

I

(Beslutninger og resolutioner, henstillinger og udtalelser)

UDTALELSER

DEN EUROPÆISKE TILSYNSFØRENDE FOR DATABESKYTTELSE

Udtalelse fra Den Europæiske Tilsynsførende for Databeskyttelse (EDPS) om EU's forhandlinger om en handelsaftale vedrørende bekæmpelse af forfalskning (ACTA)

(2010/C 147/01)

DEN EUROPÆISKE TILSYNSFØRENDE FOR DATABESKYTTELSE —

som henviser til traktaten om Den Europæiske Unions funktionsmåde, særlig artikel 16,

som henviser til Den Europæiske Unions charter om grundlæggende rettigheder, særlig artikel 8,

som henviser til Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger ⁽¹⁾,

som henviser til Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor ⁽²⁾,

som henviser til Europa-Parlamentets og Rådets forordning (EF) nr. 45/2001 af 18. december 2000 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i fællesskabsinstitutionerne og -organerne og om fri udveksling af sådanne oplysninger ⁽³⁾, særlig artikel 41,

HAR VEDTAGET FØLGENDE UDTALELSE:

I. INDLEDNING

1. EU deltager i forhandlingerne om en handelsaftale vedrørende bekæmpelse af forfalskning (ACTA). Disse forhand-

⁽¹⁾ EFT L 281 af 23.11.1995, s. 31.

⁽²⁾ EFT L 201 af 31.7.2002, s. 37.

⁽³⁾ EFT L 8 af 12.1.2001, s. 1.

linger blev indledt i 2007 blandt en gruppe interesserede parter og videreførtes efterfølgende blandt en bredere gruppe af deltagere. Disse omfatter indtil videre Australien, Canada, EU, Japan, Korea, Mexico, Marokko, New Zealand, Singapore, Schweiz og USA. Europa-Kommissionen fik i 2008 mandat fra Rådet til at deltage i disse forhandlinger.

2. Den tilsynsførende anerkender, at grænseoverskridende handel med forfalskede og piratkopierede varer er et voksende problem, der ofte involverer organiserede kriminelle netværk, og som kræver vedtagelse af passende samarbejdsmechanismer på internationalt plan for at bekæmpe denne form for kriminalitet.
3. Den tilsynsførende anfører, at EU's forhandlinger om en multilateral aftale, der har som primært formål at håndhæve de intellektuelle ejendomsrettigheder, rejser en række vigtige spørgsmål f.eks. om, konsekvenserne af de foranstaltninger, der træffes for at bekæmpe varemærkeforfalskning og piratkopiering, på borgernes grundlæggende rettigheder, navnlig retten til privatliv og databeskyttelse.
4. Den tilsynsførende beklager i den forbindelse, at Europa-Kommissionen ikke har rådført sig med ham vedrørende indholdet af en sådan aftale. Den tilsynsførende har derfor på eget initiativ vedtaget denne udtalelse baseret på artikel 41, stk. 2, i forordning (EF) nr. 45/2001 med henblik på at vejlede Kommissionen om de aspekter vedrørende privatlivets fred og databeskyttelse, der bør tages højde for i ACTA-forhandlingerne.

II. STATUS FOR OG PLANLAGT INDHOLD AF ACTA

5. Den syvende forhandlingsrunde fandt sted i Mexico den 26.-29. januar 2010 med det formål at indgå en aftale i løbet af 2010. Der er imidlertid endnu ikke officielt blevet fremlagt et udkast til en aftale.

6. Forhandlingerne sigter mod vedtagelse af en ny multilateral aftale, der har til formål at styrke håndhævelsen af intellektuelle ejendomsrettigheder og bekæmpelsen af varemærkeforfalskning og piratkopiering. Hvis denne nye aftale vedtages, vil det føre til en forbedring af de internationale standarder for håndtering af meget omfattende overtrædelser af de intellektuelle ejendomsrettigheder. Europa-Kommissionen, GD Handel, har især understreget, at formålet er at bekæmpe aktiviteter inden for varemærkeforfalskning og piratkopiering, som i væsentlig grad påvirker kommercielle interesser, frem for at fokusere på almindelige borgeres aktiviteter ⁽⁴⁾.
7. Hvad angår indholdet af aftalen, angives det i det sammendrag af de vigtigste elementer til drøftelse, som Europa-Kommissionen, GD Handel, offentliggjorde i november 2009, at ACTA's mål om at bekæmpe piratkopiering og varemærkeforfalskning vil blive søgt opfyldt ved hjælp af tre hovedelementer: i) internationalt samarbejde, ii) håndhævelsespraksis og iii) definition af et retsgrundlag for håndhævelsen af intellektuelle ejendomsrettigheder inden for en række identificerede områder, herunder navnlig det digitale miljø ⁽⁵⁾. De planlagte foranstaltninger vil primært have fokus på retlige procedurer (f.eks. påbud, midlertidige foranstaltninger), internetudbyderes rolle og ansvarsområder med hensyn til at hindre overtrædelser af ophavsretten på internettet, samt grænseoverskridende foranstaltninger til at forhindre varer i at passere grænserne. De oplysninger, der er offentliggjort, angiver imidlertid kun hovedtrækkene i aftalen, og indeholder ingen detaljer om specifikke og konkrete foranstaltninger.
8. Den tilsynsførende bemærker, at selv om formålet med ACTA kun er at forfølge omfattende overtrædelser af de intellektuelle ejendomsrettigheder, kan det ikke udelukkes, at almindelige borgeres aktiviteter også vil kunne blive registreret under ACTA, ikke mindst fordi håndhævelsesforanstaltningerne finder sted i det digitale miljø. Den tilsynsførende fremhæver, at beskyttelse af fysiske personers grundlæggende rettigheder kræver, at der er fastsat tilstrækkelige garantier. Endvidere dækker lovgivningen om databeskyttelse alle fysiske personer, herunder også personer, som potentielt kan være involveret i aktiviteter vedrørende varemærkeforfalskning og piratkopiering. Bekæmpelse af omfattende overtrædelser vil uden tvivl også involvere behandling af personoplysninger.
9. I den forbindelse tilskynder den tilsynsførende på det kraftigste Europa-Kommissionen til at etablere en offentlig og åben dialog om ACTA, eventuelt via en offentlig høring, som også kan bidrage til at sikre, at de foranstaltninger, der skal vedtages, er i overensstemmelse med kravene i EU's lovgivning om beskyttelse af privatlivets fred og om databeskyttelse.

III. ANVENDELSESOMRÅDE FOR DEN TILSYNSFØRENDES BEMÆRKNINGER

10. Den tilsynsførende opfordrer på det kraftigste EU, og navnlig Europa-Kommissionen, som har mandat til at indgå aftalen, til at finde den rette balance mellem behovet for at beskytte intellektuelle ejendomsrettigheder og behovet for at beskytte fysiske personers privatliv og sikre databeskyttelse.
11. Den tilsynsførende fremhæver, at beskyttelse af privatlivets fred og databeskyttelse er centrale værdier i EU. De er anerkendt i artikel 8 i den europæiske menneskerettighedskonvention og artikel 7 og 8 i EU's charter for Grundlæggende Rettigheder ⁽⁶⁾, og skal respekteres i alle politikker og bestemmelser, som vedtages af EU, jf. artikel 16 i traktaten om Den Europæiske Unions funktionsmåde (TEUF).
12. Den tilsynsførende fremhæver endvidere, at EU ved indgåelse af enhver aftale vedrørende ACTA skal overholde de juridiske forpligtelser, som EU er pålagt med hensyn til beskyttelse af privatlivets fred og databeskyttelse, som fastsat i direktiv 95/46/EF, direktiv 2002/58/EF ⁽⁷⁾ og i Den Europæiske Menneskerettighedsdomstol ⁽⁸⁾ og EF-Domstolens retspraksis ⁽⁹⁾.
13. Beskyttelse af privatlivets fred og databeskyttelse skal inddrages allerede i begyndelsen af forhandlingerne og ikke først, når ordningerne og procedurerne er blevet fastlagt og vedtaget, og det derfor er for sent at finde alternative løsninger til at sikre privatlivets fred.
14. Den tilsynsførende bemærker, at han i lyset af de få oplysninger, der er offentliggjort, ikke er i stand til at tilvejebringe en analyse af de specifikke bestemmelser i ACTA. Den tilsynsførende vil i denne udtalelse derfor fokusere på at påvise de mulige trusler mod beskyttelse af privatlivets fred og databeskyttelse under de eventuelle konkrete foranstaltninger, som aftalen kan medføre inden for de følgende to områder: håndhævelse af intellektuelle ejendomsrettigheder i det digitale miljø (kapitel IV) og internationale samarbejdsmekanismer (kapitel V).

⁽⁶⁾ Den Europæiske Unions Charter om Grundlæggende Rettigheder, EUT C 303 af 14.12.2007, s. 1.

⁽⁷⁾ Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (Direktiv om databeskyttelse inden for elektronisk kommunikation), EUT L 201 af 31.7.2002, s. 37.

⁽⁸⁾ Fortolker de vigtigste elementer og betingelser i artikel 8 i den europæiske konvention til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder, som blev vedtaget i Rom den 4. november 1950, idet de finder anvendelse på forskellige områder. Se især den retspraksis, der henvises til andetsteds i udtalelsen.

