skydd av immateriella rättigheter och å andra sidan rätten till integritets- och dataskydd. Europeiska datatillsynsmannen betonar att det är särskilt viktigt att i förhandlingarna ta hänsyn till integritets- och dataskydd redan från början, innan man kommer överens om några åtgärder, för att undvika att man senare måste hitta alternativa lösningar som uppfyller integritetskraven.

83. Även om immateriella rättigheter är viktiga för samhället och måste skyddas får de inte sättas framför människors grundläggande rätt till integritet och dataskydd, eller andra rättigheter, såsom rätten att betraktas som oskyldig till dess att skuldfrågan avgjorts, rättssäkerhet och yttrandefrihet.

84. Det nuvarande förslaget till Acta-avtal kommer, i den mån det innehåller eller åtminstone indirekt förespråkar åtgärder för att stänga av Internetanvändare efter tre varningar, kraftigt inskränka EU-medborgarnas grundläggande fri- och rättigheter, framförallt skyddet av personuppgifter och personlig integritet.

85. Europeiska datatillsynsmannen anser att sådana åtgärder inte är nödvändiga för att säkerställa skyddet av immateriella rättigheter. Europeiska datatillsynsmannen är övertygad om att det finns andra, mindre integritetskränkande lösningar eller åtminstone att de planerade åtgärderna kan utföras på ett mindre integritetskränkande sätt eller i mer begränsad omfattning, särskilt i form av tillfällig, målinriktad övervakning.

86. Åtgärderna för att stänga av Internetanvändare efter tre varningar är också problematiska på en mer ingående juridisk nivå, särskilt med tanke på att behandlingen av rättsliga uppgifter, framförallt av privata organisationer, måste bygga på en lämplig rättslig grund. Dessa åtgärder kan i praktiken även medföra att loggfiler lagras under längre tid, vilket skulle strida mot gällande lagstiftning.

87. Europeiska datatillsynsmannen uppmanar också EU att införa lämpliga garantier i den mån Acta-avtalet innebär att myndigheter och/eller privata organisationer i avtalsslutande länder utbyter personuppgifter med varandra. Dessa garantier bör gälla all överföring av uppgifter inom ramen för Acta-avtalet – oavsett om den sker för att upprätthålla civilrättslig, straffrättslig eller digital lagstiftning – och bör vara förenliga med dataskyddsprinciperna i konvention nr 108 och direktiv 95/46/EG. Europeiska datatillsynsmannen rekommenderar att dessa garantier ges i form av bindande avtal mellan avsändarna i EU och mottagarna i tredjeland.

88. Europeiska datatillsynsmannen vill även höras om de åtgärder som ska genomföras i fråga om överföring av uppgifter enligt Acta-avtalet för att kontrollera att de är proportionerliga och att de ger en adekvat skyddsnivå.

Utfärdat i Bryssel den 22 februari 2010.

Peter HUSTINX
Europeiska datatillsynsmannen

([48]) Se yttrandet från Europeiska datatillsynsmannen om slutrapporten från EU-USA-kontaktgruppen på hög nivå för informationsutbyte, integritetsskydd och skydd av personuppgifter av den 11 november 2008.