I

*(Resolucije, priporočila in mnenja)*

# MNENJA

# EVROPSKI NADZORNIK ZA VARSTVO PODATKOV

## Mnenje Evropskega nadzornika za varstvo podatkov o trenutnih pogajanjih Evropske unije o trgovinskem sporazumu o boju proti ponarejanju (Anti-Counterfeiting Trade Agreement – ACTA)

(2010/C 147/01)

EVROPSKI NADZORNIK ZA VARSTVO PODATKOV JE –

ob upoštevanju Pogodbe o delovanju Evropske unije in zlasti člena 16 Pogodbe,

ob upoštevanju Listine Evropske unije o temeljnih pravicah in zlasti člena 8 Listine,

ob upoštevanju Direktive Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ([1]),

ob upoštevanju Direktive 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij ([2]),

ob upoštevanju Uredbe (ES) št. 45/2001 Evropskega parlamenta in Sveta z dne 18. decembra 2000 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah in organih Skupnosti in o prostem pretoku takih podatkov ([3]) ter zlasti člena 41 Uredbe –

SPREJEL NASLEDNJE MNENJE:

### I. UVOD

1. Evropska unija sodeluje v pogajanjih o pripravi trgovinskega sporazuma o boju proti ponarejanju (Anti-Counterfeiting Trade Agreement, ACTA). Pogajanja so se začela leta 2007 v okviru prvotne skupine zainteresiranih strani in se nadaljevala s širšo skupino udeležencev, ki do danes vključuje Avstralijo, Kanado, Evropsko unijo, Japonsko, Južno Korejo, Mehiko, Maroko, Novo Zelandijo, Singapur, Švico in Združene države Amerike. Evropska komisija je mandat Sveta, da pristopi k tem pogajanjem, dobila leta 2008.

2. Evropski nadzornik za varstvo podatkov (ENVP) meni, da čezmejna trgovina s ponarejenim in piratskim blagom postaja pojav, ki vzbuja vedno več skrbi in ki pogosto vključuje organizirane kriminalne mreže, kar zahteva sprejetje primernih mehanizmov sodelovanja na mednarodni ravni za boj proti tej obliki kriminala.

3. ENVP poudarja, da se pri pogajanjih Evropske unije o večstranskem sporazumu, katerega bistvo je uveljavljanje pravic intelektualne lastnine, postavljajo bistvena vprašanja o vplivu sprejetih ukrepov za boj proti ponarejanju in piratstvu na temeljne pravice posameznikov ter zlasti njihovo pravico do zasebnosti in varstva osebnih podatkov.

4. ENVP še zlasti obžaluje, da se Evropska komisija z njim ni posvetovala o vsebini takega sporazuma. Tako je na podlagi člena 41(2) Uredbe (ES) št. 45/2001 na lastno pobudo sprejel to mnenje, da bi Komisiji zagotovil smernice v zvezi z vidiki varstva zasebnosti in osebnih podatkov, ki jih je treba upoštevati v pogajanjih o sporazumu ACTA.

### II. STANJE IN PREDVIDENA VSEBINA SPORAZUMA ACTA

5. Sedmi niz posvetovanj je potekal v Mehiki od 26. do 29. januarja 2010, njegov namen pa je bil, da bi sporazum sklenili leta 2010. Vendar pa vse do danes uradni osnutek sporazuma še ni bil izdan.

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

6. Cilj posvetovanj je sprejetje novega večstranskega sporazuma, namenjenega krepitvi uveljavljanja pravic intelektualne lastnine ter boja proti ponarejanju in piratstvu. Če bo ta novi sporazum sprejet, bo izboljšal mednarodne standarde o tem, kako ukrepati proti hudim kršitvam pravic intelektualne lastnine. Generalni direktorat Evropske komisije za trgovino je še posebej opozoril, da „je predvideni poudarek predvsem na dejavnostih ponarejanja in piratstva, ki znatno vplivajo na trgovinske interese, ne pa na dejavnostih navadnih državljanov“ ([4]).

7. Kar zadeva vsebino, *Povzetek ključnih elementov razprave*, ki ga je Generalni direktorat Evropske komisije za trgovino izdal novembra 2009, nakazuje, da bo na podlagi sporazuma ACTA boj proti piratstvu in ponarejanju potekal s tremi osnovnimi sredstvi: (i) mednarodnim sodelovanjem, (ii) praksami izvrševanja in (iii) opredelitvijo pravnega okvira za uveljavljanje pravic intelektualne lastnine na različnih področjih, še zlasti v digitalnem okolju ([5]). S predvidenimi ukrepi se bodo obravnavali predvsem pravni postopki (kot so sodne prepovedi, začasni ukrepi), vloga in odgovornost ponudnikov internetnih storitev pri odvračanju od kršitev avtorskih pravic na spletu ter ukrepi čezmejnega sodelovanja pri preprečevanju, da bi blago prečkalo meje. Javno znane informacije pa samo prinašajo splošne smernice sporazuma ter podrobno ne obravnavajo nobenega posebnega in konkretnega ukrepa.

8. ENVP ugotavlja, da je poglavitni cilj sporazuma ACTA sicer preganjati hude kršitve pravic intelektualne lastnine, a ni mogoče izključiti, da bodo na podlagi sporazuma ACTA zajete tudi dejavnosti navadnih državljanov, še zlasti ker se izvršilni ukrepi uveljavljajo v digitalnem okolju. ENVP poudarja, da morajo biti zato sprejeta ustrezna jamstva za varovanje temeljnih pravic posameznikov. Poleg tega zakonodaja o varstvu podatkov zajema vse posameznike, tudi tiste, ki so morda vpleteni v dejavnosti ponarejanja in piratstva; v boj proti hudim kršitvam bo prav gotovo vključena tudi obdelava osebnih podatkov.

9. ENVP zato resno spodbuja Evropsko komisijo, naj začne javen in pregleden dialog o sporazumu ACTA, morda z javnim posvetovanjem, kar bi pomagalo zagotoviti, da bodo sprejeti ukrepi v skladu z zahtevami zakonodaje EU glede varstva zasebnosti in podatkov.

## III. **OBSEG PRIPOMB EVROPSKEGA NADZORNIKA ZA VARSTVO PODATKOV**

10. ENVP resno poziva EU, zlasti pa Evropsko komisijo, ki je dobila mandat za sklenitev sporazuma, naj poišče pravo ravnovesje med zahtevami za varovanje pravic intelektualne lastnine ter pravicami posameznikov do zasebnosti in varstva podatkov.

11. ENVP poudarja, da sta zasebnost in varstvo podatkov temeljni vrednoti Evropske unije, priznani v členu 8 EKČP ter členih 7 in 8 Listine Evropske unije o temeljnih pravicah ([6]), ki ju je treba upoštevati pri vseh politikah in pravilih, ki jih EU sprejme v skladu s členom 16 Pogodbe o delovanju Evropske unije (PDEU).

12. ENVP poudarja tudi, da mora biti vsak dogovor, ki ga Evropska unija doseže o sporazumu ACTA, v skladu s pravnimi obveznostmi, ki jih ima EU v zvezi z zakonodajo o zasebnosti in varstvu osebnih podatkov, kakor je zlasti določeno v Direktivi 95/46/ES, Direktivi 2002/58/ES ([7]) ter sodni praksi Evropskega sodišča za človekove pravice ([8]) in Sodišča Evropske unije ([9]).

13. Varstvo zasebnosti in podatkov je treba upoštevati od samega začetka pogajanj, in ne takrat, ko so programi in postopki že opredeljeni in dogovorjeni ter je že prepozno za iskanje drugih rešitev, ki bi bile ustrezne z vidika zasebnosti.

