I

(Uznesenia, odporúčania a stanoviská)

STANOVISKÁ

EURÓPSKY DOZORNÝ ÚRADNÍK PRE OCHRANU ÚDAJOV

Stanovisko Európskeho dozorného úradníka pre ochranu údajov k prebiehajúcim rokovaniam Európskej únie týkajúcim sa obchodnej dohody o boji proti falšovaniu (ACTA)

(2010/C 147/01)

EURÓPSKY DOZORNÝ ÚRADNÍK PRE OCHRANU ÚDAJOV,

so zreteľom na Zmluvu o fungovaní Európskej únie, najmä na jej článok 16,

so zreteľom na Chartu základných práv Európskej únie, najmä na jej článok 8,

so zreteľom na smernicu Európskeho parlamentu a Rady 95/46/ES z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov [1],

so zreteľom na smernicu Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002 týkajúcu sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií [2],

so zreteľom na nariadenie Európskeho parlamentu a Rady (ES) č. 45/2001 z 18. decembra 2000 o ochrane jednotlivcov so zreteľom na spracovanie osobných údajov inštitúciami a orgánmi Spoločenstva a o voľnom pohybe takýchto údajov [3], najmä na jeho článok 41,

PRIJAL TOTO STANOVISKO:

I. ÚVOD

1. Európska únia sa zúčastňuje na rokovaniach týkajúcich sa návrhu obchodnej dohody o boji proti falšovaniu (ďalej len „dohoda ACTA“). Tieto rokovania sa začali v roku 2007 v rámci počiatočnej skupiny zainteresovaných strán a potom pokračovali so širšou skupinou účastníkov, k dnešnému dňu k nim patrí Austrália, Európska únia, Japonsko, Kanada, Kórea, Maroko, Mexiko, Nový Zéland, Singapur, Švajčiarsko a USA. Európska komisia získala v roku 2008 od Rady mandát na účasť na týchto rokovaniach.

2. EDPS uznáva, že cezhraničný obchod s falšovaným a pirátskym tovarom vyvoláva stále väčšie obavy často v spojitosti s organizovanými kriminálnymi sieťami, na základe čoho vzniká potreba prijať príslušné mechanizmy spolupráce na medzinárodnej úrovni na boj proti tejto forme trestnej činnosti.

3. EDPS uvádza, že rokovanie Európskej únie o viacstrannej zmluve, ktorej základným predmetom je vymáhanie práv duševného vlastníctva, vyvoláva závažné otázky, pokiaľ ide o vplyv opatrení prijatých na boj proti falšovaniu a pirátstvu na základné práva fyzických osôb a najmä ich právo na ochranu súkromia a údajov.

4. V tejto súvislosti je EDPS obzvlášť ľúto, že s ním Európska komisia nekonzultovala obsah takejto dohody. EDPS preto, konajúc z vlastného podnetu, prijal toto stanovisko založené na článku 41 ods. 2 nariadenia (ES) č. 45/2001 s cieľom poskytnúť Komisii usmernenie k príslušným aspektom ochrany súkromia a údajov, ktoré by sa mali posúdiť pri rokovaniach o dohode ACTA.

II. SÚČASNÝ STAV A PREDPOKLADANÝ OBSAH DOHODY ACTA

5. Siedme kolo rokovaní sa konalo v Mexiku 26. – 29. januára 2010 s cieľom uzavrieť dohodu v priebehu roka 2010. Doteraz však nebol uverejnený žiadny oficiálny návrh dohody.

[1] Ú. v. ES L 281, 23.11.1995, s. 31.
[2] Ú. v. ES L 201, 31.7.2002, s. 37.
[3] Ú. v. ES L 8, 12.1.2001, s. 1.

6. Rokovanie je zamerané na prijatie novej viacstrannej dohody navrhnutej na posilnenie práv duševného vlastníctva (ďalej len „PDV“) a na boj proti falšovaniu a pirátstvu. Prijatím tejto novej dohody by sa zlepšili medzinárodné normy týkajúceho sa toho, ako postupovať proti rozsiahlemu porušovaniu PDV. GR Európskej komisie pre obchod konkrétne uviedlo, že „zameranie je orientované skôr na falšovanie a pirátske aktivity, ktoré výrazne ovplyvňujú obchodné záujmy, než na aktivity obyčajných občanov“ ([4]).

7. Pokiaľ ide o obsah dohody, GR Európskej komisie pre obchod uverejnilo v novembri 2009 Súhrn hlavných prvkov, o ktorých sa rokuje (*Summary of key elements under discussion*), v ktorom sa uvádza, že cieľ dohody ACTA, ktorým je boj proti pirátstvu a falšovaniu, sa zrealizuje prostredníctvom troch primárnych prvkov: i) medzinárodnej spolupráce, ii) postupov vymáhania a iii) vymedzenia právneho rámca pre vymáhanie PDV v niektorých identifikovaných oblastiach a najmä v digitálnom prostredí ([5]). Predpokladané opatrenia sa budú zaoberať najmä právnymi postupmi (ako napr. súdne príkazy, dočasné opatrenia), úlohou a povinnosťami poskytovateľov internetových služieb (PIS) pri odradzovaní od porušovania autorských práv cez internet a opatreniami cezhraničnej spolupráce na zabránenie tomu, aby sa tovar dostal za hranice. Uverejnené informácie však poskytujú len všeobecné línie dohody a nezachádzajú do podrobností žiadnych špecifických a konkrétnych opatrení.

8. EDPS poznamenáva, že aj keď zamýšľaným cieľom dohody ACTA je sledovať len rozsiahle porušenia PDV, nemožno vylúčiť, že by sa aktivity bežných občanov nemohli postihovať podľa dohody ACTA, najmä ak sa opatrenia na vymáhanie uskutočňujú v digitálnom prostredí. EDPS zdôrazňuje, že toto si vyžaduje stanovenie príslušných záruk na ochranu základných práv jednotlivcov. Okrem toho sa právne predpisy na ochranu práv vzťahujú na všetky fyzické osoby vrátane osôb, ktoré sa prípadne podieľajú na aktivitách v oblasti falšovania a pirátstva. Boj proti rozsiahlym porušeniam bude určite zahŕňať aj spracovanie osobných údajov.

9. V tejto súvislosti EDPS dôrazne odporúča Európskej komisii, aby usporiadala verejné a transparentné diskusie o dohode ACTA, pokiaľ možno formou verejných konzultácií, čo by tiež pomohlo zabezpečiť, aby opatrenia, ktoré sa majú prijať, boli v súlade s požiadavkami práva EÚ o ochrane súkromia a údajov.

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

([5]) Pozri uvedenú poznámku pod čiarou č. 2.

III. **ROZSAH PRIPOMIENOK EDPS**

10. EDPS dôrazne vyzýva EÚ a najmä Európsku komisiu, ktorá získala mandát na uzatvorenie dohody, aby nastolili vhodnú rovnováhu medzi požiadavkami ochrany práv duševného vlastníctva a právami jednotlivcov na ochranu súkromia a údajov.

11. EDPS zdôrazňuje, že ochrana súkromia a údajov sú základnými hodnotami Európskej únie uznanými v článku 8 EDĽP a článkoch 7 a 8 Charty základných práv EÚ ([6]), ktoré sa musia dodržiavať vo všetkých politikách a pravidlách prijatých EÚ podľa článku 16 zmluvy o fungovaní Európskej únie (ZFEÚ).

12. Okrem toho EDPS zdôrazňuje, že každá dohoda v súvislosti s dohodou ACTA, ktorú Európska únia dosiahne, musí byť v súlade s právnymi povinnosťami uloženými Európskej únii, pokiaľ ide o právo týkajúce sa ochrany súkromia a údajov, ako je uvedené najmä v smernici 95/46/ES, smernici 2002/58/ES ([7]) a v judikatúre Európskeho súdu pre ľudské práva ([8]) a Súdneho dvora ([9]).

13. Ochrana súkromia a údajov sa musí zohľadňovať hneď od počiatku rokovaní, nie až potom, čo sa vymedzia a dohodnú systémy a postupy, a teda je príliš neskoro na hľadanie alternatívneho riešenia rešpektujúceho súkromie.

14. Vzhľadom na to, že je málo informácií verejne sprístupnených, EDPS konštatuje, že nie je schopný poskytnúť analýzu konkrétnych ustanovení dohody ACTA. EDPS sa teda vo svojom stanovisku zameriava na opísanie potenciálnych hrozieb pre ochranu súkromia a údaje na základe konkrétnych opatrení, ktoré môžu, ako bolo uvedené, z dohody vyplynúť v týchto dvoch oblastiach: vymožiteľnosť práv duševného vlastníctva v digitálnom prostredí (kapitola IV) a medzinárodné mechanizmy spolupráce (kapitola V).

([6]) Charta základných práv Európskej únie, Ú. v. EÚ C 303, 14.12.2007, s. 1.

([7]) Smernica Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002 týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (tzv. „smernica o súkromí a elektronických komunikáciách“) Ú. v. ES L 201, 31.7.2002, s. 37.

([8]) Vysvetlenie hlavných prvkov a podmienok uvedených v článku 8 Európskeho dohovoru o ochrane ľudských práv a základných slobôd (EDĽP) prijatého v Ríme 4. novembra 1950, pretože sa uplatňujú na rôzne oblasti. Pozri hlavne judikatúru uvedenú na iných miestach v tomto stanovisku.

([9]) Pozri najmä: Vec C-275/06, *Productores de Música de España* (Promusicae), Zb. [2008], s. I-271 a vec C-557/07, *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten*, nyr.