⁽⁹⁾ Se især sag C-275/06, *Productores de Música de España* (Promusicae), Sml. I, s. 271 og sag C-557/07, *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten*, endnu ikke offentliggjort.

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

⁽⁵⁾ Se fodnote 2 ovenfor.

IV. HÅNDHÆVELSE AF INTELLEKTUELLE EJENDOMSRETTIGHEDER I DET DIGITALE MILJØ

IV.1. Behovet for at analysere, hvilke konsekvenser politikkerne om afbrydelse af internetforbindelsen efter tredje påståede krænkelse (de såkaldte »three-strikes«-politikker) kan have for beskyttelsen af privatlivets fred/databeskyttelse

15. Ifølge Europa-Kommissionen vil ACTA skabe et retsgrundlag til bekæmpelse af piratkopiering i det digitale miljø⁽¹⁰⁾. Dette grundlag vil fastsætte betingelserne for internetudbydere og andre online-mellemleds⁽¹¹⁾ ansvar i forbindelse med materiale, som overtræder reglerne om ophavsret, og som passerer gennem deres faciliteter. Retsgrundlaget kan endvidere danne baggrund for de foranstaltninger og den klageadgang, som internetbrugere skal underlægges, hvis de uploader eller downloader materiale, der overtræder ejendomsrettighederne. Oplysningerne om dette retsgrundlag er ikke officielt frigivet, men der er i lyset af de oplysninger, der er tilgængelige fra forskellige kanaler, grund til at antage, at det vil medføre, at internetudbydere pålægges at vedtage politikker om afbrydelse af internetforbindelsen efter tredje påståede krænkelse (*three strikes Internet disconnection policies*), som også kaldes »graderede reaktions«-ordninger. Disse ordninger vil give copyrightindehavere mulighed for at overvåge internetbrugere og identificere personer, der mistænkes for at overtræde ejendomsrettighederne. Når internetudbydere er blevet underrettet om, at en person mistænkes for at overtræde ejendomsrettighederne, advarer de den pågældende person. Efter tre advarsler afskæres vedkommende fra internetadgang.
16. Sideløbende med ACTA-forhandlingerne gennemføres »three-strikes«-politikkerne i visse medlemsstater, herunder Frankrig. Disse politikker drøftes også i forskellige EU-fora, som f.eks. dialogen med interessenterne om ulovlig upload og download, som GD MARKT har indledt i forbindelse med vedtagelsen af Kommissionens meddelelse om bedre håndhævelse af intellektuelle ejendomsrettigheder i det indre marked⁽¹²⁾. Dette emne drøftes også i Europa-Parlamentet inden for rammerne af den igangværende debat om et udkast til Europa-Parlamentets resolution om bedre håndhævelse af intellektuelle ejendomsrettigheder i det indre marked (benævnt Gallo-betænkningen).

⁽¹⁰⁾ Se fodnote 2 ovenfor.

⁽¹¹⁾ De forskellige online-mellemlid kan defineres på baggrund af deres funktionelle roller. I den virkelige verden skal disse mellemlid som regel udføre flere af disse funktioner. Online-mellemlid omfatter: a) *internetleverandører*: brugerne er koblet på netværket ved tilslutning til en internetleverandørs server, b) *netværksudbydere*: giver adgang til routerne, dvs. de tekniske hjælpemidler, der er nødvendige til overførsel af data, c) *værtsudbydere*: udlejer plads på deres server, hvor brugere eller indholdsudbydere kan uploade indhold. Brugere kan uploade og downloade materiale til en onlinetjeneste, som f.eks. en bulletin eller et P2P-netværk.

⁽¹²⁾ Meddelelse fra Kommissionen til Rådet, Europa-Parlamentet og Det Europæiske Økonomiske og Sociale Udvalg om bedre håndhævelse af intellektuelle ejendomsrettigheder i det indre marked, Bruxelles, den 11. september 2009, KOM(2009) 467 endelig.

17. Disse former for praksis er et voldsomt indgreb i privatlivet. De indebærer en generel overvågning af internetbrugernes aktiviteter, også aktiviteter, som er fuldt lovlige. De påvirker millioner af lovlige internetbrugere, herunder også mange børn og unge. De udføres af private parter og ikke af retshåndhavende myndigheder. Internettet spiller endvidere en central rolle i næsten alle aspekter af det moderne liv, og det har derfor store konsekvenser at blive afskåret fra adgang til internettet, da det også afskærer adgangen til oplysninger om arbejde, kultur, e-forvaltnings-systemer osv.

18. Det er på den baggrund relevant at vurdere, hvorvidt disse politikker er i overensstemmelse med EU's lovgivning om databeskyttelse og beskyttelse af privatlivets fred, herunder især om »three-strikes«-politikkerne er nødvendige for at håndhæve de intellektuelle ejendomsrettigheder. Det bør i den sammenhæng endvidere undersøges, om der findes andre, mindre indgribende metoder.

19. Det er stadig usikkert, om »three-strikes«-politikker vil blive indføjet i ACTA. De behandles imidlertid også inden for andre områder og har potentielt meget store konsekvenser for databeskyttelsen og beskyttelsen af privatlivets fred. Den tilsynsførende mener derfor, at det er meget vigtigt at drøfte dem i denne udtalelse. Inden den ovennævnte analyse indledes, vil den tilsynsførende kort beskrive det gældende retsgrundlag for databeskyttelse og beskyttelse af privatlivets fred.

20. Det skal bemærkes, at »three-strikes«-politikkerne ikke blot vækker bekymring, for så vidt angår databeskyttelse og beskyttelse af privatlivets fred, men også i forbindelse med andre værdier, som f.eks. retten til retfærdig rettergang og ytringsfrihed. Denne udtalelse vil dog kun beskæftige sig med de emner, der har relevans for databeskyttelse og beskyttelse af privatlivets fred.

IV.2. »Three-strikes«-politikkerne og anvendelse af EU's lovgivning om beskyttelse af privatlivets fred/databeskyttelse

Mulig realisering af »three-strikes«-politikkerne

21. Kort sagt giver »three-strikes«-politikkerne copyrightindehavere, der anvender automatiserede tekniske hjælpemidler,

sandsynligvis leveret af tredjeparter, mulighed for at identificere påståede overtrædere af loven om ejendomsrettigheder ved at overvåge internetbrugernes aktiviteter, f.eks. via overvågning af fora, blogs eller ved at optræde som fildelere i peer-to-peer-netværk, for at identificere fildelere, der mistænkes for at udveksle copyright-materiale⁽¹³⁾.

22. Når de internetbrugere, der mistænkes for at have overtrådt lovgivningen om ejendomsrettigheder, er identificeret via indsamling af deres internetprotokoladresser (IP-adresser), sender copyrightindehaverne disse IP-adresser til de relevante internetudbydere, som derefter advarer indehaveren af IP-adressen om dennes mulige overtrædelse af intellektuelle ejendomsrettigheder. Efter et vist antal advarsler fra internetudbyderen, skal denne automatisk afslutte eller ophæve abonnentens adgang til internetforbindelse⁽¹⁴⁾.

Det gældende retsgrundlag for databeskyttelse/beskyttelse af privatlivets fred

23. »Three-strikes«-politikkerne skal overholde kravene til beskyttelse af privatlivets fred, som fastsat i artikel 8 i den europæiske menneskerettighedskonvention og artikel 7 i EU's Charter for Grundlæggende Rettigheder, og stammer fra retten til databeskyttelse som fastsat i artikel 8 i EU's Charter for Grundlæggende Rettigheder og artikel 16 i TEUF og som videreudviklet i direktiv 95/46/EF og direktiv 2002/58/EF.

24. Den tilsynsførende mener, at overvågningen af internetbrugernes adfærd samt registrering af deres IP-adresser er en overtrædelse af deres ret til respekt for deres privatliv og korrespondance. Det er med andre ord en overtrædelse af deres ret til respekt for privatlivet. Denne holdning ligger på linje med Den Europæiske Menneskerettighedsdomstols retspraksis⁽¹⁵⁾.

⁽¹³⁾ P2P-teknologi er en distribueret computersoftwarearkitektur, som giver mulighed for at koble individuelle computere til andre computere og kommunikere direkte med disse.

⁽¹⁴⁾ Som eksempler på alternative sanktioner kan f.eks. nævnes begrænset adgang til internettets forskellige funktioner, f.eks. forbindelseshastigheden, volumen osv.

⁽¹⁵⁾ Se især Den Europæiske Menneskerettighedsdomstol, den 26. juni 2006, *Weber og Saravia mod Tyskland* (dec.), nr. 54934/00, præmis 77, samt ECHR af 1. juli 2008, *Liberty m.fl. mod Det Forenede Kongerige*, nr. 58243/00.

25. Direktiv 95/46/EF finder anvendelse⁽¹⁶⁾, eftersom »three-strikes«-politikkerne omfatter behandling af IP-adresser, som — under de rette omstændigheder — bør betragtes som personoplysninger. IP-adresser er identifikatorer, som ligner en streng af tal adskilt af punktummer, f.eks. 122.41.123.45. Et abonnement hos en internetudbyder giver abonnenten adgang til internettet. Når abonnenten vil på internettet, får han/hun tildelt en IP-adresse via det udstyr, der anvendes til at komme på internettet (f.eks. en computer)⁽¹⁷⁾.