14. Ker je bilo javnosti danih na voljo tako malo informacij, ENVP meni, da ne more analizirati posebnih določb sporazuma ACTA. V tem mnenju se bo zato osredotočil na prikaz mogočih groženj za varstvo zasebnosti in podatkov, ki bi jih sporazum, kakršen je bil predstavljen, s svojimi dejanskimi ukrepi lahko sprožil na naslednjih dveh področjih: uveljavljanje pravic intelektualne lastnine v digitalnem okolju (poglavje IV) in mehanizmi mednarodnega sodelovanja (poglavje V).

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

([5]) Glej zgornjo opombo 2.

([6]) Listina Evropske unije o temeljnih pravicah, UL C 303, 14.12.2007, str. 1.

([7]) Direktiva 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah), UL L 201, 31.7.2002, str. 37.

([8]) Razlaga ključnih elementov in pogojev, ki so določeni v členu 8 Evropske konvencije o varstvu človekovih pravic in temeljnih svoboščin (EKČP), ki je bila sprejeta 4. novembra 1950 v Rimu, saj se nanašajo na različna področja. Glej sodno prakso, navedeno v tem mnenju.

([9]) Glej zadevo *Productores de Música de España* (Promusicae), C-275/06, ZOdl., str. I-271, in zadevo *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten*, C-557/07, še neobjavljena.

## IV. UVELJAVLJANJE PRAVIC INTELEKTUALNE LASTNINE V DIGITALNEM OKOLJU

### IV.1 Potreba po analizi posledic politike treh napak pred odklopom interneta na varstvo zasebnosti/podatkov

15. Evropska komisija meni, da bo s sporazumom ACTA ustvarjen pravni okvir za boj proti piratstvu v digitalnem okolju ([10]). Ta okvir bo določal pogoje, na podlagi katerih bodo ponudniki internetnih storitev in drugi internetni posredniki ([11]) lahko odgovarjali zaradi kršitev avtorskega dela, ki se bodo zgodile prek njihovih zmogljivosti. Z okvirjem bodo zagotovljeni tudi ukrepi in pravna sredstva, naloženi internetnim uporabnikom zaradi kršenja avtorskega dela z njegovim prenašanjem na računalnik ali strežnik. Medtem ko podrobnosti o takem okviru še niso bile uradno objavljene, se lahko na podlagi podatkov, pridobljenih iz različnih virov, predvideva, da bi lahko vključeval uvedbo obveznosti za ponudnike internetnih storitev, da sprejmejo politiko treh napak pred odklopom interneta, imenovano tudi shema „postopnega odziva“. Take sheme bodo imetnikom avtorskih pravic omogočale, da spremljajo uporabnike interneta in odkrijejo domnevne kršitelje avtorskih pravic. Po navezavi stika s ponudniki internetnih storitev bi ti opozorili uporabnika, opredeljenega kot kršitelja, da mu bo po treh opominih onemogočen dostop do interneta.

16. Politika treh napak pred odklopom interneta se med pogajanji o sporazumu ACTA že izvaja v nekaterih državah članicah, npr. v Franciji. O politikah se razpravlja tudi na različnih forumih EU, kot je dialog zainteresiranih strani o nezakonitem nalaganju na računalnik in strežnik, ki ga trenutno vodi Generalni direktorat Evropske komisije za notranji trg in storitve, v povezavi s sprejetjem sporočila Komisije o izboljšanju uveljavljanja pravic intelektualne lastnine na notranjem trgu ([12]). Razprave o tej temi potekajo tudi v Evropskem parlamentu v okviru aktualne razprave o osnutku resolucije Evropskega parlamenta o izboljšanju uveljavljanja pravic intelektualne lastnine na notranjem trgu (v nadaljnjem besedilu: poročilo Gallo).

17. Take prakse močno posegajo v zasebnost posameznikov. Njihova posledica je splošno nadzorovanje dejavnosti uporabnikov interneta, tudi tistih, ki so popolnoma zakonite. Zadevajo milijone uporabnikov interneta, ki se ravnajo po zakonu, tudi številne otroke in mladostnike. Izvajajo jih zasebne stranke, in ne organi pregona. Poleg tega ima internet danes glavno vlogo v skoraj vseh vidikih sodobnega življenja, zato so lahko posledice odklopa interneta velike, saj posameznikom onemogoči dostop do dela, kulture, storitev e-uprave itd.

18. V zvezi s tem je treba oceniti obseg, v katerem so te politike v skladu z zakonodajo EU o varstvu podatkov in zasebnosti, zlasti pa, ali je politika treh napak pred odklopom interneta nujen ukrep za uveljavljanje pravic intelektualne lastnine. V tem smislu je treba še dodatno analizirati, ali obstajajo druge manj invazivne metode.

19. Še vedno ni jasno, ali bo politika treh napak pred odklopom interneta del sporazuma ACTA. Vendar se o uvedbi te politike razmišlja tudi na drugih področjih, in tako imaj lahko ogromen vpliv na varstvo osebnih podatkov in zasebnosti. ENVP iz teh razlogov meni, da je to politiko nujno obravnavati v tem mnenju. Pred izvedbo navedene analize bo na kratko opisal veljavni pravni okvir za varstvo osebnih podatkov in zasebnosti.

20. Treba je opozoriti, da politika treh napak pred odklopom interneta vzbuja skrb ne le glede osebnih podatkov in zasebnosti, ampak tudi glede drugih vrednot, kot sta predpisani postopek in svoboda govora. V tem mnenju bodo obravnavana samo vprašanja, ki so povezana z varstvom osebnih podatkov in zasebnostjo posameznikov.

### IV.2 Politika treh napak pred odklopom interneta in uporaba pravnega okvira EU za varstvo podatkov in zasebnosti

*Kako vzpostaviti politiko treh napak pred odklopom interneta*

21. Na kratko, imetniki avtorskih pravic bi na podlagi politike treh napak pred odklopom interneta z uporabo avtomatiziranih tehničnih sredstev, ki bi jih po možnosti zagotovile tretje stranke, opredelili domnevne kršitve avtorskih pravic s spremljanjem dejavnosti uporabnikov interneta, na primer

([10]) Glej zgornjo opombo.

([11]) Različne spletne posrednike je mogoče določiti v skladu z njihovimi funkcionalnimi vlogami. Vendar imajo posredniki v resničnem svetu več navedenih funkcij. Spletni posredniki vključujejo: a) *ponudnike dostopa*: uporabniki dostopajo do omrežja tako, da se priključijo na strežnik ponudnika dostopa; b) *ponudnike omrežja*: zagotovijo usmerjevalnike, tj. ustrezna tehnična orodja, potrebna za prenos podatkov; c) *ponudnike gostovanja*: dajejo v najem prostor na svojih strežnikih, kamor lahko uporabniki ali ponudniki vsebin nalagajo svoje vsebine. Uporabniki lahko nalagajo podatke na spletno storitev, kot je oglasna deska ali omrežje P2P.

([12]) Sporočilo Evropske komisije Svetu, Evropskemu parlamentu in Evropskemu ekonomsko-socialnemu odboru o krepitvi uveljavljanja pravic intelektualne lastnine na notranjem trgu, Bruselj, 11. september 2009, COM(2009) 467 konč.

z nadzorovanjem forumov in blogov, ali pa bi se pretvarjali, da si izmenjujejo datoteke na omrežjih za neposredno izmenjavo datotek, da bi opredelili izmenjevalce, ki si domnevno izmenjujejo avtorska dela ([13]).