IV. VYMOŽITEĽNOSŤ PRÁV DUŠEVNÉHO VLASTNÍCTVA V DIGITÁLNOM PROSTREDÍ

IV.1. Potreba analyzovania vplyvov „politík trikrát a dosť na odpojenie od internetu“ na ochranu súkromia/údajov

15. Podľa Európskej komisie sa dohodou ACTA vytvorí právny rámec na boj proti pirátstvu v digitálnom prostredí. ([10]) Týmto rámcom sa vytvoria podmienky, na základe ktorých sa PIS a iní online sprostredkovatelia ([11]) môžu považovať za zodpovedných na základe toho, že cez ich zariadenia prechádza materiál porušujúci autorské práva. Rámec môže poskytovať aj opatrenia a opravné prostriedky, ktoré sa uložia užívateľom internetu na základe vkladania alebo preberania materiálu porušujúceho autorské práva. Aj keď podrobnosti takéhoto rámca neboli oficiálne uverejnené, vzhľadom na informácie dostupné z iných zdrojov, sa dá predpokladať, že by mohol zahŕňať uloženie povinností prevádzkovateľom internetových služieb, aby prijali „politiky trikrát a dosť na odpojenie od internetu“, ktoré sa označujú aj ako systémy „postupnej reakcie“. Takéto systémy umožnia nositeľom autorských práv monitorovať užívateľov internetu a identifikovať údajných porušovateľov autorských práv. PIS by mal po kontaktovaní údajného porušovateľa upozorniť užívateľa identifikovaného ako porušovateľa a po prvých troch upozorneniach by mal byť odpojený od internetu.

16. V rovnakom čase ako rokovania o dohode ACTA sa v niektorých členských štátoch, napr. vo Francúzsku, zavádzajú politiky trikrát a dosť na odpojenie od internetu. Diskutuje sa o nich na rôznych fórach EÚ, ako napr. Dialóg zainteresovaných strán o nezákonnom vkladaní a preberaní (Stakeholders' Dialogue on illegal up – and downloading), ktoré v súčasnosti prebiehajú s podporou GR MARKT v súvislosti s prijatím oznámenia Komisie o zvyšovaní účinnosti vymáhania práv duševného vlastníctva na vnútornom trhu ([12]). Diskusie o tejto téme sa uskutočňujú aj v Európskom parlamente v súvislosti s neukončenou debatou o návrhu uznesenia Európskeho parlamentu o zvyšovaní účinnosti vymáhania práv duševného vlastníctva na vnútornom trhu (nazvané aj ako „Gallovej správa“).

17. Takéto postupy výrazne zasahujú do súkromnej sféry jednotlivcov. Znamenajú všeobecné monitorovanie aktivít užívateľov internetu vrátane takých, ktoré sú ukážkovo zákonné. Ovplyvňujú milióny užívateľov internetu dodržiavajúcich právne predpisy vrátane mnohých detí a dospievajúcich. Nevykonávajú ich orgány činné v trestnom konaní, ale súkromné strany. Okrem toho internet v súčasnosti zohráva ústrednú úlohu takmer vo všetkých aspektoch moderného života, a preto účinky odpojenia od internetu môžu byť nesmierne – odrezanie jednotlivcov od práce, kultúry, aplikácií eGovermentu a pod.

18. Na základe tohto je dôležité posúdiť, do akej miery sú tieto politiky v súlade s právnymi predpismi EÚ o ochrane súkromia a údajov a konkrétnejšie, či politiky trikrát a dosť na odpojenie od internetu predstavujú nevyhnutné opatrenie na vymáhanie práv duševného vlastníctva. V tejto súvislosti by sa malo ďalej analyzovať, či neexistujú iné, menej rušivé metódy.

19. Ešte stále nie je jasné, či sa politiky trikrát a dosť na odpojenie od internetu zahrnú do dohody ACTA. Tieto politiky sa však posudzujú aj v iných oblastiach a majú – potenciálne – nesmierny vplyv na ochranu osobných údajov a súkromia. Z týchto dôvodov EDPS považuje za potrebné venovať sa im v tomto stanovisku. Pred uskutočnením uvedenej analýzy EDPS v krátkosti vysvetlí platný právny rámec na ochranu súkromia a údajov.

20. Je potrebné pripomenúť, že okrem ochrany údajov a súkromia politiky trikrát a dosť na odpojenie od internetu vzbudzujú obavy, pokiaľ ide o iné hodnoty, ako napr. riadny proces a sloboda prejavu. Toto stanovisko je však zamerané len na tie ostatné aspekty, ktoré sa týkajú ochrany osobných údajov a súkromia fyzických osôb.

IV.2. Politiky trikrát a dosť na odpojenie od internetu a uplatňovanie právneho rámca EÚ na ochranu súkromia a údajov

Ako môžu byť nastavené politiky trikrát a dosť na odpojenie od internetu

21. V krátkosti, v rámci politík trikrát a dosť na odpojenie od internetu by nositelia autorských práv používajúci automatické technické prostriedky poskytované prípadne tretími stranami identifikovali údajné porušenie autorského práva tým, že sa zapoja do monitorovania aktivít užívateľov

([10]) Pozri uvedenú poznámku pod čiarou č. 2.

([11]) Jednotlivých online sprostredkovateľov možno definovať podľa ich funkčných úloh. V reálnom svete však sprostredkovatelia obvykle preberajú viaceré z týchto funkcií. K online sprostredkovateľom patria: a) *poskytovatelia prístupu:* užívatelia pripojení k sieti pripojením sa k serveru poskytovateľa prístupu; b) *poskytovatelia sietí:* poskytujú routre, *t. j.* technické zariadenia potrebné na prenos údajov; c) *poskytovateľ webhostingu*: prenajímajú priestor na svojom serveri, na základe čoho užívatelia alebo poskytovatelia obsahu môžu vložiť obsah. Užívatelia môžu vložiť a prevziať materiál na online službu, ako napríklad buletin alebo siete P2P.

([12]) Oznámenie Komisie Rade, Európskemu parlamentu, Európskemu hospodárskemu a sociálnemu výboru – Zvyšovanie účinnosti presadzovania práv duševného vlastníctva na vnútornom trhu, v Bruseli 11. septembra 2009, KOM(2009) 467 v konečnom znení.

internetu, napríklad prostredníctvom dohľadu nad fórami, blogmi, alebo budú pôsobiť ako osoby vymieňajúce si súbory v sieťach peer-to-peer na identifikovanie jednotlivcov, ktorí si vymieňajú súbory a ktorí si údajne vymieňajú materiál chránený autorským právom ([13]).

22. Po identifikovaní užívateľov internetu, ktorí sa údajne podieľajú na porušovaní autorských práv, získavaním adries ich internetových protokolov (IP adries), by nositelia autorských práv posielali IP adresy týchto užívateľov príslušnému poskytovateľovi internetových služieb alebo príslušným poskytovateľom internetových služieb, ktorí by upozornili predplatiteľa, ktorému IP adresa patrí, o jeho možnej účasti na porušovaní autorských práv. Určitý počet upozornení zo strany PIS by automaticky znamenal, že PIS automaticky ukončí alebo pozastaví internetové pripojenie predplatiteľa ([14]).

Platný právny rámec EÚ na ochranu údajov/súkromia

23. Politiky trikrát a dosť na odpojenie od internetu musia byť v súlade s požiadavkami vyplývajúcimi z práva na súkromie, ako je ustanovené v článku 8 EDĽP a článku 7 Charty základných práv, ako to vyplýva z práva na ochranu údajov, ako je ustanovené v článku 8 Charty základných práv a článku 16 ZFEÚ a v smernici 95/46/ES a smernici 2002/58/ES.

24. Podľa stanoviska EDPS monitorovanie správania užívateľa internetu a ďalšie získavanie ich IP adries znamená zasahovanie do práv užívateľov na rešpektovanie ich súkromného života a ich korešpondencie, inými slovami dochádza k zasahovaniu do ich práva na súkromný život. Toto stanovisko je v súlade s judikatúrou Európskeho súdu pre ľudské práva ([15]).

25. Uplatňuje sa smernica 95/46/ES ([16]), pretože politiky trikrát a dosť na odpojenie od internetu zahŕňajú spracovanie IP adries, ktoré by sa v každom prípade podľa príslušných okolností mohli považovať za osobné údaje. IP adresy sú identifikátormi, ktoré majú podobu sledu čísiel oddelených bodkami, napr. 122.41.123.45. Predplatením u poskytovateľa prístupu na internet sa účastníkovi umožní prístup na internet. Vždy, keď si účastník želá prístup na internet, pridelí sa mu IP adresa prostredníctvom zariadenia, ktoré používa na prístup k internetu (napríklad počítač) ([17]).

26. Ak sa užívateľ podieľa na danej činnosti, napríklad vkladá materiál na internet, tretie strany ho môžu identifikovať na základe IP adresy, ktorú používa. Napríklad užívateľ, ktorého IP adresa je 122.41.123.45, údajne vložil materiál porušujúci autorské práva na službu P2P 1. januára 2010 o 15.00 h. ISP si potom bude vedieť dať do súvisu takúto IP adresu s menom predplatiteľa, ktorému je priradená táto adresa, a tak zistiť jeho totožnosť.