26. Hvis en bruger foretager en given aktivitet, som f.eks. at uploade materiale på internettet, kan en tredjepart identificere brugeren via den IP-adresse, brugeren anvendte. F.eks. uploadede en bruger med IP-adressen 122.41.123.45 angiveligt materiale, der overtræder reglerne om ophavsret, på en P2P-tjeneste kl. 15 den 1. januar 2010. Internetudbyderen kan forbinde IP-adressen til abonnenten og dermed fastslå hans/hendes identitet.

27. Det er på baggrund af artikel 2 i direktiv 95/46/EF, hvor personoplysninger defineres som »enhver form for information om en identificeret eller identificerbar fysisk person (»den registrerede«); ved identificerbar person forstås en person, der direkte eller indirekte kan identificeres, bl.a. ved et identifikationsnummer«⁽¹⁸⁾, kun muligt at konkludere, at IP-adresser og oplysninger om de aktiviteter, der er knyttet til disse adresser, hører ind under definitionen på personoplysninger i de tilfælde, der er relevante i denne sammenhæng. En IP-adresse fungerer som et identifikationsnummer, der gør det muligt at finde frem til navnet på den abonnent, der har fået tildelt IP-adressen. Endvidere omhandler de oplysninger, der indsamles om den abonnent, der har en IP-adresse (»han/hun uploadede materiale på webstedet ZS kl. 15 den 1. januar 2010«), tydeligvis aktiviteter, der udføres af en identificerbar person (indehaveren af IP-adressen), og er dermed at betragte som personoplysninger.

⁽¹⁶⁾ Domstolen indtager en bredtfaende holdning til anvendelsesområdet for direktiv 95/46/EF, hvis bestemmelser skal tolkes i lyset af artikel 8 i ECHR. Domstolen anførte i sin dom af 20. maj 2003, *Rundfunk*, forenede sager C-465/00, C-138/01 og C-139/01, Sml. I, s. 4989, præmis 68, at »bestemmelserne i direktiv 95/46/EF, for så vidt de omhandler behandling af personoplysninger, der kan krænke de grundlæggende frihedsrettigheder og navnlig privatlivets fred, nødvendigvis skal fortolkes under hensyntagen til grundrettighederne, som ifølge fast retspraksis hører til de almindelige retsgrundsætninger, Domstolen skal beskytte«.

⁽¹⁷⁾ Internetudbyderen kan tildele en person den samme IP-adresse, hver gang han/hun surfer på internettet (benævnt en statisk IP-adresse). Andre IP-adresser er dynamiske, dvs. at internetudbyderen tildeler kunden en ny IP-adresse, hver gang han/hun kobler sig på internettet. Internetudbyderen kan naturligvis knytte IP-adressen til kontoen for den abonnent, der har fået tildelt IP-adressen (dynamisk eller statisk).

⁽¹⁸⁾ Definitionen uddybes i betragtning 26: »beskyttelsesprincipperne skal gælde enhver oplysning om en identificeret eller identificerbar person; for at afgøre, om en person er identificerbar, tages alle de hjælpemidler i betragtning, der med rimelighed kan tænkes bragt i anvendelse for at identificere den pågældende enten af den registeransvarlige eller af enhver anden person; beskyttelsesprincipperne gælder ikke oplysninger, som er gjort anonyme på en sådan måde, at den registrerede ikke længere kan identificeres; ...«.

28. Denne opfattelse deles fuldt ud af Artikel 29-Gruppen, der i et dokument vedrørende databeskyttelse i forbindelse med intellektuelle ejendomsrettigheder fastslog, at IP-adresser, der indsamles for at håndhæve de intellektuelle ejendomsrettigheder, dvs. for at identificere internetbrugere, der mistænkes for at have overtrådt intellektuelle ejendomsrettigheder, udgør personoplysninger, for så vidt som de anvendes til at håndhæve disse rettigheder over for en given person⁽¹⁹⁾.

29. Direktiv 2002/58/EF finder også anvendelse, eftersom »three-strikes«-politikkerne omfatter indsamling af trafik- og kommunikationsdata. Direktiv 2002/58/EF indeholder bestemmelser om anvendelsen af denne form for data og fastsætter princippet om kommunikationshemmelighed ved brug af offentlige kommunikationsnet og i forbindelse med de dermed forbundne data.

IV.3. Er »three-strikes«-politikkerne en nødvendig foranstaltning?

30. Den europæiske menneskerettighedskonvention fastsætter i sin artikel 8 nødvendighedsprincippet, ifølge hvilket enhver foranstaltning, der krænker fysiske personers ret til privatliv, kun er tilladt, hvis den er berettiget ud fra et legitimt formål og er nødvendig i et demokratisk samfund⁽²⁰⁾. Nødvendighedsprincippet er også anført i artikel 7 og 13 i direktiv 95/46/EF og artikel 15 i direktiv 2002/58/EF⁽²¹⁾. For at efterleve dette princip skal der foretages en analyse af foranstaltningens forholdsmæssighed, vurderet ud fra en passende balance mellem de interesse-

rede parter og med hensyntagen til det demokratiske samfund som helhed⁽²²⁾. Det indebærer endvidere en vurdering af, om der findes alternative, mindre indgribende foranstaltninger.

31. Selvom den tilsynsførende anerkender vigtigheden af at styrke de intellektuelle ejendomsrettigheder, mener han, at »three-strikes«-politikkerne i deres nuværende form, hvor de involverer visse generelle elementer, er en uforholdsmæssig foranstaltning og derfor ikke kan betragtes som nødvendige. Den tilsynsførende er ydermere overbevist om, at det er muligt at finde alternative, mindre indgribende løsninger, eller at de planlagte politikker kan gennemføres på en mindre indgribende måde eller med et mere begrænset anvendelsesområde. På et mere detaljeret juridisk plan rejser denne fremgangsmåde også problemer. Konklusionerne i denne forbindelse forklares i det nedenstående.

»Three-strikes«-ordningen er uforholdsmæssig

32. Den tilsynsførende ønsker at understrege de pålagte foranstaltningers vidtrækkende natur. Det er i den henseende nødvendigt at gøre opmærksom på følgende elementer:

i) det forhold, at (ubemærket) overvågning påvirker millionvis af fysiske personer samt *alle* brugere, uanset om de er mistænkt for overtrædelser eller ej.

ii) overvågningen indebærer systematisk registrering af data, hvoraf flere kan føre til civile og endog strafretlige søgsmål. Visse af de indsamlede oplysninger kan endvidere kvalificeres som følsomme data i henhold til artikel 8 i direktiv 95/46/EF, som indeholder krav om strengere garantier.

iii) overvågningen risikerer at føre til mange tilfælde af falske positive. Spørgsmålet om, hvorvidt ejendomsrettighederne er overtrådt, kan sjældent besvaret med et klart »ja« eller »nej«. Domstolene skal ofte behandle et stort antal tekniske og juridiske oplysninger og meget lange sagsbeskrivelser, før de kan afgøre, hvorvidt der er tale om en overtrædelse eller ej⁽²³⁾.

⁽¹⁹⁾ Artikel 29-Gruppens arbejdsdokument vedrørende databeskyttelse i forbindelse med intellektuelle ejendomsrettigheder (WP 104), vedtaget den 18. januar 2005. Denne gruppe nedsættes i medfør af artikel 29 i direktiv 95/46/EF. Den er en uafhængig europæisk tilsynsmyndighed for databeskyttelse og beskyttelse af privatlivet. Dens opgaver er beskrevet i artikel 30 i direktiv 95/46/EF og artikel 15 i direktiv 2002/58/EF. Der henvises også til gruppens udtalelse 4/2007 om begrebet personoplysninger (WP 136), vedtaget den 20. juni 2007, navnlig s. 16.

⁽²⁰⁾ Artikel 8 i Den Europæiske Menneskerettighedskonvention henviser udtrykkeligt til kravet om, at ethvert indgreb eller enhver begrænsning skal være »nødvendigt i et demokratisk samfund«.

⁽²¹⁾ Det er i henhold til artikel 13 i direktiv 95/46/EF kun muligt at indføre en begrænsning, hvis den er »en nødvendig foranstaltning af hensyn til: a) statens sikkerhed, b) forsvaret, c) den offentlige sikkerhed, d) forebyggelse, efterforskning, afsløring og retsforfølgning i straffesager eller i forbindelse med brud på etiske regler for lovregulerede erhverv, e) væsentlige økonomiske eller finansielle interesser hos en medlemsstat eller Den Europæiske Union, herunder valuta-, budget- og skatteanliggender; f) en kontrol-, tilsyns- eller reguleringsopgave, selv af midlertidig karakter, der er et led i den offentlige myndighedsudøvelse på de i litra c), d) og e) nævnte områder, g) beskyttelsen af den registreredes interesser eller andres rettigheder og frihedsrettigheder«. I henhold til artikel 15 i direktiv 2002/58/EF kan en sådan indskrænkning kun vedtages, hvis den »er nødvendig, passende og forholdsmæssig i et demokratisk samfund af hensyn til den nationale sikkerhed (dvs. statens sikkerhed), forsvaret, den offentlige sikkerhed, eller forebyggelse, efterforskning, afsløring og retsforfølgning i straffesager eller uautoriseret brug af det elektroniske kommunikationssystem efter artikel 13, stk. 1, i direktiv 95/46/EF«.