22. Ko bi z zbiranjem naslovov internetnega protokola (naslovov IP) opredelili internetne uporabnike, domnevno vpletene v kršenje avtorskih pravic, bi imetniki avtorskih pravic naslove IP teh uporabnikov poslali zadevnemu(-im) ponudniku(-om) internetnih storitev, in ti bi uporabnike, ki jim naslov IP pripada, obvestili o njihovem morebitnem sodelovanju pri kršitvi avtorskih pravic. Ko bi ponudnik internetnih storitev naročniku internetne povezave izdal določeno število opominov, bi lahko samodejno prekinil ali začasno ustavil naročnikovo internetno povezavo ([14]).

*Veljavni pravni okvir EU za varstvo osebnih podatkov in zasebnosti*

23. Politika treh napak pred odklopom interneta mora biti v skladu z zahtevami, ki izhajajo iz pravice do zasebnosti, kot je določeno v členu 8 EKČP in členu 7 Listine o temeljnih pravicah, ter pravice do varstva podatkov, kot je določeno v členu 8 Listine o temeljnih pravicah in členu 16 PDEU ter kot je opredeljeno v Direktivi 95/46/ES in Direktivi 2002/58/ES.

24. ENVP meni, da spremljanje vedenja internetnih uporabnikov in nadaljnje zbiranje njihovih naslovov IP pomeni oviranje njihovih pravic do spoštovanja zasebnega življenja in dopisovanja; z drugimi besedami, to je oviranje njihove pravice do zasebnega življenja. To mnenje je v skladu s sodno prakso Evropskega sodišča za človekove pravice ([15]).

25. Direktiva 95/46/ES se uporablja ([16]), ker politika treh napak pred odklopom interneta vključuje obdelavo naslovov IP, ki se – v vsakem primeru v zadevnih okoliščinah – štejejo za osebne podatke. Naslovi IP so označevalniki, ki so videti kot niz števil, ločenih s pikami, na primer 122.41.123.45. Naročnina pri ponudniku dostopa do interneta naročniku omogoča dostop do interneta. Vsakokrat, ko se želi povezati na internet, dobi naslov IP prek naprave, ki jo uporablja za dostop do interneta (npr. računalnika) ([17]).

26. Če uporabnik opravlja neko dejavnost, na primer vsebine nalaga na internet, ga lahko tretje stranke opredelijo prek naslova IP, ki ga uporablja. Na primer uporabnik, ki ima naslov IP 122.41.123.45, je 1. januarja 2010 ob treh zjutraj na storitev P2P naložil vsebine, ki domnevno kršijo avtorske pravice. Ponudnik internetnih storitev bo nato lahko tak naslov IP povezal z imenom naročnika, ki mu je dodelil ta naslov, in tako določil njegovo istovetnost.

27. Če se upošteva opredelitev pojma osebni podatki, kot je določena v členu 2 Direktive 95/46/ES, „osebni podatek pomeni katero koli informacijo, ki se nanaša na določeno ali določljivo fizično osebo (posameznik, na katerega se nanašajo osebni podatki); določljiva oseba je tista, ki se lahko neposredno ali posredno identificira, predvsem s sklicevanjem na identifikacijsko številko“ ([18]), je mogoče sklepati le, da so naslovi IP in informacije o dejavnostih, povezane s temi naslovi, osebni podatki v vseh tukaj pomembnih primerih. Naslov IP se uporablja kot identifikacijska številka, ki omogoča ugotovitev imena naročnika, ki mu je bil naslov IP dodeljen. Informacije, zbrane o naročniku, ki ima tak naslov IP („naložil je nekatere vsebine na internetno stran ZS 1. januarja 2010 ob treh zjutraj“), *se nanašajo na, tj.* so brez dvoma o dejavnostih določljivega posameznika (imetnika naslova IP) in jih je zato treba upoštevati kot osebne podatke.

([13]) Tehnologija P2P je porazdeljena arhitektura programske opreme, ki omogoča posameznim računalnikom, da se povežejo in neposredno komunicirajo z drugimi računalniki.

([14]) Primeri drugih sankcij lahko vključujejo omejevanje funkcionalnosti internetne povezave z znižanjem njene hitrosti, zmanjšanjem obsega itd.

([15]) Glej zlasti sodbi ESČP z dne 26. junija 2006 v zadevi *Weber in Saravia proti Nemčiji* (dec.), št. 54934/00, točka 77, in z dne 1. julija 2008 v zadevi *Liberty in drugi proti Združenemu kraljestvu*, št. 58243/00.

([16]) Sodišče ima širok pristop k uporabi Direktive 95/46/ES, katere določbe je treba razlagati ob upoštevanju člena 8 EKČP. Sodišče je v sodbi z dne 20. maja 2003 v združenih zadevah *Rundfunk*, C-465/00, C-138/01 in C-139/01, ZOdl., str. I-4989, točka 68, odločilo, da „je treba določbe Direktive 95/46/ES, če se nanašajo na obdelavo osebnih podatkov, ki lahko privede do kršenja temeljnih svoboščin, zlasti pravice do zasebnosti, nujno razlagati glede na temeljne pravice, ki so v skladu z ustaljeno sodno prakso sestavni del splošnih načel prava, katerih spoštovanje zagotavlja Sodišče“.

([17]) Naslov IP, ki ga ponudnik dostopa do interneta dodeli posamezniku, je lahko ob vsakem njegovem iskanju po internetu isti (v nadaljnjem besedilu: statični naslov IP). Drugi naslovi IP so lahko dinamični, kar pomeni, da ponudnik dostopa do interneta svojim naročnikom vsakokrat, ko ti vzpostavijo povezavo z internetom, dodeli drugačen naslov IP. Ponudniki dostopa do interneta lahko tako povežejo naslov IP z naročnikovim računom, ki so mu dodelili (dinamični ali statični) naslov IP.

([18]) Uvodna izjava 26: „ker se morajo načela varstva uporabljati za vse informacije v zvezi z določeno ali določljivo osebo; ker bi bilo treba za odločitev o tem, ali je oseba določljiva ali ne, upoštevati vsa sredstva, za katera se pričakuje, da jih bo uporabil bodisi upravljavec ali katera koli druga oseba za določitev take osebe; ker se načela varstva ne uporabljajo za podatke, ki so spremenjeni v anonimne tako, da posameznik, na katerega se osebni podatki nanašajo, ni več določljiv; […]“

28. S temi pogledi se v celoti strinja delovna skupina iz člena 29, ki je v dokumentu o vprašanjih v zvezi z varstvom podatkov, povezanih s pravicami intelektualne lastnine, navedla, da so naslovi IP, zbrani za uveljavljanje pravic intelektualne lastnine, tj. za opredelitev internetnih uporabnikov, ki so domnevno kršili pravice intelektualne lastnine, osebni podatki, če se uporabljajo za uveljavljanje takih pravic zoper določenega posameznika ([19]).

29. Direktiva 2002/58/ES se prav tako uporablja, saj je posledica politike treh napak pred odklopom interneta zbiranje podatkov o prometu in komunikaciji. Direktiva 2002/58/ES upravlja uporabo takih podatkov ter določa načelo zaupnosti sporočil prek javnih komunikacijskih omrežjih in podatkov, ki so povezani s temi sporočili.