27. Vzhľadom na vymedzenie osobných údajov v článku 2 smernice 95/46/ES, ktoré „znamenajú akúkoľvek informáciu, ktorá sa týka identifikovanej alebo identifikovateľnej fyzickej osoby (‚údajového subjektu'); identifikovateľná osoba je osoba, ktorú možno identifikovať, priamo alebo nepriamo, najmä pomocou overenia identifikačného čísla" ([18]), možno usúdiť, že IP adresy a informácie týkajúce sa aktivít súvisiacich s takýmito adresami predstavujú osobné údaje vo všetkých prípadoch, o ktoré tu ide. IP adresy skutočne slúžia ako identifikačné číslo, ktoré umožňuje zistiť meno účastníka, ktorému bola priradená IP adresa. Okrem toho získané informácie o účastníkovi, ktorý je držiteľom takejto IP adresy („ktorý vložil 1. januára 2010 určitý materiál na webovú stránku ZS o 15.00 h"), *sa týkajú*, t. j. jasne sa vzťahujú na aktivity identifikovateľnej fyzickej osoby (držiteľa IP adresy) a musia sa teda považovať za osobné údaje.

([13]) Technológia P2P je počítačová softvérová architektúra, ktorá umožňuje, aby sa jednotlivé počítače spájali a komunikovali priamo s inými počítačmi.

([14]) K alternatívnym sankciám by patrilo obmedzenie funkčnosti internetu, napríklad rýchlosť pripojenia, objem a pod.

([15]) Pozri najmä EDĽP 26. júna 2006, *Weber a Saravia proti Nemecku* (dec.), č. 54934/00, ods. 77 a EDĽP 1. júla 2008, *Liberty a iní proti UK*, č. 58243/00.

([16]) Súdny dvor pristupuje zoširoka k uplatňovaniu smernice 95/46/ES, ustanovenia ktorej sa musia vykladať z hľadiska článku 8 EDĽP. Súdny dvor uviedol vo svojom rozsudku z 20. mája 2003, *Rundfunk*, spojené veci C-465/00, C-138/01 a C-139/01, Zb. [2003], s. I-4989, ods. 68, že „ustanovenia smernice 95/46/ES, pokiaľ ide o úpravu spracúvania osobných údajov, ktoré môžu spôsobiť ujmu na základných slobodách, najmä na práve na súkromný život, sa musia vykladať v súlade so základnými právami, ktoré v zmysle ustálenej judikatúry tvoria neoddeliteľnú súčasť všeobecných právnych zásad, ktorých dodržiavanie Súdny dvor zaručuje".

([17]) IP adresa, ktorú PIS priradí fyzickej osobe, môže byť vždy rovnaká pri surfovaní po internete (označujú sa ako statické IP adresy). Iné IP adresy sú dynamické, čo znamená, že poskytovateľ prístupu na internet priradí rôzne IP adresy svojim klientom vždy, keď sa pripoja na internet. Je zrejmé, že PIS môže dať do súvisu IP adresu s účtom účastníka, ktorému priradil (dynamickú alebo statickú) IP adresu.

([18]) V odôvodnení 26 je toto vymedzenie doplnené: „keďže zásady ochrany sa musia vzťahovať na všetky informácie týkajúce sa identifikovanej alebo identifikovateľnej osoby; keďže k určeniu, či je osoba identifikovateľná, by sa mali vziať do úvahy všetky prostriedky, u ktorých je primeraná pravdepodobnosť, že ich využije kontrolór, alebo ľubovoľná iná osoba na identifikáciu príslušnej osoby; keďže zásady ochrany sa nebudú vzťahovať na údaje poskytnuté anonymne, a to tak, že predmet údajov sa už nebude dať identifikovať; …".

28. S týmto stanoviskami sa plne stotožňuje pracovná skupina zriadená podľa článku 29, ktorá v dokumente o otázkach ochrany údajov v súvislosti s právami duševného vlastníctva uviedla, že IP adresy získané na účely vymáhania práv duševného vlastníctva, t. j. na identifikáciu internetových užívateľov, ktorí údajne porušili práva duševného vlastníctva, sú osobnými údajmi, pretože sa používajú proti danej fyzickej osobe na účely vymáhania takýchto práv ([19]).

29. Uplatňuje sa aj smernica 2002/58/ES, keďže politiky trikrát a dosť na odpojenie od internetu znamenajú získavanie prevádzkových a komunikačných údajov. V smernici 2002/58/ES sa upravuje využívanie takýchto údajov a ustanovuje zásada dôvernosti komunikácií prenášaných pomocou verejných komunikačných sietí a údajov obsiahnutých v týchto komunikáciách.

IV.3. **Či politiky trikrát a dosť na odpojenie od internetu predstavujú nevyhnutné opatrenie**

30. V článku 8 EDĽP je stanovená zásada nevyhnutnosti, podľa ktorej každé opatrenie, ktoré porušuje právo na súkromie fyzických osôb, je povolené iba vtedy, ak predstavuje nevyhnutné opatrenie v rámci demokratickej spoločnosti na legitímny cieľ, ktorý sleduje ([20]). Zásadu nevyhnutnosti možno nájsť v článkoch 7 a 13 smernice 95/46/ES a článku 15 smernice 2002/58/ES ([21]). Podľa tejto zásady sa vyžaduje analýza primeranosti opatrenia, ktorá sa musí posudzovať na základe rovnováhy príslušných záujmov, ktorá sa nastoľuje v súvislosti s demokratickou spoločnosťou ako celku. ([22]) Okrem toho znamená posúdenie, či neexistujú alternatívne opatrenia, ktoré sú menej rušivé.

31. Aj keď EDPS uznáva dôležitosť vymáhania práv duševného vlastníctva, je názoru, že politiky trikrát a dosť na odpojenie od internetu, ako sú teraz známe – zahŕňajúce určité prvky všeobecného uplatňovania – predstavujú neprimerané opatrenie, a preto sa nemôžu považovať za nevyhnutné opatrenie. EDPS je ďalej presvedčený, že existujú alternatívne menej rušivé riešenia alebo že možno vykonávať predpokladané politiky menej rušivým spôsobom alebo v menšom rozsahu. Prístup trikrát a dosť predstavuje problémy aj na detailnejšej právnej úrovni. Tieto závery budú vysvetlené ďalej v texte.

Politiky prístupu trikrát a dosť sú neprimerané

32. EDPS chce zdôrazniť, že uložené opatrenia majú ďalekosiahly charakter. V tejto súvislosti je potrebné uviesť tieto prvky:

i) skutočnosť, že (neoznámené) monitorovanie by ovplyvnilo milióny jednotlivcov a *všetkých* užívateľov bez ohľadu na to, či sú podozriví.

ii) monitorovanie by znamenalo systematické zaznamenávanie údajov, z ktorých niektoré môžu spôsobiť, že ľudia budú postavení pred občianske alebo dokonca trestné súdy, okrem toho niektoré získané informácie by sa tak podľa článku 8 smernice 95/46/ES kvalifikovali ako citlivé údaje, ktoré si vyžadujú prísnejšie záruky.

iii) monitorovanie by mohlo spustiť mnohé prípady mylných zistení. Porušovanie autorských práv nie je otázkou priamočiareho „áno“ alebo „nie“. Súdy musia často preskúmať značné množstvo technických a právnych informácií na niekoľkých desiatkach strán, aby dokázali určiť, či došlo k porušeniu ([23]).

([19]) Pracovný dokument pracovnej skupiny zriadenej podľa článku 29 o otázkach ochrany údajov v súvislosti s právami duševného vlastníctva (WP 104) bol prijatý 18. januára 2005. Táto pracovná skupina bola zriadená podľa článku 29 smernice 95/46/ES. Je nezávislým európskym poradným orgánom na ochranu údajov a súkromia. Jej úlohy sú uvedené v článku 30 smernice 95/46/ES a článku 15 smernice 2002/58/ES. Pozri aj stanovisko pracovnej skupiny 4/2007 o pojme osobné údaje (WP 136), ktoré bolo prijaté 20. júna 2007, a to na s. 16.

([20]) V článku 8 EDĽP sa výslovne uvádza požiadavka, že každý zásah alebo obmedzenie musia byť „nevyhnutné v demokratickej spoločnosti“.

([21]) V článku 13 smernice 95/46/ES sa obmedzenie povoľuje len, keď predstavuje „nevyhnutné opatrenia na zabezpečenie údajov o: a) štátnej bezpečnosti; b) obrane; c) verejnej bezpečnosti; d) prevencii, vyšetrovaní, pátraní a trestnom konaní alebo porušení etiky pre predpísané profesie; e) dôležitom hospodárskom alebo finančnom záujme členského štátu alebo Európskej únie vrátane peňažných, rozpočtových a daňových záležitostí; monitorovaní, inšpekcii alebo regulačnej funkcii spojenej aj s výkonom oficiálneho orgánu v prípadoch uvedených v písmenách c), d) a e); g) ochrane osoby pracujúcej s údajmi alebo práv a slobôd ostatných.“ V článku 15 smernice 2002/58/ES sa požaduje, že „ak také obmedzenie predstavuje nevyhnutné, vhodné a primerané opatrenie v demokratickej spoločnosti na zabezpečenie národnej bezpečnosti (t. j. bezpečnosti štátu), obrany, verejnej bezpečnosti a na zabránenie, vyšetrovanie, odhaľovanie a stíhanie trestných činov alebo neoprávnené používanie elektronického komunikačného systému podľa článku 13 ods. 1 smernice 95/46/ES“.

([22]) Pozri aj EDĽP z 2. augusta 1984, *Malone proti Spojenému kráľovstvu*, Séria A č. 82, s. 32, ods. 81 a ďalšie. a EDĽP zo 4. decembra 2008, *Marper proti Spojenému kráľovstvu* [GC], č. 30562/04 a 30566/04, ods. 101 a ďalšie.