⁽²²⁾ Se også Den Europæiske Menneskerettighedsdomstol, den 2. august 1984, *Malone mod Det Forenede Kongerige*, serie A, nr. 82, s. 32, præmis 81 og s. samt Den Europæiske Menneskerettighedsdomstol, den 4. december 2008, *Marper mod Det Forenede Kongerige* [GC], nr. 30562/04 og 30566/04, præmis 101 og s.

⁽²³⁾ Domstolene skal bl.a. vurdere: om materialet er ophavsretligt beskyttet, om der er sket en krænkelse af rettigheder, om anvendelsen kan anses for at være rimelig, gældende lovgivning, skader osv.

- iv) overvågningens eventuelle konsekvenser, som kan føre til spærring af internetadgangen. Dette kan være i strid med individers ret til ytringsfrihed og til information og med deres adgang til kultur, e-forvaltningssystemer, markedsadgang, e-mail og i visse tilfælde arbejdsrelaterede aktiviteter. Det er i den forbindelse især vigtigt at være opmærksom på, at konsekvenserne ikke blot vil ramme den påståede lovovertræder, men alle hans/hendes familiemedlemmer med samme internetopkobling, herunder skoleelever, der har brug for internetadgang i forbindelse med deres skoleaktiviteter.
- v) det forhold, at den enhed, der foretager vurderingen og træffer afgørelsen, typisk er en privat enhed (dvs. copyrighthaverne eller internetudbyderen). Den tilsynsførende har tidligere givet udtryk for sine betænkeligheder angående den private sektors (f.eks. internetudbydere eller copyrighthaveres) overvågning af fysiske personer på områder, der i princippet henhører under de retshåndhævende myndigheders kompetence ⁽²⁴⁾.
33. Den tilsynsførende er ikke overbevist om, at foranstaltningernes fordele opvejer deres konsekvenser for fysiske personers grundlæggende rettigheder. Det er i rettighedsindehavernes og samfundets interesse at beskytte ophavsretten. Indskrænkningerne af de grundlæggende rettigheder forekommer imidlertid ikke berettigede, hvis man sammenholder konsekvenserne af indgrebet, dvs. omfanget af indgrebet i privatlivet som illustreret i det ovenstående, med det forventede udbytte, idet det oftest forhindrer meget små overtrædelser af intellektuelle ejendomsrettigheder. Som angivet i generaladvokat Kokotts forslag til afgørelse i sagen »Promusicae«: »Det er ikke sikkert, at privat filesharing, navnlig når det foregår uden vinding for øje, udgør en tilstrækkeligt alvorlig trussel mod ophavsrettigheder til at begrunde, at denne undtagelse bringes i anvendelse. Hvorvidt privat filesharing forårsager en ægte skade, er nemlig omtvistet« ⁽²⁵⁾.
34. Der skal i denne sammenhæng også mindes om Europa-Parlamentets reaktion på »three-strikes«-ordningerne i forbindelse med gennemgangen af telekommunikationspakken, navnlig ændringsforslag 138 til rammedirektivet ⁽²⁶⁾. I henhold til dette ændringsforslag må foranstaltninger, der kan begrænse disse grundlæggende rettigheder eller frihedsrettigheder, kun indføres, hvis de er hensigtsmæssige, forholdsmæssigt afpassede og nødvendige i et demokratisk samfund, og gennemførelsen af dem skal være undergivet passende proceduremæssige garantier i overensstemmelse med den europæiske konvention til
- beskyttelse af menneskerettigheder og med fællesskabsrettens generelle principper, herunder effektiv retsbeskyttelse og ret til en retfærdig rettergang ⁽²⁷⁾.
35. Hvad dette angår, understreger den tilsynsførende desuden, at enhver begrænsning af de grundlæggende rettigheder vil blive underkastet en grundig behandling på både EU-plan og nationalt plan. Der kan i den forbindelse trækkes en parallel til direktiv 2006/24/EF ⁽²⁸⁾ om lagring af data. Der afviges heri fra det generelle databeskyttelsesprincip om sletning af data, så snart de ikke længere er nødvendige til det formål, hvortil de blev indsamlet eller behandlet. Dette direktiv indeholder krav om, at trafikdata lagres som led i bekæmpelsen af grov kriminalitet. Det skal bemærkes, at lagring kun er tilladt i forbindelse med »grov kriminalitet«, at lagringen er begrænset til »trafikdata«, hvilket i princippet udelukker oplysninger om indholdet af kommunikationerne, og at der skal ydes strenge garantier. Der er ikke desto mindre blevet rejst tvivl om dets forenelighed med de grundlæggende rettigheder. Forfatningsdomstolen i Rumænien fastslog, at en omfattende lagring er uforenelig med grundlæggende rettigheder ⁽²⁹⁾. Der verserer ligeledes en sag ved forfatningsdomstolen i Tyskland ⁽³⁰⁾.

Andre, mindre indgribende modeller

36. Ovenstående resultater understøttes af, at der findes mindre indgribende modeller til opnåelse af det samme formål. Den tilsynsførende insisterer på, at disse mindre indgribende modeller undersøges nærmere og afprøves i praksis.

⁽²⁴⁾ Udtalelse fra Den Europæiske Tilsynsførende for Databeskyttelse af 23. juni 2008 om forslaget til Europa-Parlamentets og Rådets afgørelse om et flerårigt fællesskabsprogram til beskyttelse af børn, der bruger internet og andre kommunikationsteknologi, EUT C 2 af 7.1.2009, s. 2.

⁽²⁵⁾ Se fodnote 8, præmis 106, i den sag, der henvises til.

⁽²⁶⁾ Se Europa-Parlamentets og Rådets direktiv 2009/140/EF af 25. november 2009, EUT L 337 af 18.12.2009, s. 37.

⁽²⁷⁾ Den endelige ordlyd af ændringsforslag 138 er som følger: »Artikel 1, stk. 3a. Foranstaltninger truffet af medlemsstaterne vedrørende slutbrugeres adgang til eller benyttelse af tjenester og applikationer via elektroniske kommunikationsnet skal overholde fysiske personers grundlæggende rettigheder og frihedsrettigheder, som de garanteres ved den europæiske konvention til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder og fællesskabsrettens generelle principper. De af disse foranstaltninger vedrørende slutbrugeres adgang til eller benyttelse af tjenester og applikationer via elektroniske kommunikationsnet, der kan begrænse disse grundlæggende rettigheder eller frihedsrettigheder, må kun indføres, hvis de er hensigtsmæssige, forholdsmæssigt afpassede og nødvendige i et demokratisk samfund, og gennemførelsen af dem skal være undergivet passende proceduremæssige garantier i overensstemmelse med den europæiske konvention til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder og med fællesskabsrettens generelle principper, herunder effektiv retsbeskyttelse og ret til en retfærdig rettergang. Følgelig må disse foranstaltninger kun træffes under hensyntagen til princippet om uskyldsfornødning og retten til privatlivets fred. En forudgående, retfærdig og upartisk procedure skal garanteres, herunder den eller de berørte personers ret til at blive hørt, med forbehold af behovet for passende betingelser og proceduremæssige ordninger i behørigt begrundede hastetilfælde i overensstemmelse med den europæiske konvention til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder. Retten til en effektiv og rettidig domstolskontrol skal garanteres.«