### IV.3 **Ali je politika treh napak pred odklopom interneta nujen ukrep**

30. V členu 8 EKČP je določeno načelo nujnosti, v skladu s katerim je vsak ukrep, ki krši pravico do zasebnosti posameznikov, dovoljen samo, če je nujen ukrep v demokratični družbi za zakonit cilj, za katerega si prizadeva ta družba ([20]). Načelo nujnosti je mogoče najti tudi v členih 7 in 13 Direktive 95/46/ES ter členu 15 Direktive 2002/58/ES ([21]). Načelo zahteva analizo sorazmernosti ukrepa, ki jo je treba oceniti na podlagi ravnovesja vključenih interesov, ki se postavi v okoliščine demokratične družbe kot celote ([22]). To pomeni tudi oceno ali obstajajo alternativni ukrepi, ki so manj intruzivni.

31. Čeprav ENVP priznava pomembnost uveljavljanja pravic intelektualne lastnine, vseeno meni, da je politika treh napak pred odklopom interneta, kot jo poznamo danes – ki vključuje nekatere splošne elemente – nesorazmeren ukrep in je zato ni mogoče šteti za nujen ukrep. ENVP je prepričan tudi, da obstajajo druge manj intruzivne rešitve ali da se predvidene politike lahko izvajajo manj intruzivno in v bolj omejenem obsegu. Politika treh napak pred odklopom interneta tudi na podrobnejši pravni ravni pomeni težave. Te ugotovitve bodo predstavljene v nadaljevanju.

*Politika treh napak je nesorazmerna*

32. ENVP želi poudariti daljnosežno naravo uvedenih ukrepov. V zvezi s tem je treba navesti naslednje elemente:

(i) dejstvo, da bi (neopaženo) spremljanje vplivalo na milijone posameznikov in *vse* uporabnike, ne glede na to, ali so osumljeni ali ne;

(ii) posledica spremljanja bi bilo sistematično evidentiranje podatkov, od katerih bi nekateri lahko povzročili, da bi lahko posameznike privedli na civilna ali celo kazenska sodišča; poleg tega bi se lahko nekatere tako zbrane informacije štele za občutljive podatke v skladu s členom 8 Direktive 95/46/ES, ki zahtevajo strožje zaščitne ukrepe;

(iii) spremljanje bo verjetno sprožilo veliko primerov napačnih prepoznav. Kršitev avtorskih pravic ni vprašanje, na katero se lahko odgovori preprosto z „da“ ali „ne“. Sodišča morajo pogosto proučiti ogromno tehničnih in pravnih podrobnosti, da lahko določijo, ali gre za kršitev ([23]);

([19]) Mnenje delovne skupine iz člena 29 z dne 18. januarja 2005 o vprašanjih podatkov, povezanih s pravicami intelektualne lastnine (DS 104). Ta delovna skupina je bila ustanovljena v skladu s členom 29 Direktive 95/46/ES. Je neodvisen evropski svetovalni organ na področju varstva podatkov in zasebnosti. Naloge skupine so opredeljene v členu 30 Direktive 95/46/ES in členu 15 Direktive 2002/58/ES. Glej tudi Mnenje 4/2007 delovne skupine z dne 20. junija 2007 o pojmu osebnih podatkov (DS 136), zlasti str. 16.

([20]) Člen 8 EKČP se izrecno sklicuje na zahtevo, da mora biti vsako poseganje ali omejitev „nujno v demokratični družbi“.

([21]) S členom 13 Direktive 95/46/ES se dovoljuje omejitev samo, kadar taka omejitev pomeni: „potrebni ukrep za zaščito: (a) državne varnosti; (b) obrambe; (c) javne varnosti; (d) preprečevanja, preiskovanja, odkrivanja in pregona kaznivih dejanj ali kršitve etike za zakonsko urejene poklice; (e) pomembnega gospodarskega ali finančnega interesa države članice ali Evropske unije, vključno z denarnimi, proračunskimi in davčnimi zadevami; (f) spremljanja, pregledovanja ali urejanja, povezanega, četudi občasno, z izvajanjem javne oblasti v primerih iz (c), (d) in (e); (g) posameznika, na katerega se nanašajo osebni podatki, ali pravic in svoboščin drugih.“ S členom 15 Direktive 2002/58/ES se zahteva, naj „kadar takšna omejitev pomeni potreben, primeren in ustrezen ukrep znotraj demokratične družbe za zaščito državne varnosti (to je Državne varnosti), obrambe, javne varnosti in preprečevanje, preiskovanje, odkrivanje in pregon kriminalnih dejanj ali nedovoljene uporabe elektronskega komunikacijskega sistema iz člena 13(1) Direktive 95/46/ES“.

([22]) Glej tudi sodbi ESČP z dne 2. avgusta 1984 v zadevi *Malone proti Združenemu kraljestvu*, serija A, št. 82, točka 81 in naslednje, ter z dne 4. decembra 2008 v zadevi *Marper proti Združenemu kraljestvu*, [GC], št. 30562/04 in 30566/04, točka 101 in naslednje.

([23]) Sodišča bodo morala oceniti, ali so vsebine res avtorsko zaščitene, katere pravice so bile kršene, ali se uporaba šteje za primer poštene uporabe, veljavno zakonodajo, odškodnine itd.

(iv) mogoči *učinki* spremljanja, ki lahko povzročijo odklop dostopa do interneta. To bi oviralo posameznikovo pravico do svobode izražanja, svobode do informacij in dostopa do kulture, storitev e-uprave, trga, e-pošte, v nekaterih primerih pa tudi do z delom povezanih dejavnosti. V tem okviru se je zlasti pomembno zavedati, da bo posledice čutil ne samo domnevni kršitelj, temveč tudi vsa njegova družina, ki uporablja isto internetno povezavo, vključno s šolarji, ki internet uporabljajo pri šolskih dejavnostih;

(v) dejstvo, da bo subjekt, ki bo pripravil oceno in sprejel odločitev, po navadi zasebni subjekt (tj. imetnik avtorskih pravic ali ponudnik internetnih storitev). ENVP je že v prejšnjem mnenju navedel pomisleke glede tega, da bi posameznike spremljal zasebni sektor (tj. ponudniki dostopa do interneta ali imetniki avtorskih pravic) na področjih, ki so načelno v okviru pristojnosti organov pregona ([24]).

33. ENVP ni prepričan, da prednosti takih ukrepov odtehtajo posledice za temeljne pravice posameznikov. Varstvo avtorskih pravic je v interesu imetnikov teh pravic in družbe. Vseeno pa se omejitev temeljnih pravic ne zdi upravičena, če se primerjajo teža oviranja, tj. obseg vdora v zasebnost, kakor je bilo opozorjeno z zgornjimi elementi, in pričakovane koristi odvračanja od kršitev pravic intelektualne lastnine, ki – večinoma – vključujejo le manjše kršitve pravic intelektualne lastnine. Kot je navedeno v sklepnih predlogih generalne pravobranilke Kokott v zadevi *Promusicae*: „Vendar pa ni gotovo, da zasebna izmenjava datotek, zlasti brez namena pridobivanja dobička, dovolj resno ogroža varstvo avtorskih pravic, tako da bi se lahko upravičila uporaba te izjeme. Sporno je namreč, v kolikšni meri zasebna izmenjava datotek povzroča dejansko škodo“ ([25]).

34. V tem smislu je vredno omeniti tudi odziv Evropskega parlamenta na „sheme treh napak“ v okviru ocene telekomunikacijskega svežnja, zlasti spremembe 138 k okvirni direktivi ([26]). V spremembi je bilo določeno, da so omejitve temeljnih pravic in svoboščin mogoče, samo če so te primerne, sorazmerne in nujne v okviru demokratične družbe, njihovo uveljavljanje pa je pogojeno s primernim procesnim jamstvom v skladu z EKČP in splošnimi načeli prava Skupnosti, vključno z učinkovitim sodnim varstvom in predpisanim postopkom ([27]).