([23]) Súdy môžu posúdiť, či je materiál skutočne chránený autorským právom, ktoré bolo porušené, ak sa použitie môže posudzovať ako prípad týkajúci sa správneho používania (fair use), platného práva, škôd a pod.

iv) potenciálne *účinky* monitorovania, ktoré by mohli spôsobiť odpojenie od prístupu k internetu. Toto by mohlo zasahovať do práv fyzických osôb na slobodu vyjadrenia, slobodu informácií a prístup ku kultúre, aplikáciám e-Governmentu, trhom, e-mailu a v niektorých prípadoch k aktivitám súvisiacim s prácou. V tejto súvislosti je obzvlášť dôležité uvedomiť si, že účinky pocíti nielen údajný porušovateľ, ale aj rodinní príslušníci, ktorí používajú rovnaké internetové spojenie vrátane školákov, ktorí používajú internet na aktivity súvisiace so školou.

v) skutočnosť, že subjekt, ktorý posudzuje a prijíma rozhodnutia, bude spravidla súkromným subjektom (t. j. nositeľ autorských práv alebo PIS). EDPS už uviedol v predchádzajúcom stanovisku svoje obavy týkajúce sa monitorovania fyzických osôb súkromným sektorom (napr. PIS alebo nositelia autorských práv), v oblastiach, ktoré sú zásadne v kompetencii orgánov činných v trestnom konaní ([24]).

33. EDPS nie je presvedčený, že výhody opatrení prevážia vplyv na základné práva fyzických osôb. Ochrana autorského práva je záujmom nositeľov práv a spoločnosti. Obmedzenia základných práv sa však nezdajú opodstatnené pri porovnaní závažnosti zásahu, t. j. rozsah narušenia súkromia, na čo poukazujú vyššie uvedené prvky, s očakávanými výhodami, odradenie od porušovania práv duševného vlastníctva zahŕňajúce – zväčša – porušovanie práv duševného vlastníctva malého rozsahu. Ako uviedla vo svojom stanovisku generálna advokátka Kokott vo veci *Promusicae*: „Nie je … isté, či tzv. filesharing medzi súkromnými osobami, zvlášť, ak tieto osoby konajú bez dosahovania zisku, ohrozuje ochranu autorských práv dostatočne závažným spôsobom, aby sa mohlo odôvodniť uplatnenie tejto výnimky. Rozsah, v akom zdieľanie súborov medzi súkromnými osobami spôsobuje skutočnú ujmu totiž zostáva kontroverznou otázkou“ ([25]).

34. V tejto súvislosti je potrebné pripomenúť reakciu Európskeho parlamentu k systému „trikrát a dosť“ v súvislosti s revíziou telekomunikačného balíka, najmä pozmeňujúceho a doplňujúceho návrhu 138 k rámcovej smernici ([26]). V tomto pozmeňujúcom a doplňujúcom návrhu bolo uvedené, že každé obmedzenie základných práv alebo slobôd sa môže uložiť len, ak je vhodné, primerané a nevyhnutné v rámci demokratickej spoločnosti a ich vykonávanie podlieha primeraným procesným zárukám v súlade s EDĽP a všeobecnými zásadami práva Spoločenstva vrátane platnej právnej ochrany a riadneho procesu ([27]).

35. Z tohto hľadiska EDPS ďalej zdôrazňuje, že každé obmedzenie základných práv bude podliehať dôkladnej kontrole na úrovni EÚ i na vnútroštátnej úrovni. V tejto súvislosti možno vidieť paralelu so smernicou o uchovávaní údajov 2006/24/ES ([28]), ktorá sa odchyľuje od zásady všeobecnej ochrany údajov v súvislosti s vymazaním údajov, keď nie sú viac potrebné na účely, na ktoré boli získané. V tejto smernici sa vyžaduje, aby sa prevádzkové údaje uchovávali na účely boja proti závažnej trestnej činnosti. Je potrebné uviesť, že uchovávanie sa povoľuje len v prípade „závažnej trestnej činnosti“, že sa obmedzuje na „prevádzkové údaje“, ktoré v zásade vylučujú informácie o obsahu komunikácií, a že sa uvádzajú prísne záruky. Napriek tomu vznikajú pochybnosti o jej zlučiteľnosti so základnými normami základných práv. Rumunský ústavný súd rozhodol, že všeobecné zachovávanie nie je zlučiteľné so základnými právami ([29]) a prípad sa v súčasnosti rieši na nemeckom ústavnom súde ([30]).

Existencia iných menej rušivých opatrení

36. Uvedené zistenie podporuje skutočnosť, že existujú menej rušivé prostriedky na dosiahnutie rovnakého cieľa. EDPS trvá na tom, že by sa mali preskúmať a odskúšať menej rušivé modely.

([24]) Stanovisko EDPS z 23. júna 2008 o návrhu rozhodnutia Európskeho parlamentu a Rady, ktorým sa ustanovuje viacročný program Spoločenstva na ochranu detí, ktoré používajú internet a iné komunikačné technológie, Ú. v. EÚ C 2, 7.1.2009, s. 2.

([25]) Pozri vec uvedenú v poznámke pod čiarou 8, bod 106.

([26]) Pozri smernicu 2009/140/ES Európskeho parlamentu a Rady z 25. novembra 2009, Ú. v. EÚ L 337, 18.12.2009, s. 37.

([27]) Konečné znenie tzv. pozmeňujúceho a doplňujúceho návrhu 138 znie takto: „Článok 1.3a Opatrenia prijaté členskými štátmi, ktoré sa týkajú prístupu koncových užívateľov k službám a aplikáciám prostredníctvom elektronických komunikačných sietí alebo ich využívania, dodržiavajú základné práva a slobody fyzických osôb, tak ako sa zaručujú v Európskom dohovore o ochrane ľudských práv a základných slobôd a vo všeobecných zásadách práva Spoločenstva. Akékoľvek takéto opatrenia týkajúce sa prístupu alebo použitia služieb a aplikácií koncovými používateľmi prostredníctvom elektronických komunikačných sietí, ktoré môžu spôsobiť obmedzenie týchto základných práv a slobôd, sa môžu zaviesť len v tom prípade, ak sú vhodné, primerané a nevyhnutné v demokratickej spoločnosti, a ich uplatňovanie podlieha primeraným procesným zárukám v súlade s Európskym dohovorom o ochrane ľudských práv a základných slobôd a so všeobecnými zásadami práva Spoločenstva vrátane účinnej súdnej ochrany a riadneho procesu. Rovnako tieto opatrenia možno prijať len s náležitým zohľadnením zásady prezumpcie neviny a práva na súkromie. Predchádzajúce spravodlivé a nestranné konanie sa zaručuje vrátane práva dotknutej osoby alebo dotknutých osôb na vypočutie, s výhradou potreby vhodných podmienok a vhodných procedurálnych opatrení v náležite odôvodnených naliehavých prípadoch v súlade s Európskym dohovorom o ochrane ľudských práv a základných slobôd. Právo na účinné a včasné súdne preskúmanie sa zaručuje.“

([28]) Pozri smernicu 2006/24/ES Európskeho parlamentu a Rady z 15. marca 2006, Ú. v. EÚ 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. V tejto súvislosti EDPS pripomína, že zmenená a doplnená smernica 2002/22/ES o univerzálnej službe a právach užívateľov týkajúcich sa elektronických komunikačných sietí a služieb (označovaná ako „smernica o právach občanov"), ktorá je súčasťou nedávno prepracovaného telekomunikačného balíka, obsahuje určité pravidlá a postupy na obmedzenie porušovania autorských práv v malom rozsahu spotrebiteľmi ([31]). Medzi tieto postupy patrí povinnosť členských štátov pripraviť štandardizované informácie verejného záujmu o rôznych témach, v ktorých sa budú osobitne uvádzať porušenia autorských a práv a s nimi súvisiacich práv a ich právnych dôsledkov ([32]). Členské štáty môžu potom požiadať PIS, aby ich distribuoval svojim klientom a zahrnul do ich zmlúv.

38. Systém slúži na informovanie a odradenie jednotlivcov od šírenia informácií chránených autorským právom a podieľania sa na aktivitách porušujúcich toto právo, pričom súčasne zabraňuje monitorovaniu užívania internetu a súvisiacim aspektom v oblasti ochrany súkromia a údajov. Smernica o právach občanov sa musí implementovať v máji 2011, teda tieto postupy zatiaľ nie sú zavedené. Z tohto dôvodu ešte nebolo možné otestovať ich výhody. Preto sa zdá, že je predčasné prehliadnuť prípadný užitočný výsledok týchto nových postupov a zahrnúť ich namiesto „politík trikrát a dosť na odpojenie od internetu", ktoré oveľa viac obmedzujú základné práva.

39. Okrem uvedeného by sa malo pripomenúť, že smernica 2004/48/ES z 28. apríla 2004 o vymožiteľnosti práv duševného vlastníctva poskytuje rôzne nástroje na vymáhanie práv duševného vlastníctva na súdoch (analyzované ďalej v texte v odseku 43 a ďalších odsekoch) ([33]).