⁽²⁸⁾ Europa-Parlamentets og Rådets direktiv 2006/24/EF af 15. marts 2006, EUT L 105 af 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. Den tilsynsførende minder om, at det ændrede direktiv 2002/22/EF om forsyningspligt og brugerrettigheder i forbindelse med elektroniske kommunikationsnet og -tjenester (»forsyningspligtdirektivet«), som indgår i den nyligt reviderede telekommunikationspakke, indeholder visse bestemmelser og procedurer, som har til formål at begrænse mindre grove overtrædelser af ophavsretten blandt forbrugerne⁽³¹⁾. Disse procedurer omfatter en forpligtelse for medlemsstaterne til at offentliggøre standardiserede oplysninger af offentlig interesse om forskellige emner, og der gøres specifikt opmærksom på overtrædelser af ophavsretten og beslægtede rettigheder og de retlige konsekvenser heraf⁽³²⁾. Medlemsstater kan pålægge internetudbydere at videreformidle sådanne oplysninger til alle deres kunder og indføje det i deres kontrakter.
38. Systemet har til formål at informere og afskrække fysiske personer fra at videreformidle oplysninger, der er underlagt ophavsret, og fra at udføre aktiviteter, der krænker ophavsretten, samtidig med at man undgår overvågning af brugen af internettet og tilknyttede aspekter vedrørende privatlivets fred og databeskyttelse. Forsyningspligtdirektivet skal gennemføres inden maj 2011, og de omtalte procedurer er derfor endnu ikke indført. Det har følgelig endnu ikke været muligt at afprøve deres fordele. Det forekommer derfor at være for tidligt at få et overblik over det eventuelle positive udbytte af disse nye procedurer for i stedet at fokusere på »three-strikes«-politikkerne, som medfører langt større indskrænkninger af de grundlæggende rettigheder.
39. Der skal udover ovenstående også mindes om, at direktiv 2004/48/EF af 28. april 2004 om håndhævelsen af intellektuelle rettigheder indeholder en række forskellige redskaber til at håndhæve de intellektuelle rettigheder ved domstolene (der drøftes nedenfor i punkt 43 og s)⁽³³⁾.
40. IPRE-direktivet er først for nylig blevet gennemført i medlemsstaternes nationale lovgivning. Det er derfor for tidligt at vurdere, om bestemmelserne i direktivet er velegnede til at sikre håndhævelse af intellektuelle ejendomsrettigheder. Der må således stilles spørgsmålstegn ved behovet for at udskifte det nuværende retsbaserede system, der endnu ikke er blevet afprøvet. Ovenstående rejser naturligt spørgsmålet om, hvorfor eksisterende overtrædelser ikke kan håndteres hensigtsmæssigt inden for rammerne af de gældende civil- og strafferetlige sanktioner for overtrædelse af reglerne om ophavsret. Inden Kommissionen foreslår sådanne politiske foranstaltninger, bør den derfor tilvejebringe pålidelige oplysninger, der påviser, at de nuværende juridiske rammer ikke har haft de ønskede virkninger.
41. Det står heller ikke klart, hvorvidt man har overvejet alternative økonomiske forretningsmodeller, som ikke involverer systematisk overvågning af fysiske personer. Hvis f.eks. copyrightindehavere kan påvise tab på grund af brug af P2P, kan rettighedsindehavere og internetudbydere tilbyde abonnemeter med differentieret internetadgang, hvor en del af betalingen for et abonnement med ubegrænset adgang sendes videre til copyrightindehaverne.
- Muligheden for at foretage en målrettet, men mindre indgribende, overvågning*
42. Udover brug af vidt forskellige modeller, der som nævnt bør undersøges nærmere og afprøves, er det under alle omstændigheder muligt at foretage målrettet overvågning på en mindre indgribende måde.
43. De intellektuelle ejendomsrettigheder kan også håndhæves via overvågning af et begrænset antal fysiske personer, der mistænkes for alvorligere overtrædelser af reglerne om ophavsret. IPRE-direktivet indeholder visse retningslinjer i denne forbindelse. Det fastsætter, under hvilke betingelser myndighederne kan kræve, at personoplysninger i internetudbydernes varetægt skal udleveres med henblik på håndhævelse af intellektuelle ejendomsrettigheder. I henhold til artikel 8 kan de kompetente retslige myndigheder som svar på en velbegrundet og forholdsmæssig afpasset begæring pålægge internetudbydere at give oplysninger om oprindelsen af og distributionskanalerne for de varer eller tjenesteydelser, der krænker en intellektuel ejendomsrettighed, såfremt der er tale om overtrædelser i *kommerciel målestok*⁽³⁴⁾.
44. Kriteriet om »kommerciel målestok« er derfor afgørende. I henhold til dette kriterium kan overvågning være forholdsmæssig afpasset til begrænsede, enkeltstående situationer,

⁽³¹⁾ Se Europa-Parlamentets og Rådets direktiv 2009/136/EF af 25. november 2009, EUT L 337 af 18.12.2009, s. 11.

⁽³²⁾ Det fastsættes navnlig i artikel 21, stk. 4, i direktiv 2009/136/EF, at »Medlemsstaterne kan kræve, at virksomheder som omhandlet i stk. 3 videreformidler almenyttige oplysninger gratis til eksisterende og nye abonnenter, hvor dette er relevant, under anvendelse af de samme midler, som virksomhederne sædvanligvis benytter til at kommunikere med abonnenterne. I så fald leveres disse oplysninger af de relevante offentlige myndigheder i et standardiseret format og omfatter bl.a. følgende emner: a) de mest gængse former for anvendelse af elektroniske kommunikationstjenester til at foretage ulovlige handlinger eller formidle skadeligt indhold, især hvor dette kan skade respekten for andres rettigheder og frihedsrettigheder, herunder overtrædelser af ophavsretten og beslægtede rettigheder og de retlige konsekvenser heraf (...).« I artikel 20, stk. 1, hedder det videre, at »Medlemsstaterne kan også kræve, at kontrakten skal indeholde enhver oplysning, som de relevante offentlige myndigheder måtte give til dette formål om brugen af elektroniske kommunikationsnet og -tjenester til at foretage ulovlige handlinger eller til at formidle skadeligt indhold, samt om midler til at beskytte mod trusler mod den personlige sikkerhed, privatlivets fred og personoplysninger, jf. artikel 21, stk. 4, som er relevante for den pågældende ydelse«.

⁽³³⁾ EUT L 157 af 30.4.2004, s. 45 (herefter benævnt IPRE-direktivet).

⁽³⁴⁾ Dette bekræftes også i betragtning 14 i IPRE-direktivet.

hvor der foreligger velbegrunder mistanke om misbrug af ejendomsrettigheder i kommerciel målestok. Dette kriterium omfatter tilfælde af privatpersoners tydelige misbrug af ejendomsrettigheder, som har til formål at opnå direkte eller indirekte økonomiske eller kommercielle fordele.

45. For at ovennævnte skal være effektivt kan copyrightindehavere foretage målrettet overvågning af visse IP-adresser for at fastlægge omfanget af overtrædelser. Det betyder, at copyrightindehavere også vil få mulighed for at registrere rapporter om påståede overtrædelser. Sådanne oplysninger bør først anvendes, efter at overtrædelsens betydning er blevet konstateret. Der kan f.eks. være tale om tydelige tilfælde af grove overtrædelser samt mindre, men gentagne overtrædelser over en vis periode, som har til formål at skaffe lovovertræderen kommercielle eller økonomiske fordele. Kriteriet om, at der skal være sket gentagne overtrædelser inden for en vis periode, fremhæves og forklares mere detaljeret i nedenstående drøftelse af princippet om opbevaring.
46. Det betyder, at indsamlingen af oplysninger med henblik på at påvise internetmisbrug i disse tilfælde kan anses for at være forholdsmæssig og nødvendig for forberedelsen af retlige skridt, herunder retssager.
47. Den tilsynsførende mener, at de nationale databeskyttelsesmyndigheder som en ekstra garanti bør forhåndskontrollere og forhåndsgodkende databehandling, der har til formål at indsamle denne form for dokumentation. Det skyldes, at databehandlingerne vil udgøre en specifik risiko for fysiske personers rettigheder og frihedsrettigheder i kraft af deres formål, dvs. håndhævelsesforanstaltninger, som kan vise sig at være retsstridige, samt i lyset af de indsamlede datas følsomhed. Det faktum, at behandlingen indebærer overvågning af elektroniske kommunikationer, understøtter behovet for øget tilsyn.
48. Den tilsynsførende mener, at IPRE-direktivets kriterium om »kommerciel målestok« er meget velegnet til at fastsætte grænserne for overvågningen, så proportionalitetsprincippet overholdes. Der foreligger desuden ingen pålidelig dokumentation for, at det ikke er muligt at træffe effektive retlige skridt mod overtrædelse af reglerne om ophavsret i henhold til IPRE-direktivets kriterier. At det modsatte synes at være tilfældet fremgår bl.a. af rapporter fra Tyskland, hvor der efter gennemførelsen af IPRE-direktivet i 2008 er blevet udstedt cirka 3 000 retsafgørelser, der pålægger internetudbydere at udlevere oplysninger om 300 000 abonnenter til domstolene.
49. Eftersom IPRE-direktivet kun har været i kraft i to år, er det sammenfattende vanskeligt at forstå, hvorfor lovgiverne ønsker at tilsidesætte de kriterier, der fastsættes i dette direktiv, til fordel for mere indgribende metoder, når EU netop er begyndt at teste de nye metoder, der er vedtaget.

Det er af samme årsag også vanskeligt at forstå behovet for at udskifte det nuværende retsbaserede system med andre former for foranstaltninger (ud over at rejse spørgsmålet om en retfærdig rettergang, som ikke vil blive behandlet her).

IV.4. »Three-strikes«-politikkerne og deres overensstemmelse med mere detaljerede databeskyttelsesbestemmelser

50. Der er andre mere specifikke juridiske årsager til, at »three-strikes«-ordningen er problematisk i forhold til databeskyttelse. Den tilsynsførende ønsker at sætte fokus på det tvivlsomme retsgrundlag for den behandling, som fastsættes i direktiv 95/46/EF, og den forpligtelse til at slette logfiler, der fastsættes i direktiv 2002/58/EF.

Retsgrundlag for databehandling

51. »Three-strikes«-ordningerne indebærer behandling af personoplysninger, hvoraf nogle vil blive anvendt i forbindelse med de retslige eller administrative procedurer til spærring af internetadgangen for personer, der gentagne gange har overtrådt reglerne om ophavsret. På denne baggrund kvalificerer sådanne oplysninger sig som følsomme oplysninger i henhold til artikel 8 i direktiv 95/46/EF. Det fastsættes i artikel 8, stk. 5, at »Behandling af oplysninger om lovovertrædelser, straffedomme eller sikkerhedsforanstaltninger må kun foretages under kontrol af en offentlig myndighed, eller hvis der gælder tilstrækkelige, specifikke garantier i medfør af den nationale lovgivning ...«.
52. Der skal i denne sammenhæng atter gøres opmærksom på artikel 29-Gruppens udtalelse, hvori behandlingen af juridiske data drøftes⁽³⁵⁾. Gruppen anfører, at »Enhver person har naturligvis ret til at behandle juridiske data i forbindelse med vedkommendes egen retsvist, men princippet er ikke så vidtrækkende, at det tillader, at tredjemand foretager indgående efterforskning, indsamling og centralisering af personoplysninger, herunder navnlig en systematisk generel efterforskning, som f.eks. søgning på internettet (...). En sådan efterforskning hører under de retlige myndigheder«⁽³⁶⁾. Selv om det kan være nødvendigt at indsamle målrettet, specifik dokumentation, navnlig i forbindelse med grove overtrædelser, for at fremsætte et retskrav, er den tilsynsførende helt enig med Artikel 29-Gruppen, for så vidt angår den manglende legitimitet ved efterforskninger i stor skala, der omfatter behandling af enorme mængder data om internetbrugere.
53. Ovenfor beskrevne drøftelse af proportionalitetsprincippet og kriteriet om »kommerciel målestok« er relevant for at fastsætte, på hvilke betingelser det vil være legitimt at indsamle IP-adresser og dertil hørende oplysninger.