35. ENVP glede na to še dodatno poudarja, da bo vsako omejevanje temeljnih pravic predmet temeljitega pregleda na ravni EU in nacionalni ravni. V tem smislu se lahko potegne vzporednica z Direktivo o hrambi podatkov 2006/24/ES ([28]), ki odstopa od splošnega načela varstva podatkov glede izbrisa podatkov, ko ti niso več potrebni za namen, za katerega so bili zbrani. S to direktivo se zahteva, naj se podatki o prometu hranijo za namen boja proti hudim kaznivim dejanjem. Treba je pripomniti, da je hramba dovoljena samo za „huda kazniva dejanja“, da je omejena na „podatke o prometu“, kar načelno izključuje informacije o vsebini sporočil, in da so navedena stroga jamstva. Kljub temu so se pojavili dvomi o njeni skladnosti s standardi temeljnih pravic; romunsko ustavno sodišče je odločilo, da splošna hramba ni v skladu s temeljnimi pravicami ([29]), zadeva pa poteka tudi pred nemškim ustavnim sodiščem ([30]).

*Obstoj drugih manj intruzivnih sredstev*

36. Zgornje ugotovitve so podkrepljene z dejstvom, da za doseganje istega namena obstajajo manj intruzivna sredstva. ENVP vztraja, da bi bilo treba take manj intruzivne modele proučiti in preizkusiti.

([24]) Mnenje ENVP z dne 23. junija 2008 o predlogu sklepa o oblikovanju večletnega programa Skupnosti za zaščito otrok, ki uporabljajo internet in druge komunikacijske tehnologije, UL C 2, 7.1.2009, str. 2.

([25]) Glej zadevo, navedeno v opombi 8, str. 106.

([26]) Glej Direktivo 2009/140/ES Evropskega parlamenta in Sveta z dne 25. novembra 2009, UL L 337, 18.12.2009, str. 37.

([27]) Končno besedilo tako imenovane spremembe 138 se glasi: „Ukrepi, ki jih države članice sprejmejo glede dostopa do in uporabe storitev in aplikacij prek elektronskih komunikacijskih omrežij s strani končnih uporabnikov, spoštujejo temeljne pravice in svoboščine fizičnih oseb, zagotovljene z Evropsko konvencijo o varstvu človekovih pravic in temeljnih svoboščin ter s splošnimi načeli prava Skupnosti. Kateri koli izmed teh ukrepov glede dostopa do ali uporabe do storitev in aplikacij prek elektronskih komunikacijskih omrežij s strani končnih uporabnikov, ki bi lahko omejile te temeljne pravice ali svoboščine, se lahko naložijo le, če so ustrezni, sorazmerni in potrebni v demokratični družbi, za njihovo izvajanje pa veljajo ustrezni postopkovni zaščitni ukrepi v skladu z Evropsko konvencijo o varstvu človekovih pravic in temeljnih svoboščin ter v skladu s splošnimi načeli prava Skupnosti, vključno z učinkovitim sodnim varstvom in predpisanim postopkom. Skladno s tem se ti ukrepi lahko sprejmejo le ob ustreznem spoštovanju načela domneve nedolžnosti in pravice do zasebnosti. Zagotovi se predhoden, pošten in nepristranski postopek, vključno s pravico do zaslišanja zadevne osebe ali zadevnih oseb, ob upoštevanju potrebe po ustreznih pogojih in postopkovnih ureditvah v ustrezno utemeljenih nujnih primerih skladno z Evropsko konvencijo o varstvu človekovih pravic in temeljnih svoboščin. Zagotovi se pravica do učinkovitega in pravočasnega sodnega nadzora.“

([28]) Direktiva 2006/24/ES Evropskega parlamenta in Sveta z dne 15. marca 2006, UL L 105, 13.4.2006, str. 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. ENVP v tem smislu opozarja, da spremenjena Direktiva 2002/22/ES o univerzalni storitvi in pravicah uporabnikov v zvezi z elektronskimi komunikacijskimi omrežji in storitvami (v nadaljnjem besedilu: Direktiva o pravicah državljanov), ki je del nedavno spremenjenega telekomunikacijskega svežnja, vsebuje nekatera pravila in postopke za omejevanje manjših kršitev avtorskih pravic pri uporabnikih ([31]). Taki postopki vključujejo obveznosti držav članic, da pripravljajo standardizirane informacije o različnih temah, ki so v javnem interesu, zlasti pa o kršitvah avtorskih in sorodnih pravic ter njihovih pravnih posledicah ([32]). Države članice lahko nato od ponudnikov internetnih storitev zahtevajo, naj jih razdelijo vsem strankam in vključijo v pogodbe.

38. Sistem je namenjen obveščanju in odvračanju posameznikov od razširjanja avtorsko zaščitenih informacij in udeležbe pri kršitvah, medtem ko se izogiba spremljanju uporabe interneta in skrbi zaradi varstva zasebnosti in osebnih podatkov. Direktiva o pravicah državljanov se mora začeti izvajati maja 2011, tako da taki postopki še niso vzpostavljeni. Tako še ni bilo priložnosti, da bi se preizkusile njihove prednosti. Zdi se še prezgodaj pregledati mogoče koristne rezultate teh novih postopkov in jih sprejeti namesto politike treh napak pred odklopom interneta, ki mnogo bolj omejuje temeljne pravice.

39. Poleg zgoraj navedenega je treba spomniti, da Direktiva 2004/48/ES z dne 28. aprila 2004 o uveljavljanju pravic intelektualne lastnine določa različna orodja za uveljavljanje pravic intelektualne lastnine pred sodišči (obravnavana v odstavku 43 in naslednjih) ([33]).

([31]) Glej Direktivo 2009/136/ES Evropskega parlamenta in Sveta z dne 25. novembra 2009, UL L 337, 18.12.2009, str. 11.

([32]) Zlasti člen 21(4) Direktive 2009/136/ES določa, da „[d]ržave članice lahko zahtevajo, da podjetja iz odstavka 3 brezplačno širijo informacije javnega interesa obstoječim in novim naročnikom, če je to primerno, prek enakih sredstev, kot jih ponavadi sama uporabljajo za komuniciranje z naročniki. V tem primeru takšne informacije zagotovijo zadevni javni organi v standardizirani obliki, med drugim pa zajemajo naslednje teme: (a) najobičajnejše oblike uporabe elektronskih komunikacijskih storitev za izvajanje nezakonitih dejavnosti ali za širjenje škodljive vsebine, zlasti kjer bi to lahko škodovalo spoštovanju pravic in svoboščin drugih, vključno s kršenjem avtorskih pravic in sorodnih pravic, ter njihove pravne posledice […]“ Nadalje, v skladu s členom 20(2) „[d]ržave članice lahko zahtevajo tudi, da mora pogodba vključevati vse informacije, ki jih v ta namen lahko dajejo zadevni javni organi o uporabi elektronskih komunikacijskih omrežij in storitev za izvajanje nezakonitih dejavnosti ali za razširjanje škodljive vsebine ter o načinih zaščite osebne varnosti, zasebnosti in osebnih podatkov iz člena 21(4) in ki se navezujejo na ponujeno storitev“.

([33]) UL L 157, 30.4.2004, str. 45 (v nadaljnjem besedilu: Direktiva IPRE).