40. Smernica IPRE bola len pred nedávnom transponovaná do právnych predpisov členských štátov. Doposiaľ nebol dostatok času na vyhodnotenie, či sú jej ustanovenia primerané na účely vymáhania práv duševného vlastníctva. Z tohto dôvodu každá potreba nahradiť súčasný systém založený na súdnych konaniach, ktorá zatiaľ nebol otestovaná, je prinajmenšom pochybná. Z uvedeného vyplýva nevyhnutná otázka, prečo nemožno existujúce porušenia primerane riešiť na základe existujúcich sankcií občianskeho a trestného práva za porušovanie autorského práva. Z tohto dôvodu by Komisia mala pred navrhnutím takýchto opatrení politiky vydať spoľahlivé informácie, z ktorých bude vyplývať, že súčasný právny rámec neprináša plánované účinky.

41. Okrem toho nie je jasné, či sa seriózne zvážili alternatívne modely ekonomickej činnosti, ktoré by nezahŕňali systematické monitorovanie fyzických osôb. Napríklad, ak nositelia autorských práv preukážu svoje straty v dôsledku využívania P2P, nositelia práv a PIS by mohli, napríklad vyskúšať diferencované predplatenie prístupu k internetu, keď sa časť ceny za predplatenie s neobmedzeným prístupom rozdelí majiteľom autorských práv.

Možnosť vykonávať cielené monitorovanie menej rušivým spôsobom

42. Okrem používania úplne odlišných modelov, ktoré by sa mali, ako už bolo uvedené, preskúmať a otestovať, cielené monitorovanie by sa malo v každom prípade uskutočňovať menej rušivým spôsobom.

43. Cieľ, ktorým je vymáhanie práv duševného vlastníctva, je možné dosiahnuť aj monitorovaním len obmedzeného počtu jednotlivcov podozrivých z podieľania sa na netriviálnom porušovaní autorských práv. Smernica IPRE poskytuje v tomto ohľade určité usmernenie. Sú v nej ustanovené podmienky, podľa ktorých orgány môžu nariadiť poskytnutie osobných údajov, ktoré uchovávajú poskytovatelia prístupu na internet, na účely vymáhania práv duševného vlastníctva. V článku 8 je ustanovené, že príslušné súdne orgány môžu nariadiť, aby PIS poskytli osobné informácie, ktoré uchovávajú o údajných porušovateľoch (napr. informácie o pôvode a distribučných sieťach tovarov alebo služieb, ktoré porušujú právo duševného vlastníctva) ako reakciu na odôvodnenú a primeranú požiadavku v prípadoch porušovania *na obchodnej úrovni* ([34]).

44. Na základe toho je kritérium „obchodnej úrovne" rozhodujúce. Podľa tohto kritéria monitorovanie môže byť primerané v kontexte obmedzených, špecifických *ad hoc* situácií,

([31]) Pozri smernicu 2009/136/ES Európskeho parlamentu a Rady z 25. novembra 2009, Ú. v. EÚ L 337, 18.12.2009, s. 11.

([32]) Konkrétne v článku 21 ods. 4 smernice 2009/136/ES je ustanovené, že „Členské štáty môžu vyžadovať, aby podniky uvedené v odseku 3 podľa potreby bezplatne poskytovali informácie vo verejnom záujme existujúcim a novým účastníkom, a to rovnakými prostriedkami, ktoré tieto podniky bežne používajú pri svojej komunikácii s účastníkmi. V takom prípade takéto informácie poskytujú príslušné orgány verejnej moci v štandardizovanom formáte, pričom sa okrem iného týkajú: a) najčastejšieho využitia elektronických komunikačných služieb na nezákonnú činnosť alebo na šírenie škodlivého obsahu, a to najmä ak sa môže dotýkať dodržiavania práv a slobôd iných osôb vrátane porušovania autorských a súvisiacich práv, a právnych následkov (...)." Okrem toho podľa článku 20 ods. 1, „Členské štáty môžu vyžadovať aj to, aby sa v zmluve uviedli všetky informácie, ktoré by mohli na tento účel poskytnúť príslušné orgány verejnej moci o používaní elektronických komunikačných sietí a služieb s cieľom zapojiť sa do nezákonnej činnosti alebo šíriť škodlivý obsah, ako aj o prostriedkoch ochrany proti rizikám z hľadiska osobnej bezpečnosti, súkromia a osobných údajov, ktoré sa uvádzajú v článku 21 ods. 4 a týkajú sa poskytovanej služby."

([33]) Ú. v. EÚ L 157, 30.4.2004, s. 45. (ďalej len „smernica IPRE").

([34]) Ďalej je to potvrdené v odôvodnení 14 smernice IPRE.

keď existujú podložené podozrenia o zneužívaní autorského práva na obchodnej úrovni. Toto kritérium by mohlo zahŕňať situácie jasného zneužívania autorského práva súkromnými osobami s cieľom získať priame alebo nepriame obchodné výhody.

45. Na uplatnenie uvedeného by sa nositelia autorských práv mohli v praxi podieľať na cielenom monitorovaní určitých IP adries s cieľom overiť rozsah porušenia autorského práva. Znamenalo by to, že nositeľom autorských práv by sa malo tiež povoliť, aby z rovnakých dôvodov sledovali správy o údajom porušovaní. Takéto informácie by sa mali používať len po overení významnosti porušenia. Jasnými prípadmi sú napríklad závažné porušenia, ako aj nevýznamné neustále pokračujúce porušovania počas určitej doby na účely obchodnej výhody alebo finančného zisku. Dôraz sa kladie na potrebu kontinuity počas určitého časového úseku a vysvetľuje sa ďalej v texte v diskusii týkajúcej sa zásady zachovania.

46. Znamenalo by to, že v takýchto prípadoch získavanie informácií na účely preukázania údajného zneužívania internetu možno považovať za primerané a nevyhnutné na účely prípravy právneho konania vrátane súdneho sporu.

47. EDPS zvažuje ako ďalšiu záruku, aby vnútroštátne orgány na ochranu údajov vopred skontrolovali a povolili operácie na spracovanie údajov zamerané na získavanie dôkazov takéhoto typu. Tieto stanoviská sa zakladajú na skutočnosti, že operácie na spracovanie údajov by predstavovali osobitné riziká pre práva a slobody jednotlivcov z hľadiska ich cieľov, t. j. vykonávania krokov na vymáhanie, ktoré by prípadne mohli byť trestné, a z hľadiska citlivosti získaných údajov. Skutočnosť, že spracovanie zahŕňa monitorovanie elektronických komunikácií je ďalším faktorom, ktorý vyzýva k zvýšeniu dohľadu.

48. EDPS sa domnieva, že „obchodná úroveň" zahrnutá v smernici IPRE je veľmi vhodným prvkom, ktorý stanovuje limity pre monitorovanie s cieľom dodržiavať zásadu primeranosti. Okrem toho, zatiaľ sa nezdá, že existujú spoľahlivé dôkazy, z ktorých vyplýva na základe kritérií stanovených v smernici IPRE, že sa účinné právne kroky proti porušovaniu autorských práv ukazujú ako nemožné alebo neefektívne. Opačný prípad napríklad vyplýva zo správ, napr. z Nemecka, kde sa od roku 2008 po transpozícii smernice IPRE vydalo okolo 3 000 súdnych príkazov, podľa ktorých PIS poskytli súdu informácie o 300 000 účastníkoch.

49. Skrátka, keďže smernica IPRE je účinná iba dva roky, je ťažké pochopiť, prečo by sa zákonodarcovia mali presunúť z kritérií zahrnutých v tejto smernici k viac rušivým postupom, keď EÚ práve začína testovať tieto, ktoré sa prijali nedávno. Z rovnakého dôvodu je tiež ťažké pochopiť, prečo je potrebné nahradiť existujúci systém založený na súdoch iným typom opatrení (okrem otázok týkajúcich sa riadneho procesu, ktoré sa tu neriešia).

IV.4. **Súlad politík trikrát a dosť na odpojenie od internetu s podrobnejšími ustanoveniami na ochranu údajov**

50. Existujú iné špecifickejšie právne dôvody, prečo je tento prístup trikrát a dosť problematický z hľadiska ochrany údajov. EDPS by chcel upozorniť na pochybný právny dôvod pre spracovanie, ktoré sa požaduje podľa smernice 95/46/ES, a na povinnosť vymazať zaznamenané súbory, ktorá sa uvádza v smernici 2002/58/ES.

Právny dôvod na spracovanie

51. Systémy trikrát a dosť znamenajú spracovanie osobných údajov, z ktorých niektoré sa použijú na právne alebo správne konanie s cieľom odpojiť od internetu jednotlivcov, ktorí opakovane porušujú práva. Z tohto pohľadu sa takéto údaje považujú za citlivé údaje podľa článku 8 smernice 95/46/ES. V článku 8 ods. 5 sa stanovuje, že „Spracovanie údajov týkajúcich sa trestných činov, registra trestov alebo bezpečnostných opatrení možno vykonávať iba pod kontrolou oficiálneho úradu, alebo ak sú k dispozícii vhodné špecifické bezpečnostné opatrenia podľa vnútroštátneho práva …"

52. V tejto súvislosti je dôležité pripomenúť už uvedený dokument pracovnej skupiny zriadenej podľa článku 29, ktorý sa zaoberá problematikou spracovania súdnych údajov ([35]). Pracovná skupina uvádza, že „Aj keď samozrejme každý má právo na spracovanie súdnych údajov v priebehu svojho vlastného sporu, zásada nezachádza tak ďaleko, aby povoľovala podrobné vyšetrovanie, získavanie a sústreďovanie osobných údajov tretími osobami vrátane systematického prieskumu vo všeobecnom meradle, ako sledovanie internetu (...). Takéto vyšetrovanie patrí do pôsobnosti súdnych orgánov" ([36]). Zatiaľ čo môže byť potrebné stanoviť získavanie cielených, konkrétnych dôkazov, najmä v prípadoch závažného porušovania, a uplatňovať právny nárok, EDPS plne súhlasí s názormi pracovnej skupiny podľa článku 29 o nedostatočnej oprávnenosti rozsiahlych vyšetrovaní zahŕňajúcich spracovanie obrovského množstva údajov o užívateľoch internetu.