⁽³⁵⁾ Se stk. 28 i denne udtalelse.

⁽³⁶⁾ Fremhævelse tilføjet.

54. Internetudbydere kan forsøge at lovliggøre den behandling, som copyrightindehavere foretager, ved at indsætte klausuler i deres kundekontrakter, der giver dem mulighed for at overvåge kundernes data og annullere deres abonnementer. Kunder, der har underskrevet sådanne kontrakter, vil blive anset for at have godkendt overvågningen. Denne fremgangsmåde rejser imidlertid først og fremmest det grundlæggende spørgsmål om, hvorvidt fysiske personer kan give internetudbyderen deres samtykke til en databehandling, der ikke udføres af internetudbyderen, men af tredjeparter, som ikke hører under internetudbyderens ansvarsområde.

55. Dernæst rejser den spørgsmålet om gyldigheden af samtykker. I artikel 2, litra h), i direktiv 95/46/EF, defineres samtykke som »enhver frivillig, specifik og informeret viljetilkendegivelse, hvorved den registrerede indvilliger i, at personoplysninger, der vedrører den pågældende selv, gøres til genstand for behandling«. Det er i den forbindelse vigtigt, at et samtykke for at være gyldigt, uanset de omstændigheder, hvorunder det er givet, skal være en frivillig, specifik og informeret viljetilkendegivelse af den registreredes ønsker, som fastsat i direktivets artikel 2, litra h). Den tilsynsførende er alvorligt i tvivl om, hvorvidt fysiske personer, der bedes om at give deres samtykke til overvågning af deres internetaktiviteter, vil have et reelt valg, ikke mindst fordi alternativet er ikke at have internetadgang, hvilket udgør en potentiel trussel mod mange andre områder af deres liv.

56. For det tredje er det yderst tvivlsomt, om denne form for overvågning nogensinde vil kunne anses for at være *nødvendig* af hensyn til opfyldelsen af en kontrakt, som den registrerede er part i, som påkrævet i artikel 7, litra b) i direktiv 95/46/EF, eftersom overvågningen tydeligvis ikke indgår som del af den kontrakt, den registrerede har indgået, men blot er et middel for internetudbyderen til at varetage andre interesser.

Sletning af logfiler

57. I henhold til direktiv 2002/58/EF, mere præcist artikel 6, må trafikdata som f.eks. IP-adresser, kun indsamles og opbevares i forbindelse med formål, der er direkte relateret til selve kommunikationen, herunder debitering, trafikstyring og forebyggelse af svig. Derefter skal oplysningerne slettes. Dette berører ikke de forpligtelser, der fastsættes i direktivet om lagring af data, der som nævnt, kræver, at trafikdata opbevares og **kun** udleveres til politi og anklagemyndighed for at bidrage til en efterforskning af **grov kriminalitet** ⁽³⁷⁾.

⁽³⁷⁾ Se stk. 35 i denne udtalelse.

58. I henhold til ovenstående skal internetudbydere kun slette logfiler, der viser aktiviteter, som ikke længere er nødvendige til ovennævnte formål. Eftersom logfiler ikke er nødvendige i forbindelse med debitering, burde tre til fire uger være tilstrækkelig til, at internetudbyderne kan foretage trafikstyring ⁽³⁸⁾.

59. Det betyder, at internetudbydere ikke bør linke logfilerne til de relevante abonnenters IP-adresser, når de kontaktes af copyrightindehavere, medmindre det sker inden for den begrænsede periode, der beskrives ovenfor. Logfiler bør kun lagres ud over denne periode, hvis det er berettiget og ligger inden for de formål, der fastsættes i lovgivningen.

60. Det betyder i praksis, at internetudbydere ikke kan imødekomme copyrightindehaveres anmodning, medmindre anmodningen fremsættes meget hurtigt, da de ganske enkelt ikke længere er i besiddelse af oplysningerne. Det er i sig selv med til at definere, hvad der menes med de acceptable overvågningspraksisser, der beskrives i ovenstående afsnit.

Risiko for afledte virkninger

61. Den tilsynsførende er ikke blot bekymret for de virkninger, som »three-strikes«-politikkerne vil få for privatlivets fred og databeskyttelsen, men også for deres afledte virkninger. Godkendelse af »three-strikes«-politikker kan være en glidebane, der fører til endnu mere overvågning af internetbrugeres aktiviteter inden for forskellige områder og med forskellige formål.

62. Den tilsynsførende opfordrer indtrængende Kommissionen til at sikre, at ACTA ikke går videre og ikke undergraver EU's eksisterende ordning til håndhævelse af intellektuelle ejendomsrettigheder, som overholder grundlæggende rettigheder, frihedsrettigheder og borgerrettigheder, som f.eks. beskyttelse af personoplysninger.

V. DATABESKYTTELSESFORBEHOLD MED HENSYN TIL INTERNATIONALE SAMARBEJDSMEKANISMER

63. Med hensyn til spørgsmålet om håndhævelse af ejendomsrettigheder er det inden for rammerne af ACTA blevet foreslået at styrke det internationale samarbejde med en række

⁽³⁸⁾ Trafikstyring omfatter analyser af netværkstrafikken på computerne for at optimere eller sikre ydeevnen, kortere reaktionstid og/eller øget båndbredde.

foranstaltninger, der muliggør en effektiv håndhævelse af intellektuelle ejendomsrettigheder inden for ACTA-underskriverens jurisdiktioner.

64. Hvad angår de tilgængelige oplysninger, vil en række af de foranstaltninger, der er planlagt for at sikre håndhævelse af intellektuelle ejendomsrettigheder antageligt indebære international udveksling af oplysninger om påståede krænkelse af de intellektuelle ejendomsrettigheder blandt offentlige myndigheder (såsom toldmyndigheder, politi og retsvæsen) samt mellem offentlige og private aktører (såsom internetudbydere og organisationer med IP-rettigheder). Denne form for dataoverførsler rejser en række spørgsmål vedrørende databeskyttelse.

V.1. Er de dataudvekslinger, der planlægges inden for rammerne af ACTA, legitime, nødvendige og forholdsmæssige?

65. På det nuværende stadie af forhandlingsprocessen, hvor en række konkrete elementer af databehandlingen stadig ikke er definerede eller kendte, er det umuligt at fastslå, om de foreslåede foranstaltninger er i overensstemmelse med grundlæggende databeskyttelsesprincipper og EU's databeskyttelseslovgivning.
66. For det første er det tvivlsomt, om dataoverførsler til tredjelande inden for rammerne af ACTA er legitime. Det er også tvivlsomt, om de foranstaltninger, der er vedtaget på området på internationalt plan, er relevante, så længe der ikke foreligger en aftale mellem EU-medlemsstaterne om harmonisering af håndhævelsesforanstaltningerne i det digitale miljø samt om de former for strafferetlige sanktioner, der skal anvendes⁽³⁹⁾.
67. Det ser i lyset af det ovenstående ud til, at det vil være nemmere at overholde principperne om nødvendighed og forholdsmæssighed i forbindelse med dataoverførsler under ACTA, hvis aftalen udtrykkeligt begrænses til at omfatte bekæmpelse af de groveste overtrædelser af de intellektuelle ejendomsrettigheder, og ikke overførsler af massedata ved enhver mistanke om krænkelse af de intellektuelle ejendomsrettigheder. Det forudsætter en nøjagtig definition af de »groveste overtrædelser af de intellektuelle ejendomsrettigheder«, hvor dataoverførsel er tilladt.
68. Det er endvidere vigtigt at være opmærksom på de personer, der er involveret i dataudvekslingerne, samt på hvorvidt oplysningerne kun vil blive delt mellem offentlige myndigheder, eller om de også vil omfatte udvekslinger mellem private aktører og offentlige myndigheder. Som nævnt tidligere i denne udtalelse rejser inddragelsen af private aktører på et område, der i princippet hører under de retshåndhavende myndigheders kompetence, en række spørgsmål⁽⁴⁰⁾. Betingelserne for, hvornår private

aktører kan involveres i indsamling og udveksling af personoplysninger i forbindelse med overtrædelser af de intellektuelle ejendomsrettigheder med offentlige myndigheder, bør begrænses til særlige omstændigheder og ledsages af de fornødne garantier.