40. Direktiva o uveljavljanju pravic intelektualne lastnine (Direktiva IPRE) je bila šele pred kratkim prenesena v pravo držav članic. Do zdaj ni bilo dovolj časa za oceno, ali so njene določbe ustrezne za namene uveljavljanja pravic intelektualne lastnine. Zato je vsaka potreba po nadomestitvi sedanjega še ne preizkušenega sistema na podlagi sodnih postopkov vsaj dvomljiva. Zgoraj navedeno postavlja neizogibno vprašanje, zakaj obstoječih kršitev ni mogoče ustrezno obravnavati z obstoječimi civilnimi in kazenskimi sankcijami, ki so predvidene za kršitve avtorskih pravic. Komisija bi morala zato pred predlaganjem takih ukrepov politike pripraviti zanesljive informacije, ki dokazujejo, da z obstoječim pravnim okvirom niso bili doseženi načrtovani učinki.

41. Ni jasno niti, ali so bili resno proučeni drugi gospodarski modeli, ki ne bi vključevali sistematičnega spremljanja posameznikov. Na primer, če bi imetniki avtorskih pravic dokazali izgubo zaradi uporabe P2P, bi lahko skupaj s ponudniki internetnih storitev na primer poskusili uvesti različne naročnine za dostop do interneta, kjer bi del zneska za naročnino z neomejenim dostopom dobili imetniki avtorskih pravic.

*Možnost izvajanja ciljno usmerjenega spremljanja na manj intruziven način*

42. Poleg uporabe popolnoma različnih modelov, ki jih je treba, kot je navedeno, proučiti in preizkusiti, bi se lahko ciljno usmerjeno spremljanje izvajalo vsekakor manj intruzivno.

43. Namen uveljavljanja pravic intelektualne lastnine je mogoče prav tako doseči s spremljanjem samo omejenega števila posameznikov, ki so osumljeni hudih kršitev avtorskih pravic. Direktiva IPRE v zvezi s tem določa nekatere smernice. Določa pogoje, pod katerimi lahko organi odredijo, naj se osebni podatki, ki jih imajo ponudniki dostopa do interneta, razkrijejo za namene uveljavljanja pravic intelektualne lastnine. Člen 8 določa, da lahko pristojni pravosodni organi ukažejo ponudnikom internetnih storitev, naj predložijo osebne podatke, ki jih imajo o domnevnih kršiteljih (npr. podatke o izvoru distribucijskih omrežij blaga ali storitev, ki kršijo pravico intelektualne lastnine), kot odgovor na utemeljeno in sorazmerno zahtevo v primerih kršitev v *trgovinsko pomembnem obsegu* ([34]).

44. Zato je „trgovinsko pomemben obseg“ odločilno merilo. V skladu z njim je lahko spremljanje sorazmeren ukrep v omejenih, posebnih in *ad hoc* primerih, v katerih obstajajo

([34]) To je dodatno potrjeno v uvodni izjavi 14 Direktive IPRE.

dobro utemeljeni sumi zlorabe avtorskih pravic v trgovinsko pomembnem obsegu. To merilo bi lahko obsegalo primere jasnih zlorab avtorskih pravic s strani posameznikov, ki so nameravali pridobiti neposredno ali posredno gospodarsko in trgovinsko korist.

45. Da bi bili v praksi zgoraj navedeni ukrepi učinkoviti, bi lahko imetniki avtorskih pravic izvajali ciljno usmerjeno spremljanje nekaterih naslovov IP, da bi preverili obseg kršitev avtorskih pravic. To bi pomenilo, da bi imetniki avtorskih pravic lahko sproti sledili poročilom o domnevnih kršitvah z istim namenom. Take informacije se lahko uporabijo le, ko se preveri pomembnost kršitve (na primer jasni primeri večjih in manjših, vendar stalnih kršitev v določenem obdobju zaradi gospodarskih koristi in finančnega dobička). Potreba po stalnosti v nekem časovnem obdobju je poudarjena in podrobneje razložena v nadaljevanju v razpravi o načelu ohranjanja.

46. To bi pomenilo, da se lahko v takih primerih zbiranje informacij za namene dokazovanja domnevne zlorabe interneta šteje za sorazmerno in nujno za pripravo pravnih postopkov, vključno s pravnimi spori.

47. ENVP meni, da bi morali nacionalni organi za varstvo podatkov kot dodatno jamstvo postopke obdelave podatkov, ki so namenjeni zbiranju takšnih dokazov, prej preveriti in odobriti. Ta mnenja temeljijo na dejstvu, da bi postopki obdelave podatkov pomenili določeno tveganje za pravice in svoboščine posameznikov glede na njihove namene, tj. izvajanje prisilnih ukrepov je lahko navsezadnje kaznivo dejanje ob upoštevanju občutljive narave zbranih podatkov. Dejstvo, da obdelava podatkov vključuje spremljanje elektronskih sporočil, je še dodaten dejavnik, ki poziva k okrepljenemu nadzoru.

48. ENVP meni, da je „trgovinsko pomemben obseg“, vključen v Direktivo IPRE, zelo ustrezen element, ki omejuje spremljanje, da se upošteva načelo sorazmernosti. Poleg tega ni videti, da bi bili na voljo zanesljivi dokazi, ki bi v skladu z merili, določenimi v Direktivi IPRE, pokazali, da učinkovito pravno ukrepanje zoper kršitve avtorskih pravic ni mogoče ali učinkovito. Na primer, zdi se, da poročila, kot je iz Nemčije, kažejo nasprotno, saj je bilo od leta 2008, po prenosu Direktive IPRE, izdanih približno 3 000 sodnih nalogov, skladno s katerimi so ponudniki internetnih storitev sodiščem razkrili podatke o približno 300 000 naročnikih.

49. Skratka, težko je razumeti, zakaj bi se zakonodajalci odmaknili od meril Direktive IPRE, ki velja šele dve leti, in se pomaknili proti bolj intruzivnim metodam, ko EU komaj začenja preizkušanje nedavno sprejetih metod. Iz istega razloga je prav tako težko razumeti potrebo po zamenjavi trenutnega sistema, temelječega na sodišču, z drugimi vrstami ukrepov (poleg drugih vprašanj glede predpisanega postopka, ki se tukaj ne obravnavajo).

### IV.4 **Skladnost politike treh napak pred odklopom interneta s podrobnejšimi določbami glede varstva podatkov**

50. Obstajajo tudi drugi natančnejši pravni razlogi, zakaj je pristop treh napak sporen z vidika osebnih podatkov. ENVP želi poudariti dvomljivo pravno podlago za obdelavo podatkov, ki se zahteva z Direktivo 95/46/ES, in obveznosti iz Direktive 2002/58/ES za opustitev datotek z zapisi o poteku izvajanja računalniškega programa (dnevnikov).