53. Diskusie o uvedenej zásade primeranosti opísané vyššie a kritérium „obchodnej úrovne" sú dôležité na určenie, za akých podmienok bude získavanie IP adries a súvisiacich informácií oprávnené.

([35]) Pozri odsek 28 tohto stanoviska.
([36]) Doplnené je zvýraznenie.

54. PIS by sa mohli pokúsiť o získanie oprávnenia na spracovanie vykonávané nositeľmi autorských práv vložením doložky do svojich zmlúv s klientmi umožňujúcej monitorovanie údajov a ukončenie ich predplatenia. Ak by klienti takéto zmluvy uzavreli, súhlasili by s monitorovaním. Tento postup však prináša prvú zásadnú otázku, či fyzické osoby môžu poskytnúť PIS súhlas na spracovanie údajov, ktoré nebude vykonávať PIS, ale tretie strany, ktoré nepatria do „právomoci" PIS.

55. Po druhé je tu otázka platnosti súhlasu. Podľa článku 2 písm. h) smernice 95/46/ES súhlas znamená „slobodne poskytnutú a informovanú indikáciu jeho prianí, ktorou osoba pracujúca s údajmi prejaví svoj súhlas, aby sa osobné údaje, ktoré sa ho týkajú, spracovali". Dôležitým aspektom platnosti súhlasu je, že musí byť bez ohľadu na okolnosti, za ktorých bol poskytnutý, slobodným, konkrétnym a informovaným prejavom vôle dotknutej osoby, ako je definované v článku 2 ods. h) smernice. EDPS má vážne pochybnosti o tom, či fyzické osoby vyzvané k súhlasu na monitorovanie svojich internetových aktivít budú mať možnosť skutočného výberu – najmä preto, že alternatívou bude zamietnutie prístupu k internetu, a tak potenciálne ohrozia mnohé ďalšie oblasti ich života.

56. Po tretie je veľmi otázne, či sa takéto monitorovanie môže niekedy považovať za *nevyhnutné* pre plnenie zmluvy, ktorej zmluvnou stranou je dotknutý subjekt, ako sa požaduje v článku 7 ods. b) smernice 95/46/ES, pretože monitorovanie samozrejme nie je predmetom zmluvy, ktorú dotknutý subjekt uzavrel, ale iba prostriedkom pre PIS na iné záujmy.

Vymazanie zaznamenaných súborov

57. Podľa smernice 2002/58/ES, konkrétnejšie v jej článku 6, sa môžu byť prevádzkové údaje, ako napr. IP adresy získavať a uchovávať len z dôvodov priamo súvisiacich s vlastnou komunikáciou vrátane fakturácie, riadenia prevádzky a na účely boja proti podvodom. Potom sa musia údaje vymazať. Týmto nie sú dotknuté povinnosti vyplývajúce zo smernice o uchovávaní údajov, podľa ktorej, ako sa rozoberá, sa vyžaduje uchovávanie prevádzkových údajov a ich poskytnutie polícii a prokurátorom na pomoc **len** pri vyšetrovaní **závažného trestného činu** ([37]).

([37]) Pozri odsek 35 tohto stanoviska.

58. V súlade s uvedeným by poskytovatelia internetových služieb mali vymazať každý zaznamenaný súbor, ktorý odhaľuje aktivity užívateľov internetu, ktoré už nie sú potrebné na uvedené účely. Pri zohľadnení, že zaznamenané súbory nie sú nevyhnutné na účely fakturácie, by podľa všetkého mali byť pre PIS tri alebo štyri týždne dostačujúce na účely prevádzkového riadenia ([38]).

59. To znamená, že pri kontaktovaní nositeľov autorských práv, pokiaľ došlo k takémuto kontaktu vo vymedzenom období uvedenom vyššie, by PIS nemal mať súbory, na základe ktorých by sa IP adresy mohli dať do súvisu s príslušnými účastníkmi. Zaznamenané súbory mimo takéhoto obdobia by sa mali zachovať len z oprávnených dôvodov v rámci rozsahu účelov stanovených zákonom.

60. V praxi to znamená, že pokiaľ sa požiadavky nositeľa autorských práv adresované PIS neuskutočnia veľmi rýchlo, nebudú môcť byť splnené jednoducho preto, že PIS už nebude mať k dispozícii informácie. To samé o sebe stanovuje hranice toho, čo sa myslí pod prijateľnými monitorovacími postupmi vo vyššie uvedenom oddiele.

Riziká vedľajších účinkov

61. EDPS sa ďalej obáva nielen vplyvu na súkromie a ochranu osobných údajov, ale aj ich vedľajších účinkov. Ak by sa politiky trikrát a dosť na odpojenie od internetu povolili, mohlo by to viesť k legitimizovaniu ešte masívnejšieho dohľadu nad aktivitami užívateľov internetu v rôznych oblastiach a pre rôzne účely.

62. EDPS vyzýva Komisiu, aby zabezpečila, že dohoda ACTA nepôjde nad rámec a proti súčasnému systému EÚ na vymáhanie práv duševného vlastníctva, ktoré rešpektujú základné práva a slobody a občianske slobody, ako napr. ochrana osobných údajov.

V. **ASPEKTY OCHRANY ÚDAJOV Z HĽADISKA MECHANIZMOV MEDZINÁRODNEJ SPOLUPRÁCE**

63. Jedným z prostriedkov predložených účastníkmi ACTA na účely riešenia otázky vymáhania PDV je zvýšiť

([38]) K riadeniu prevádzky patrí analýza prevádzky počítačovej siete s cieľom optimalizovať alebo zaručiť výkon, znížiť oneskorenie a/alebo zvýšiť využiteľnú šírku pásma.

medzinárodnú spoluprácu viacerými opatreniami, ktoré by umožnili efektívne vymáhanie práv duševného vlastníctva v jurisdikciách signatárov ACTA.

64. Vzhľadom na dostupné informácie možno predpokladať, že rad opatrení plánovaných na zabezpečenie vymáhania práv duševného vlastníctva sa bude týkať medzinárodnej výmeny informácií o údajnom porušovaní PDV medzi verejnými orgánmi (napr. colná správa, polícia a súdnictvo), ale aj medzi verejnými a súkromnými subjektmi (napr. PIS a organizácie nositeľov práv duševného vlastníctva). Takéto prenosy údajov vyvolávajú z hľadiska ochrany údajov množstvo otázok.

V.1. **Sú predpokladané výmeny údajov v kontexte dohody ACTA legitímne, nevyhnutné a primerané?**

65. V súčasnom štádiu priebehu rokovaní, v ktorom viaceré konkrétne prvky spracovania údajov nie sú ešte vymedzené alebo sú neznáme, nie je možné overiť, či navrhovaný rámec opatrení je v súlade so základnými zásadami ochrany údajov a práva EÚ o ochrane údajov.

66. Ako prvú možno spochybniť legitímnosť prenosov údajov do tretích krajín v kontexte dohody ACTA. Spochybniť možno význam prijímania opatrení na medzinárodnej úrovni v tejto oblasti, pokiaľ nedôjde k dohode v rámci členských štátov EÚ o harmonizácii opatrení na vymáhanie práv v digitálnom prostredí a druhoch uplatňovaných trestných sankcií ([39]).

67. Vzhľadom na uvedené sa ukazuje, že zásady nevyhnutnosti a primeranosti prenosov údajov v rámci dohody ACTA by sa dali ľahšie splniť, ak by dohoda bola výslovne obmedzená na boj proti najzávažnejším trestným činom porušovania PDV namiesto povolenia hromadných prenosov údajov týkajúcich sa každého podozrenia z porušenia PDV. Bude si to vyžadovať presné vymedzenie rozsahu toho, čo predstavuje „najzávažnejšie trestné činy porušovania PDV“, v prípade ktorých možno uskutočniť prenosy údajov.

68. Navyše by sa osobitná pozornosť mala venovať osobám podieľajúcim sa na výmene údajov a tomu, či sa údaje vymieňajú len medzi verejnými orgánmi, alebo či bude zahŕňať aj výmenu medzi súkromnými subjektmi a verejnými orgánmi. Ako už bolo uvedené v tomto stanovisku, zapojenie súkromných subjektov do oblasti, ktorá je v zásade v kompetencii orgánov činných v trestnom konaní, vyvoláva mnohé obavy ([40]). Podmienky, na základe ktorých sa súkromné subjekty budú podieľať na získavaní a výmene osobných údajov v súvislosti s porušovaním práv duševného vlastníctva s orgánmi verejnej správy, by sa mali byť prísne obmedziť na konkrétne okolnosti s primeranými zárukami.

V.2. **Platné právo o ochrane údajov, ktorými sa riadia prenosy údajov v kontexte dohody ACTA**

Všeobecný režim prenosov údajov

69. Všeobecný rámec ochrany údajov platný v EÚ je ustanovený v smernici 95/46/ES. V článkoch 25 a 26 smernice 95/46/ES je stanovený režim, ktorý sa môže použiť na prenos údajov do tretích krajín. V článku 25 sa požaduje, aby sa prenosy uskutočňovali len do krajín, ktoré zabezpečujú adekvátnu úroveň ochrany, inak sú takéto prenosy v zásade zakázané.