V.2. Gældende lovgivning om databeskyttelse, der finder anvendelse på videregivelse af personoplysninger inden for rammerne af ACTA

En generel ordning for videregivelse af personoplysninger

69. EU's generelle rammer for databeskyttelse er fastsat i direktiv 95/46/EF. I artikel 25 og 26 i dette direktiv fastsættes den ordning, der er gældende for videregivelse af personoplysninger til tredjelande. Artikel 25 indeholder krav om, at videregivelse kun må finde sted til lande, der sikrer et tilstrækkeligt beskyttelsesniveau. Er dette ikke tilfældet, er videregivelse af personoplysninger i princippet forbudt.
70. Vurderingen af, om beskyttelsesniveauet i et tredjeland er tilstrækkeligt, foretages af Europa-Kommissionen fra sag til sag. Kommissionen har på baggrund af grundige analyser fra Artikel 29-Gruppen truffet adskillige beslutninger, hvori den godkender beskyttelsesniveauet i en række lande⁽⁴¹⁾.
71. Den tilsynsførende bemærker, at de fleste deltagere i ACTA ikke figurerer på denne liste over lande, der leverer en tilstrækkelig databeskyttelse, som Kommissionen har udarbejdet. Med undtagelse af Schweiz og — under visse omstændigheder — Canada og USA har ingen andre deltagere i ACTA fået vurderet deres beskyttelsesniveau til at være tilstrækkeligt. For at der kan videregives oplysninger fra EU til disse lande, skal en af betingelserne i artikel 26, stk. 1, i direktiv 95/46/EF derfor være opfyldt, eller parterne i videregivelsen skal angive tilstrækkelige garantier i overensstemmelse med direktivets artikel 26, stk. 2.
- Særlig ordning for videregivelse af oplysninger på det strafferetlige område*
72. Selv om direktiv 95/46/EF er det vigtigste databeskyttelsesinstrument i EU, er dets anvendelsesområde begrænset, idet det udelukker en række aktiviteter, bl.a. statens aktiviteter på det strafferetlige område (artikel 3). Videregivelse af oplysninger på det strafferetlige område falder derfor uden for anvendelsesområdet for direktiv 95/46/EF og er underlagt de generelle databeskyttelsesprincipper, der er

⁽³⁹⁾ Et forslag om strafferetlige sanktioner drøftes aktuelt i Rådet, KOM(2006) 168 af 26. april 2006.

⁽⁴⁰⁾ Se punkt 32 og 52 i denne udtalelse. Se endvidere Udtalelse fra Den Europæiske Tilsynsførende for Databeskyttelse om den endelige rapport fra EU-USA-Kontaktgruppen på Højt Plan om Informationsdeling og Beskyttelse af Privatlivets Fred og Personoplysninger, EUT C 128 af 6.6.2009, s.1.

⁽⁴¹⁾ Jf. Europa-Kommissionens beslutninger om konstatering af et tilstrækkeligt beskyttelsesniveau i Argentina, Canada, Schweiz, den amerikanske safe harbor-ordning og de amerikanske myndigheder i forbindelse med PNR-systemet, Guernsey, Isle of Man, og Jersey. Beslutningerne kan ses på http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm

fastsat i Europarådets konvention nr. 108 og dens tillægsprotokol, som alle EU-medlemsstater er part i⁽⁴²⁾. Derudover finder de bestemmelser, EU har vedtaget vedrørende politisamarbejde og retligt samarbejde i kriminalsager, og som er fastsat i Rådets rammeafgørelse 2008/877/RIA, også anvendelse⁽⁴³⁾.

73. Disse instrumenter bygger ligeledes på det princip, at der skal være et tilstrækkeligt beskyttelsesniveau i det tredjeland, som oplysningerne videregives til. Der findes en række undtagelser herfra, navnlig hvis tredjelandet yder tilstrækkelige garantier. I lighed med videregivelse af oplysninger i henhold til direktiv 95/46/EF kræver udveksling af oplysninger på det strafferetlige område derfor, at parterne i udvekslingen yder tilstrækkelige garantier.

Mod en ny ordning for videregivelse af oplysninger

74. EU vil sandsynligvis inden for en nær fremtid vedtage nye fælles regler for databeskyttelse på grundlag af artikel 16 i TEUF. Disse regler vil være gældende for alle EU's aktivitetsområder. Det betyder, at der inden for få år kan være indført omfattende rammer for databeskyttelse i EU, med sammenhængende regler for databeskyttelse inden for alle EU's aktivitetsområder, hvilket vil betyde ensartede garantier for alle databehandlingsaktiviteter. Som beskrevet af EU's kommissær for retlige anliggender, grundlæggende rettigheder og borgerskab, Viviane Reding⁽⁴⁴⁾, skal disse nye rammer fungere som et fælles »moderne og omfattende retsinstrument« for databeskyttelse i EU. Dette nye retsinstrument hilses ikke mindst velkommen, fordi det vil bidrage til at gøre EU's regler for databeskyttelse mere tydelige og sammenhængende.
75. I en international sammenhæng henviser den tilsynsførende også til resolutionen om internationale standarder for beskyttelse af personoplysninger og privatlivet, som netop er vedtaget af databeskyttelsesmyndighederne, og som er første skridt i retning af indførelse af internationale standarder for databeskyttelse⁽⁴⁵⁾. De internationale standarder omfatter en række databeskyttelsesgarantier på linje med de garantier, der anføres i direktiv 95/46/EF og konvention nr.

⁽⁴²⁾ Europarådets konvention om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger, vedtaget i Strasbourg den 28. januar 1981 og tillægsprotokollen til konventionen om beskyttelse af det enkelte menneske i forbindelse med databehandling af personoplysninger, om tilsynsmyndigheder og grænseoverskridende dataudveksling, Strasbourg, den 8. november 2001.

⁽⁴³⁾ Rådets rammeafgørelse 2008/877/RIA af 27. november 2008 om beskyttelse af personoplysninger i forbindelse med politisamarbejde og retligt samarbejde i kriminalsager, EUT L 350 af 30.12.2008, s. 60.

⁽⁴⁴⁾ Se besvarelsene på Europa-Parlamentets høring i forbindelse med indstillingen af Viviane Reding til kommissær, s. 5, http://www.europarl.europa.eu/hearings/static/commissioners/answers/reding_replies_da.pdf

⁽⁴⁵⁾ Resolution vedtaget i Madrid, november 2009.

108. Selv om de internationale standarder endnu ikke har retsvirkning, fungerer de som nyttige retningslinjer, for så vidt angår de databeskyttelsesprincipper, som tredjelandene kan vælge at anvende for at sikre, at deres retsgrundlag er foreneligt med EU's standarder. Den tilsynsførende mener, at de lande, der har underskrevet ACTA, også bør tage højde for de principper, der fastsættes i de internationale standarder, når de behandler personoplysninger fra EU.

V.3. Behovet for at gennemføre tilstrækkelige garantier for at beskytte videregivelse af oplysninger fra EU til tredjelande

Hvilken udformning skal garantierne have for at kunne yde en effektiv beskyttelse af videregivelse af oplysninger til tredjelande?

76. I tilfælde, hvor det kan påvises, at der er behov for at videregive personoplysninger til tredjelande, understreger den tilsynsførende, at EU — udover selve ACTA-aftalen — bør forhandle specifikke instrumenter på plads med modtagerlandene, som indeholder tilstrækkelige databeskyttelsesgarantier til at sikre udvekslingen af personoplysninger.
77. Der bør generelt fastsættes passende databeskyttelsesgarantier i en bindende aftale mellem EU og modtagertredjelandet. Den modtagende part forpligter sig i medfør af denne aftale til at overholde EU's databeskyttelseslovgivning og til at sikre fysiske personer de samme rettigheder og den samme klageadgang, som er hjemlet i EU-lovgivningen. Behovet for en bindende aftale er anført i artikel 26, stk. 2, i direktiv 95/46/EF samt artikel 13, stk. 3, litra b) i rammeafgørelsen og støttes desuden af EU's eksisterende praksis med at indgå specifikke aftaler, der skal gøre det muligt at videregive specifikke oplysninger til tredjelande⁽⁴⁶⁾.
78. Tilsvarende kan modtageren i henhold til de internationale standarder blive pålagt at garantere det beskyttelsesniveau, der er påkrævet for at videregivelsen kan finde sted. Disse garantier kan også tage form af en kontraktmæssig forpligtelse.

Indholdet af de garantier, som ACTA-underskriverne skal gøre rede for i forbindelse med videregivelse af personoplysninger

79. Den tilsynsførende understreger især, at internationale udvekslinger af oplysninger på det strafferetlige område er særligt følsomme, for så vidt angår databeskyttelse, idet det

⁽⁴⁶⁾ F.eks. Europol's og Eurojusts aftaler med USA, PNR-aftalen, Swift-aftalen, samt aftalen mellem Den Europæiske Union og Australien om luftfartsselskabers behandling og overførsel af passagerliste (PNR)-oplysninger med oprindelse i Den Europæiske Union til det australske toldvæsen.

nye instrument kan lovliggøre videregivelse af store mængder oplysninger inden for et område, hvor det har specielt store konsekvenser for enkeltpersoner. Det er derfor ekstra vigtigt med strenge og pålidelige garantier på dette område.

80. Den tilsynsførende anfører, at det kun er muligt at fastsætte specifikke betingelser og garantier på et individuelt grundlag og under hensyntagen til alle aspekter af dataudvekslingerne. Til vejledning fremhæver den tilsynsførende imidlertid nogle af de principper og garantier, som modtageretredjelande skal gøre rede for, før udvekslingerne af data kan finde sted.

— Den juridiske begrundelse for databehandlingsaktiviteterne skal kontrolleres (dvs. om behandlingen finder sted på grundlag af en juridisk forpligtelse eller samtykke fra de registrerede eller en hvilken som helst anden gyldig begrundelse), og det skal kontrolleres, om videregivelsen af oplysninger opfylder det formål, til hvilket de oprindeligt blev indsamlet. Der bør ikke finde videregivelser sted, som ikke hører under det fastsatte formål.