*Pravna podlaga za obdelavo*

51. Posledica sheme pristopa treh napak je obdelava osebnih podatkov, od katerih bodo nekateri uporabljeni v pravnih in upravnih postopkih za prekinitev dostopa do interneta večkratnim kršiteljem. S tega vidika so taki podatki opredeljeni kot občutljivi na podlagi člena 8 Direktive 95/46/ES. Člen 8(5) določa, da „[o]bdelava podatkov v zvezi s prekrški, kazenskimi obsodbami ali varnostnimi ukrepi se lahko izvaja samo pod nadzorom uradnega organa ali pa če nacionalna zakonodaja določi ustrezne posebne zaščitne ukrepe […]“

52. V tem smislu je primerno opozoriti na prej navedeni dokument delovne skupine iz člena 29, v katerem je obravnavano vprašanje obdelave pravosodnih podatkov ([35]). Delovna skupina trdi, da „medtem ko je jasno, da ima vsak posameznik pravico do obdelave pravosodnih podatkov v postopku pravdnega spora, v katerem je sam udeležen, pa načelo ne dopušča, da bi tretje stranke temeljito preiskovale, zbirale ali na enem mestu združevale osebne podatke, zlasti in vključno s splošnim sistematičnim raziskovanjem, na primer s pregledovanjem interneta […] Taka preiskava spada v pristojnost pravosodnih organov ([36])." Medtem ko je zbiranje ciljno opredeljenih in posebnih dokazov, zlasti v primerih resnih kršitev, lahko nujno za vzpostavitev in uveljavljanje pravnega zahtevka, se ENVP v celoti strinja z mnenjem delovne skupine iz člena 29 glede nezakonitosti obsežnih preiskav, ki vključujejo obdelavo ogromne količine podatkov o uporabnikih interneta.

53. Zgoraj opisana razprava o načelu sorazmernosti in merilo o „trgovinsko pomembnem obsegu“ sta pomembna pri odločanju, v kakšnih okoliščinah bo zbiranje naslovov IP in sorodnih informacij zakonito.

([35]) Glej odstavek 28 tega mnenja.
([36]) Dodan poudarek.

54. Ponudniki internetnih storitev bi lahko poskusili obdelavo, ki bi jo izvajali imetniki avtorskih pravic, napraviti za zakonito z vnašanjem klavzul v pogodbe svojih strank, ki bi jim omogočale spremljanje podatkov uporabnikov in prekinitev naročnine. Ko bi stranke sklenile take pogodbe, bi se štelo, da soglašajo s spremljanjem. Vseeno pa taka praksa najprej postavlja temeljno vprašanje, ali posamezniki lahko dajo soglasje ponudnikom internetnih storitev za obdelavo podatkov, ki pa je ne bodo izvajali ti ponudniki, temveč jo bodo izvajale tretje stranke, ki niso pod „nadzorom“ ponudnikov internetnih storitev.

55. Drugič, postavlja se vprašanje veljavnosti soglasja. Člen 2(h) Direktive 95/46/ES opredeljuje soglasje kot „vsako prostovoljno dano posebno in informirano izjavo volje, s katero posameznik, na katerega se osebni podatki nanašajo, izrazi soglasje, da se osebni podatki o njem obdelujejo“. Pomembno pri tem je, da mora biti soglasje ne glede na okoliščine, v katerih je dano, prostovoljen, določen in utemeljen znak volje posameznika, na katerega se osebni podatki nanašajo, kot je določeno v členu 2(h) Direktive, če naj bi bilo soglasje veljavno. ENVP močno dvomi, da bodo posamezniki, ki bodo vprašani glede soglasja k spremljanju njihovih internetnih dejavnosti, imeli možnost resnične izbire – zlasti ker bo druga možnost ostati brez interneta, kar bi lahko ogrozilo veliko drugih področij njihovega življenja.

56. Tretjič, zelo vprašljivo je, ali lahko tako spremljanje sploh kdaj šteje za *nujno* za izvajanje pogodbe, pri kateri je pogodbena stranka posameznik, na katerega se nanašajo osebni podatki, kakor določa člen 7(b) Direktive 95/46/ES, saj spremljanje očitno ni predmet pogodbe, sklenjene s posameznikom, na katerega se nanašajo osebni podatki, ampak samo sredstvo, s katerim ponudniki internetnih storitev zadovoljujejo druge interese.

*Izključitev dnevnikov*

57. V skladu z Direktivo 2002/58/ES in zlasti členom 6 se lahko podatki o prometu, kot so naslovi IP, zbirajo in hranijo samo iz razlogov, ki so neposredno povezani s komuniciranjem samim, vključno z zaračunavanjem storitev, vodenjem prometa in nameni preprečevanja goljufij. Potem je treba podatke izbrisati. To ne vpliva na obveznosti, ki izhajajo iz Direktive o hrambi podatkov, s katero se, kakor je bilo obravnavano, zahtevata hramba podatkov o prometu ter njihova izročitev policiji in tožilstvu za pomoč pri preiskavi **samo hudih kaznivih dejanj** ([37]).

([37]) Glej odstavek 35 tega mnenja.

58. V skladu z zgornjim bi ponudniki internetnih storitev morali izločiti vsak dnevnik, ki razkriva dejavnosti uporabnikov interneta in ni več potreben za zgornje namene. Ob upoštevanju, da dnevniki niso nujni za namene zaračunavanja storitev, se zdi, da bi morali ponudnikom internetnih storitev za vodenje prometa zadostovati trije ali štirje tedni ([38]).

59. To pomeni, ko imetniki avtorskih pravic stopijo v stik s ponudniki internetnih storitev, ti ne bi smeli imeti dnevnikov, ki bi povezovali naslove IP z ustreznimi naročniki, če se tak stik ne zgodi v zgoraj navedenem obdobju. Ohranjanje dnevnikov po navedenem obdobju bi bilo mogoče samo iz upravičenih razlogov v okviru obsega namenov, ki jih določa pravo.

60. S praktičnega vidika to pomeni, da zahteve imetnikov avtorskih pravic, naslovljene na ponudnike internetnih storitev, ne bodo mogle biti izpolnjene, razen če ne bodo izvedene zelo hitro, saj ponudniki internetnih storitev teh podatkov ne bodo več imeli. To samo po sebi omejuje to, kar se šteje za sprejemljive prakse spremljanja, ki so opisane zgoraj.

*Tveganja učinkov prelivanja*

61. ENVP je poleg tega zaskrbljen ne samo zaradi učinkov, ki jih ima lahko politika treh napak pred odklopom interneta na varstvo zasebnosti in podatkov, temveč tudi zaradi njihovih učinkov prelivanja. Če bo politika treh napak pred odklopom interneta dovoljena, lahko kaj hitro privede do uzakonitve še hujših oblik nadzora nad dejavnostmi uporabnikov interneta na različnih področjih in za različne namene.

62. ENVP poziva Komisijo, naj zagotovi, da s sporazumom ACTA ne bo presežena sedanja ureditev EU za uveljavljanje pravic intelektualne lastnine, ki spoštuje temeljne pravice in svoboščine ter državljanske svoboščine, kakršno je varstvo osebnih podatkov, ali da ne bo v nasprotju s tem sistemom.

## V. **POMISLEKI GLEDE VARSTVA PODATKOV V ZVEZI Z MEHANIZMI MEDNARODNEGA SODELOVANJA**

63. Eden od načinov, ki so ga sodelujoči pri sporazumu ACTA predlagali pri reševanju vprašanja uveljavljanja pravic intelektualne lastnine, je okrepiti mednarodno sodelovanje z

([38]) Vodenje prometa vključuje analizo prometa računalniškega omrežja zaradi izboljšanja ali jamstva izvedbe, krajšega obdobja mirovanja in/ali povečane uporabne pasovne širine.

več ukrepi, ki bi omogočili učinkovito uveljavljanje pravic intelektualne lastnine v pristojnosti podpisnikov sporazuma ACTA.

64. Glede na razpoložljive informacije je mogoče predvidevati, da bo več načrtovanih ukrepov za zagotavljanje uveljavljanja pravic intelektualne lastnine vključevalo mednarodno izmenjavo informacij o domnevnih kršitvah pravic intelektualne lastnine med javnimi organi (kot so carina, policija in pravosodje), pa tudi med javnimi in zasebnimi akterji (kot so ponudniki internetnih storitev in organizacije imetnice avtorskih pravic). Tak prenos podatkov vzbuja veliko vprašanj z vidika varstva podatkov.