70. Európska komisia posudzuje úroveň adekvátnosti poskytovanú tretími krajinami podľa jednotlivých prípadov a vydala niekoľko rozhodnutí, ktorými po dôkladnej analýze pracovnej skupiny zriadenej podľa článku 29 uznala adekvátnosť v prípade viacerých krajín ([41]).

71. EDPS konštatuje, že väčšina strán dohody ACTA nie je zahrnutá v zozname krajín, ktoré poskytujú adekvátnu ochranu údajov navrhnutú Komisiou: okrem Švajčiarska a za určitých okolností Kanady a USA, všetky ostatné strany dohody ACTA neboli uznané ako krajiny poskytujúce adekvátnu úroveň ochrany. To znamená, že v prípade údajov, ktoré sa majú preniesť z EÚ do týchto krajín, musí byť splnená jedna z podmienok článku 26 ods. 1 smernice 95/46/ES, alebo strany musia predložiť vhodné záruky na prenos údajov v súlade s článkom 26 ods. 2 smernice.

Osobitný režim prenosov údajov v oblasti uplatňovania trestného práva

72. Zatiaľ čo smernica 95/46/ES predstavuje hlavný nástroj na ochranu údajov v EÚ, v súčasnosti je jej rozsah obmedzený, pretože výslovne vylučuje aktivity týkajúce sa okrem iného činností štátu v oblasti trestného práva (článok 3). Výmeny údajov na účely uplatňovania trestného práva, preto nepatria do pôsobnosti smernice 95/46/ES a budú

([39]) O návrhu trestných sankcií sa v súčasnosti rokuje v Rade, KOM(2006) 168 z 26. apríla 2006.

([40]) Pozri odseky 32 a 52 tohto stanoviska. Pozri aj stanovisko EDPS k záverečnej správe kontaktnej skupiny EÚ – USA na vysokej úrovni pre spoločné využívanie informácií a ochranu súkromia a osobných údajov, Ú. v. EÚ C 128, 6.6.2009, s. 1.

([41]) Pozri rozhodnutia o adekvátnosti, ktoré Európska komisia vydala Argentíne, Kanade, Švajčiarsku, USA Safe Harbor (bezpečný prístav) a orgánom USA v kontexte s prenosom údajov zo záznamu o cestujúcom, Guernsey, Ostrovu Man a Jersey, k dispozícii na http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm

podliehať všeobecným zásadám ochrany údajov stanoveným v Dohovore Rady Európy č 108 a jeho dodatkovom protokole, ktorého zmluvnými stranami sú všetky členské štáty EÚ ([42]). Okrem toho budú platiť pravidlá, ktoré prijala EÚ v oblasti policajnej a justičnej spolupráce v trestných veciach, ktoré sú stanovené v rámcovom rozhodnutí Rady 2008/877/JHA ([43]).

73. Tieto nástroje tiež predstavujú zásadu, že musí existovať adekvátna úroveň ochrany údajov v tretej krajine, do ktorej majú byť údaje prenesené. Poskytlo sa niekoľko výnimiek najmä vtedy, keď tretia krajina poskytuje vhodnú záruku. Podobne ako v prípade výmeny údajov podľa smernice 95/46/ES sa preto bude v prípade výmeny údajov v oblasti uplatňovania trestného práva vyžadovať, aby účastníci prenosu údajov poskytli vhodné záruky pre uskutočnenie takéhoto prenosu.

Smerovanie k novému režimu prenosu údajov

74. V blízkej budúcnosti môžeme očakávať, že EÚ prijme na základe článku 16 ZFEÚ nové spoločné pravidlá na ochranu údajov, ktoré sa budú uplatňovať na všetky oblasti činnosti EÚ. To znamená, že za niekoľko rokov by mohol existovať komplexný rámec EÚ na ochranu údajov, v ktorom budú stanovené jednotné pravidlá na ochranu údajov vo všetkých oblastiach činnosti EÚ, ktorými sa uloží rovnaká úroveň ochrany a záruk na všetky aktivity v oblasti spracovania údajov. Ako uviedla Viviane Redingová ([44]), komisárka pre spravodlivosť, základné práva a občianstvo, tento nový rámec by mal fungovať ako jediný „moderný a komplexný právny nástroj" na ochranu údajov v EÚ. Takýto rámec je mimoriadne vítaný, pretože by mohol priniesť vyššiu mieru prehľadnosti a jednotnosti, pokiaľ ide o pravidlá platné v EÚ súvisiace s ochranou údajov.

75. Z medzinárodného hľadiska EDPS poukazuje aj na uznesenie o medzinárodných normách na ochranu osobných údajov a súkromia, ktoré nedávno prijali orgány na ochranu údajov, ktoré je prvým krokom k zavedeniu celosvetových noriem na ochranu údajov ([45]). Medzinárodné normy obsahujú viaceré záruky na ochranu údajov podobné tým, ktoré sú uvedené v smernici 95/46/ES a dohovore č. 108. Hoci medzinárodné normy nie sú zatiaľ záväzné, poskytujú užitočné usmernenie, pokiaľ ide o zásady ochrany údajov, ktoré môžu tretie krajiny dobrovoľne uplatňovať tak, aby ich právny rámec bol v súlade s normami EÚ. EDPS sa domnieva, že signatári dohody ACTA by mali tiež zohľadňovať zásady stanovené v medzinárodných normách pri spracovaní osobných údajov z EÚ.

V.3. **Potreba zaviesť vhodné záruky na ochranu prenosov údajov z EÚ do tretích krajín**

Akú formu majú mať záruky, aby účinne chránili prenosy údajov do tretích krajín?

76. Ak sa preukáže, že prenos osobných údajov do tretích krajín je potrebný, EDPS zdôrazňuje, že Európska únia by mala prerokovať s príjemcami v tretej krajine – okrem samotnej dohody ACTA – špecifické nástroje, ktoré zahŕňajú primerané záruky na ochranu údajov, ktorými sa bude riadiť výmena osobných údajov.

77. Primerané záruky na ochranu údajov by sa spravidla mali stanoviť v záväznej dohode medzi EÚ a príjemcom v tretej krajine, v ktorej sa prijímajúca strana zaväzuje rešpektovať právo EÚ o ochrane údajov a poskytnúť jednotlivcom rovnaké práva a opravné prostriedky, ako poskytuje právo EÚ. Potreba záväznej dohody vyplýva z článku 26 ods. 2 smernice 95/46/ES a článku 13 ods. 3 písm. b) rámcového rozhodnutia, a okrem toho sa opiera o existujúcu prax EÚ v uzatváraní konkrétnych dohôd, ktoré umožňujú prenosy konkrétnych údajov do tretích krajín ([46]).

78. Podobne podľa návrhu medzinárodných noriem sa od príjemcu môže požadovať, aby zaručil, že poskytne požadovanú úroveň ochrany v prípade uskutočnenia transferu. Tieto záruky by mohli mať aj formu zmluvného záväzku.

Obsah záruk, ktoré majú signatári dohody ACTA poskytnúť pri prenosoch osobných údajov

79. EDPS predovšetkým zdôrazňuje, že medzinárodné výmeny informácií na účely vymáhania práva, sú obzvlášť citlivé z hľadiska ochrany údajov, samotný rámec by mohol

([42]) Dohovor Rady Európy o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov prijatý 28. januára 1981 v Štrasburgu a dodatočný protokol k dohovoru o ochrane jednotlivcov vzhľadom na automatizované spracovanie osobných údajov týkajúce sa dozorných orgánov a cezhraničných tokov údajov, Štrasburg, 8. novembra 2001.

([43]) Rámcové rozhodnutie Rady 2008/977/SVV z 27. novembra 2008 o ochrane osobných údajov spracúvaných v rámci policajnej a justičnej spolupráce v trestných veciach, Ú. v. EÚ L 350, 30.12.2008, s. 60.

([44]) Pozri odpovede na dotazník Európskeho parlamentu pre dezignovanú komisárku Viviane Redingovú, s. 5, http://www.europarl.europa.eu/hearings/static/commissioners/answers/reding_replies_en.pdf

([45]) Rezolúcia prijatá v Madride v novembri 2009.

([46]) Napríklad dohody Europolu a Eurojustu s USA, dohoda PNR, dohoda Swift, dohoda medzi EÚ a Austráliou o spracúvaní a prenose údajov zo záznamu o cestujúcom (PNR) s pôvodom v Európskej únii leteckými dopravcami Austrálskej colnej správe.

legitimizovať hromadné prenosy údajov v oblasti, kde je vplyv na jednotlivca obzvlášť závažný a kde sú o to viac potrebné prísne a spoľahlivé záruky.

80. EDPS uvádza, že osobitné podmienky a záruky sa môžu stanoviť len na základe jednotlivých prípadov vzhľadom na všetky parametre pre výmenu údajov. Na účely usmernenia však ESPS zdôrazňuje niektoré ďalej uvedené zásady a záruky, ktoré musia predložiť príjemcovia tretej strany na uskutočnenie prenosu údajov:

— Potrebné je overiť právne odôvodnenie, podľa ktorého prebiehajú aktivity súvisiace so spracovaním údajov (t. j. zakladá sa spracovanie na právnej povinnosti, na súhlase dotknutého subjektu alebo inom platnom dôvode?), a či sa pri prenosoch údajov rešpektuje pôvodný účel získavania údajov. Mimo rozsahu konkrétneho účelu by sa nemali uskutočniť žiadne prenosy.