— Det skal tydeligt angives hvor mange og hvilken slags personoplysninger, der skal udveksles, og mængden skal begrænses til det absolut nødvendige for at opfylde formålet med videregivelsen. De personoplysninger, som indsamles og videregives, kan omfatte internetbrugers IP-adresse, dato og klokkeslæt for den mistænkte overtrædelse samt overtrædelsens art. Den tilsynsførende henstiller til, at oplysningerne ikke knyttes til en bestemt person under efterforskningen, og minder om, at en mistænkt kun bør identificeres, hvis det sker i overensstemmelse med lovgivningen og under tilsyn af en dommer. Den tilsynsførende præciserer i den forbindelse, at oplysninger vedrørende krænkelse af de intellektuelle ejendomsrettigheder udgør en særlig kategori af oplysninger, hvis behandling normalt er underlagt begrænsninger fra de retshåndhavende myndigheders side, og som kræver ekstra garantier. De personer, der er bemyndiget til at behandle oplysninger vedrørende krænkelse af de intellektuelle ejendomsrettigheder og mistanker om krænkelse samt betingelserne for behandlingen af disse oplysninger, bør derfor defineres specifikt i overensstemmelse med gældende databeskyttelseslovgivning.

— Det skal tydeligt fastsættes, hvilke personer der kan dele oplysningerne, og videre overførsel til andre modtagere bør principielt forbydes, medmindre overførslerne er nødvendige af hensyn til en specifik efterforskning. Den begrænsning er især vigtig, eftersom de udpegede modtagere ikke unødigt bør dele oplysninger med uautoriserede modtagere.

— Den tilsynsførende antager, at ACTA ikke indeholder bestemmelser om samarbejde mellem offentlige

myndigheder, men at den også vil medføre tildeling af håndhævelsesopgaver til private organisationer (såsom internetudbydere, organisationer med copyrightrettigheder osv.) Det er i sidstnævnte tilfælde vigtigt at foretage en omhyggelig vurdering af, i hvilket omfang og på hvilke betingelser private organisationer er involveret i håndhævelsen af intellektuelle ejendomsrettigheder, idet de foranstaltninger, der fastsættes i ACTA, ikke skal give internetudbydere og organisationer med IP-rettigheder en reel ret til at overvåge brugernes adfærd på nettet. Endvidere bør private organisationers behandling af personoplysninger i forbindelse med retshåndhævelse kun finde sted på et korrekt retsgrundlag. Det er også vigtigt at præcisere, hvorvidt private organisationer vil være forpligtet til at samarbejde med politiet, samt i givet fald omfanget af dette samarbejde. Det bør under alle omstændigheder begrænses til »grov kriminalitet«, som også skal defineres nøjagtigt, idet det ikke er alle overtrædelser af de intellektuelle ejendomsrettigheder, der kan betragtes som grove.

— Den metode, der anvendes til udveksling af personoplysninger, skal tydeligt fastlægges, og det skal især angives, om udvekslingen finder sted via et push-system, hvor f.eks. internetudbydere og organisationer med IP-rettigheder overfører en række oplysninger til tredjeparter i udlandet, såsom politi og retshåndhavende myndigheder, eller et pull-system, hvor f.eks. politi og retshåndhavende myndigheder har direkte adgang til private databaser eller til databaser med centraliserede oplysninger. Som nævnt tidligere i forbindelse med PNR er et push-system den eneste løsning, der er i overensstemmelse med EU's databeskyttelsesprincipper, da det berettiger EU-afsenderen, som typisk vil være den dataansvarlige, til at føre kontrol med videregivelsen af oplysninger ⁽⁴⁷⁾.

— Den periode, som modtagerne må lagre personoplysninger i, skal angives samt formålet med en sådan lagring. Denne lagringsperiode skal stå i et rimeligt forhold til det ønskede formål, hvilket betyder, at oplysningerne skal fjernes eller slettes, når det ikke længere er nødvendigt at opbevare dem for at opnå dette formål.

— De forpligtelser, der påhviler dataansvarlige i tredjelande, skal angives tydeligt. Der skal ydes garanti for, at der findes tilsynsmekanismer og/eller ansvarlighedsmechanismer i forbindelse med håndhævelsen, for at sikre, at der er adgang til effektive klage- og sanktionsforanstaltninger mod dataansvarlige i tilfælde af ukorrekt behandling eller andre relevante hændelser. Der bør

⁽⁴⁷⁾ Se Artikel 29-Gruppens udtalelse nr. 4/2003 om databeskyttelsesniveauet garanteret af USA ved overførsel af passageroplysninger, WP78, 13. juni 2003.

endvidere indføres mekanismer for klageadgang, som giver fysiske personer mulighed for at indgive klage ved en uafhængig databeskyttelsesmyndighed samt have et effektivt retsmiddel ved en uafhængig og upartisk domstol ⁽⁴⁸⁾.

- Det instrument, som parterne indgår, skal indeholde en tydelig angivelse af de registreredes rettigheder i forbindelse med deres personoplysninger, når disse oplysninger behandles af et modtagertredjeland. Det skal sikre, at de registrerede har adgang til effektive midler til at håndhæve deres rettigheder i forbindelse med behandling af deres oplysninger i udlandet.
- Derudover er gennemsigtighed afgørende, og de parter, der har vedtaget et databeskyttelsesinstrument, skal være enige om, hvordan de vil underrette de registrerede om den databehandling, der finder sted, samt om deres rettigheder og muligheden for at udøve disse rettigheder.

VI. KONKLUSIONER

81. Den tilsynsførende opfordrer på det kraftigste Europa-Kommissionen til at etablere en offentlig og gennemsigtig dialog om ACTA, eventuelt via en offentlig høring, som også kan bidrage til at sikre, at de foranstaltninger, der skal vedtages, er i overensstemmelse med kravene i EU's lovgivning om beskyttelse af privatlivets fred og om databeskyttelse.
82. I forbindelse med de igangværende forhandlinger om ACTA opfordrer den tilsynsførende Europa-Kommissionen til at finde den rette balance mellem behovet for at beskytte intellektuelle ejendomsrettigheder og behovet for at beskytte fysiske personers privatliv og sikre databeskyttelse. Den tilsynsførende fremhæver, at det er meget vigtigt, at beskyttelse af privatlivets fred og databeskyttelse inddrages allerede i begyndelsen af forhandlingerne, før der er vedtaget foranstaltninger, således at det undgås, at der senere skal findes alternative løsninger til at beskytte privatlivets fred.
83. De intellektuelle ejendomsrettigheder er vigtige for samfundet og skal beskyttes, men de bør ikke sættes over borgernes grundlæggende ret til privatliv, databeskyttelse og andre rettigheder, som f.eks. uskyldsformodning, effektiv retsbeskyttelse og ytringsfrihed.
84. Eftersom det nuværende udkast til ACTA indebærer eller i det mindste indirekte slår til lyd for »three-strikes«-poli-

tikker, vil ACTA få en meget indskrænkende virkning på EU-borgernes grundlæggende rettigheder og friheder, navnlig for så vidt angår beskyttelse af personoplysninger og privatliv.

85. Den tilsynsførende mener ikke, at »three-strikes«-politikker er nødvendige for at opfylde formålet om at håndhæve intellektuelle ejendomsrettigheder. Den tilsynsførende er overbevist om, at det er muligt at finde alternative, mindre indgribende løsninger, eller at de planlagte politikker kan gennemføres på en mindre indgribende måde eller med et mere begrænset anvendelsesområde, navnlig i form af målrettet ad hoc-overvågning.
86. »Three-strikes«-politikker er også problematiske på et mere detaljeret juridisk plan. Det skyldes ikke mindst, at især private organisationers behandling af juridiske data skal finde sted på et korrekt retsgrundlag. »Three-strikes«-ordninger kan endvidere føre til lagring af logfiler over en længere periode, hvilket vil være i strid med den eksisterende lovgivning.
87. Eftersom ACTA omfatter udveksling af personoplysninger mellem myndigheder og/eller private organisationer i signatarlandene, anmoder den tilsynsførende EU om at indføre tilstrækkelige garantier. Disse garantier skal være gældende for alle dataoverførsler inden for rammerne af ACTA, hvad enten de vedrører det civile, strafferetlige eller digitale område, og bør være i overensstemmelse med de databeskyttelsesprincipper, der fastsættes i konvention nr. 108 og direktiv 95/46/EF. Den tilsynsførende henstiller til, at disse garantier får form af bindende aftaler mellem EU-afsendere og modtagertredjelände.
88. Endelig ønsker den tilsynsførende at blive hørt i forbindelse med de foranstaltninger, der skal gennemføres, og som vedrører de dataoverførsler, der finder sted under ACTA, for at kontrollere, om de er forholdsmæssige og sikrer et tilstrækkeligt beskyttelsesniveau.

Udfærdiget i Bruxelles, den 22. februar 2010

Peter HUSTINX

Den Europæiske Tilsynsførende for
Databeskyttelse

⁽⁴⁸⁾ Se Udtalelse fra Den Europæiske Tilsynsførende for Databeskyttelse om den endelige rapport fra EU-USA-Kontaktgruppen på Højt Plan om Informationsdeling og Beskyttelse af Privatlivets Fred og Personoplysninger, 11.11.2008.