— Malo by sa jasne špecifikovať množstvo a typy osobných údajov, ktoré sa majú vymieňať, a mali by sa obmedziť na to, čo je nevyhnutné na dosiahnutie účelu prenosu. Získané a prenesené osobné údaje môžu zahŕňať najmä IP adresu užívateľov internetu, dátum a čas podozrenia z trestného činu a druh trestného činu. EDPS odporúča, aby sa údaje nespájali so žiadnym konkrétnym jednotlivcom počas fázy vyšetrovania a pripomína, že k identifikácii podozrivej osoby by malo dôjsť v súlade s právnymi predpismi a pod dohľadom sudcu. Z tohto hľadiska EDPS uvádza, že údaje týkajúce sa porušovania práv duševného vlastníctva a podozrení z porušovania sú osobitnou kategóriou údajov, ktorých spracovanie sa obvykle obmedzuje na orgány činné v trestnom konaní a vyžaduje použitie ďalších záruk. Osoby oprávnené spracúvať údaje týkajúce sa porušovania práv duševného vlastníctva a podozrení z jeho porušovania, ako aj podmienky spracovania týchto údajov sa teda musia konkrétne stanoviť v súlade s existujúcimi právnymi predpismi na ochranu údajov.

— Osoby, medzi ktorými sa údaje môžu vymieňať, musia byť jasne stanovené a ďalšie prenosy iným príjemcom by sa mali v zásade zakázať, pokiaľ takéto prenosy nie sú nevyhnutné pre konkrétne vyšetrovanie. Toto obmedzenie je obzvlášť dôležité, keďže určení príjemcovia by si nemali nenáležite vymieňať informácie s nepovolenými príjemcami.

— EDPS predpokladá, že v dohode ACTA sa nielen plánuje spolupráca medzi verejnými orgánmi, ale že sa v nej súkromné organizácie poveria vymáhaním (napr. poskytovatelia internetových služieb, organizácie autorských práv atď.). V takomto prípade musia byť podmienky a miera účasti súkromných organizácií na vymáhaní práv duševného vlastníctva starostlivo posúdiť v tom zmysle, aby opatrenia dohody ACTA neposkytovali PIS a organizáciám nositeľov práv *de facto* právo na monitorovanie online správania používateľov. Okrem toho by sa spracovanie osobných údajov súkromnými organizáciami v súvislosti s vymáhaním práva malo uskutočňovať iba na vhodnom právnom základe. Tiež je dôležité objasniť, či súkromné organizácie budú mať povinnosť spolupracovať s políciou a aký bude rozsah tejto spolupráce. V každom prípade by sa to malo obmedziť len na „závažné trestné činy“, ktorých vymedzenie sa bude tiež musieť presne stanoviť, pretože nie všetky prípady porušenia PDV sa považujú za závažné trestné činy.

— Metóda použitá na výmenu osobných údajov sa musí jasne vybrať, najmä by sa malo uviesť, či sa vykoná prostredníctvom systému „vysielania“ („push“) – napr. PIS a organizácie nositeľov PDV by uskutočňovali pod svojou kontrolou prenos niektorých údajov tretím stranám, ako napr. polícia a orgány činné v trestnom konaní sídliace v zahraničí – alebo systému „vyťaženia“ („pull“) – napr. polícia a orgány činné v trestnom konaní by mali priamy prístup k databázam súkromných osôb alebo k databázam, kde sú sústredené informácie. Ako už bolo uvedené v súvislosti s PNR, systém vysielania je jedinou možnosťou v súlade so zásadami ochrany údajov z hľadiska EÚ týkajúceho sa ochrany údajov, pretože oprávňuje odosielateľa EÚ, ktorý je s najväčšou pravdepodobnosťou správcom údajov, vykonávať kontrolu nad prenosom údajov ([47]).

— Obdobie, počas ktorého budú príjemcovia uchovávať osobné údaje, sa musí špecifikovať, rovnako ako aj účel, pre ktorý je takéto uchovávanie potrebné. Takéto obdobie uchovávania by malo byť primerané vzhľadom na účel, ktorý sa má dosiahnuť, čo znamená, že údaje by mali byť odstránené alebo vymazané, ak už nie sú potrebné na dosiahnutie tohto účelu.

— Povinnosti uložené správcom údajov v tretích krajinách by mali byť jasne stanovené. Mechanizmy dohľadu a/alebo mechanizmy vymáhateľnej zodpovednosti musia byť zabezpečené tak, aby existovali účinné právne prostriedky a sankcie voči správcom údajov v prípade neoprávneného spracovania alebo iných

([47]) Pozri stanovisko 4/2003 pracovnej skupiny zriadenej podľa článku 29 o úrovni ochrany zabezpečenej v USA v prípade prenosu údajov o cestujúcich, WP78, 13. júna 2003.

súvisiacich prípadov. Okrem toho by sa mali zaviesť mechanizmy na zabezpečenie nápravy, aby osoby mohli podať sťažnosť nezávislému orgánu na ochranu údajov a aby sa mohli hľadať účinné prostriedky nápravy pred nezávislým a nestranným súdom ([48]).

— V nástroji dohodnutom obomi stranami by sa mali jasne špecifikovať práva dotknutých subjektov, pokiaľ ide o ich osobné údaje, keď takéto údaje spracúva príjemca tretej osoby, aby sa zaručilo, že budú mať účinný prostriedok na vymáhanie svojich práv vo vzťahu k spracovaniu v zahraničí.

— Ďalej je ešte rozhodujúca transparentnosť a strany nástroja vzťahujúceho sa na ochranu údajov sa musia dohodnúť na tom, ako budú informovať dotknuté subjekty o spracovaní údajov, ktoré sa uskutočňuje, ako aj o ich právach a o tom, ako ich vykonávať.

VI. **ZÁVERY**

81. EDPS dôrazne odporúča Európskej komisii, aby usporiadala verejné a transparentné diskusie o dohode ACTA, pokiaľ možno vo forme verejných konzultácií, čo by tiež pomohlo zabezpečiť, aby opatrenia, ktoré sa majú prijať, boli v súlade s požiadavkami práva EÚ o ochrane súkromia a údajov.

82. V rámci prebiehajúcich rokovaní o dohode ACTA EDPS vyzýva Európsku komisiu, aby nastolila vhodnú rovnováhu medzi požiadavkami na ochranu práv duševného vlastníctva a právom na ochranu súkromia a údajov. EDPS zdôrazňuje, že je obzvlášť dôležité, aby sa ochrana súkromia a osobných údajov zohľadňovala od úplného začiatku rokovaní predtým, ako sa dohodne nejaké opatrenie, aby sa neskôr nemuseli hľadať alternatívne riešenia na rešpektovanie súkromia.

83. Aj keď duševné vlastníctvo je pre spoločnosť dôležité a musí sa chrániť, nemalo by sa klásť nad základné práva jednotlivcov na súkromie, ochranu údajov a ďalšie práva, ako je prezumpcia neviny, účinná súdna ochrana a sloboda prejavu.

84. Pokým súčasný návrh dohody ACTA obsahuje, alebo sa v ňom nepriamo presadzujú politiky trikrát a dosť na odpojenie od internetu, dohodou ACTA by sa veľmi obmedzili základné práva a slobody európskych občanov, najmä ochrana osobných údajov a súkromia.

85. EDPS zastáva názor, že politiky trikrát a dosť na odpojenie od internetu nie sú nevyhnutné na dosiahnutie účelu, ktorým je vymáhanie práv duševného vlastníctva. EDPS je presvedčený, že existujú alternatívne menej rušivé riešenia, alebo že plánované politiky možno vykonávať menej rušivým spôsobom alebo v obmedzenejšom rozsahu, a to predovšetkým formou cieleného *ad hoc* monitorovania.

86. Politiky trikrát a dosť na odpojenie od internetu sú tiež problematické na podrobnejšej právnej úrovni najmä preto, že spracovanie súdnych údajov, najmä súkromnými organizáciami, sa musí zakladať na vhodnom právnom základe. Realizácia systémov trikrát a dosť môže ďalej viesť k dlhodobejšiemu uchovávaniu zaznamenaných súborov, čo by bolo v rozpore s platnými právnymi predpismi.

87. Okrem toho, pokiaľ dohoda ACTA zahŕňa výmenu osobných údajov medzi orgánmi a/alebo súkromnými organizáciami so sídlom v signatárskych krajinách, EDPS vyzýva Európsku úniu, aby zaviedla príslušné záruky. Tieto záruky by mali platiť na všetky prenosy údajov v kontexte dohody ACTA – či už k nim dochádza pri vymáhaní práv v oblasti občianskoprávnej, trestnoprávnej alebo vymáhania digitálnych práv – a mali by byť v súlade so zásadami ochrany údajov stanovenými v dohovore č. 108 a smernici 95/46/ES. EDPS odporúča, aby tieto ochranné opatrenia mali formu záväzných dohôd medzi odosielateľmi v EÚ a príjemcami v tretích krajinách.

88. EDPS si ďalej želá, aby sa s ním konzultovali opatrenia, ktoré sa majú zaviesť v súvislosti s prenosom údajov, ktorý sa bude konať v rámci dohody ACTA s cieľom overiť ich primeranosť a zaručiť adekvátnu úroveň ochrany údajov.

V Bruseli 22. februára 2010

Peter HUSTINX

európsky dozorný úradník pre ochranu údajov

([48]) Pozri stanovisko Európskeho dozorného úradníka pre ochranu údajov k záverečnej správe kontaktnej skupiny EÚ – USA na vysokej úrovni pre spoločné využívanie informácií a ochranu súkromia a osobných údajov, 11.11.2008.