### V.1 **Ali je predvidena izmenjava podatkov v okviru sporazuma ACTA zakonita, nujna in sorazmerna?**

65. Glede na trenutno stanje pogajalskega procesa, v katerem številni dejanski elementi obdelave podatkov ostajajo neopredeljeni ali neznani, je nemogoče preveriti, ali je predlagani okvir ukrepov v skladu s temeljnimi načeli varstva podatkov in zakonodajo EU o varstvu podatkov.

66. Najprej je mogoče vprašati, ali je prenos podatkov tretjim državam na podlagi sporazuma ACTA zakonit. O pomenu sprejemanja ukrepov na mednarodni ravni na zadevnem področju je mogoče dvomiti, dokler ni sklenjen sporazum med državami članicami EU glede uskladitve izvršilnih ukrepov v digitalnem okolju in vrste izvajanih kazenskih sankcij ([39]).

67. Glede na zgornje se zdi, da bi bilo načeli nujnosti in sorazmernosti prenosa podatkov v skladu s sporazumom ACTA lažje izpolniti, če bi bil sporazum izrecno omejen na boj proti najhujšim kršitvam pravic intelektualne lastnine, namesto da omogoča številne prenose podatkov v zvezi z vsakim sumom kršitev pravic intelektualne lastnine. To bo zahtevalo natančno opredelitev obsega tistega, kar so „najhujše kršitve pravic intelektualne lastnine“, za katere se podatki lahko prenesejo.

68. Poleg tega bi bilo treba posebno pozornost nameniti osebam, ki sodelujejo pri izmenjavi podatkov, in vprašanju, ali si bodo podatke izmenjavali samo javni organi med seboj ali pa bodo v izmenjavo vključeni tudi zasebni akterji. Kot je bilo že prej navedeno v tem mnenju, vzbuja sodelovanje zasebnih akterjev na področju, ki je načelno v pristojnosti organov pregona, veliko skrbi ([40]). Pogoji, pod katerimi bodo zasebni akterji vključeni v zbiranje in izmenjavo osebnih podatkov v zvezi s kršitvami pravic intelektualne lastnine z javnimi organi, morajo biti strogo omejeni na posebne okoliščine in vsebovati ustrezna jamstva.

### V.2 **Veljavna zakonodaja o varstvu podatkov, s katero se urejajo prenosi podatkov na podlagi sporazuma ACTA**

*Splošna ureditev prenosa podatkov*

69. Splošni okvir varstva podatkov, veljaven v EU, je določen z Direktivo 95/46/ES. Člena 25 in 26 Direktive 95/46/ES določata veljavno ureditev za prenos podatkov tretjim državam. S členom 25 se zahteva, naj se prenosi izvajajo samo v države, ki zagotavljajo zadostno raven varstva, drugače so taki prenosi načelno prepovedani.

70. Raven ustreznosti, ki jo premorejo tretje države, za vsak primer posebej oceni Evropska komisija, ki je po temeljiti analizi delovne skupine iz člena 29 številnim državam izdala več odločb o priznanju ustreznosti ([41]).

71. ENVP ugotavlja, da večine držav, sodelujočih pri sporazumu ACTA, ni na seznamu držav, ki zagotavljajo ustrezno varstvo podatkov, kot ga je sestavila Komisija: razen za Švico in – v posebnih okoliščinah – Kanado in ZDA ni za nikogar od preostalih sodelujočih pri sporazumu ACTA priznano, da zagotavlja ustrezno raven varstva. To pomeni, da mora biti za prenos podatkov iz EU v te države izpolnjen eden od pogojev iz člena 26(1) Direktive 95/46/ES ali pa morajo tretje stranke pri prenosu podatkov predložiti ustrezne zaščitne ukrepe v skladu s členom 26(2) Direktive.

*Posebna ureditev za prenos podatkov na področju kazenskega pregona*

72. Medtem ko je Direktiva 95/46/ES glavni instrument za varstvo podatkov v EU, je njeno področje uporabe trenutno omejeno, saj izrecno izključuje dejavnosti, ki med drugim zadevajo delovanje države na področju kazenskega prava (člen 3). Izmenjava podatkov za namene kazenskega pregona tako ne bo spadala na področje uporabe Direktive 95/46/ES in bo odvisna od splošnih načel varstva podatkov, ki so določena v Konvenciji Sveta Evrope št. 108 in

([39]) O predlogu kazenskih sankcij se trenutno razpravlja v okviru Sveta, COM(2006) 168 konč. z dne 26. aprila 2006.

([40]) Glej odstavka 32 in 52 tega mnenja. Glej tudi mnenje ENVP z dne 11. novembra 2008 o končnem poročilu Kontaktne skupine na visoki ravni EU-ZDA za izmenjavo informacij ter varstvo zasebnosti in osebnih podatkov, UL C 128, 6.6.2009, str. 1.

([41]) Glej odločbe o ustreznosti, ki jih je Evropska komisija dodelila Argentini, Kanadi, Švici, Varnemu pristanu ZDA in organom ZDA v okviru PNR, Guernseyju, otoku Man, Jerseyju; na voljo na http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm

njenem protokolu, katerega pogodbenice so vse države članice EU ([42]). Prav tako se bodo uporabljala pravila, ki jih je EU sprejela glede policijskega in pravosodnega sodelovanja na področju kazenskih zadev ter ki so določena z Okvirnim sklepom Sveta 2008/877/PNZ ([43]).

73. Ti instrumenti postavljajo kot načelo tudi obstoj ustrezne ravni varstva podatkov v tretjih državah, kamor naj bi se podatki prenesli. Določena so številna odstopanja, zlasti ko tretje države zagotovijo ustrezne zaščitne ukrepe. Podobno kot pri izmenjavi podatkov v skladu z Direktivo 95/46/ES se tudi pri izmenjavi podatkov na področju kazenskega pregona zahteva, da stranke pri prenosu podatkov navedejo ustrezne zaščitne ukrepe, da se tak prenos lahko izvede.

*Proti novi ureditvi za prenos podatkov*

74. V bližnji prihodnosti se lahko pričakuje, da bo EU na podlagi člena 16 PDEU sprejela nova skupna pravila za varstvo podatkov, ki se bodo uporabljala na vseh področjih dejavnosti EU. To pomeni, da bi bil lahko v nekaj letih pripravljen celovit okvir EU za varstvo podatkov, ki bi določal skladna pravila za varstvo podatkov na vseh področjih dejavnosti EU, kar bi vodilo do enake ravni zaščitnih ukrepov in jamstev za vse dejavnosti obdelave podatkov. Kot je poudarila Viviane Reding ([44]), komisarka za pravosodje, temeljne pravice in državljanstvo, bi moral ta novi okvir delovati kot enoten „sodoben in celovit pravni instrument“ za varstvo podatkov v EU. Tak okvir je še posebno dobrodošel, saj bi prinesel več jasnosti in doslednosti glede pravil, ki se v EU uporabljajo v zvezi z varstvom podatkov.

75. ENVP v mednarodnem okviru opozarja tudi na Resolucijo o mednarodnih standardih za varstvo osebnih podatkov in zasebnosti, ki so jo pred kratkim sprejeli organi za varstvo podatkov in ki je prvi korak k vzpostavitvi globalnih standardov za varstvo podatkov ([45]). Mednarodni standardi vključujejo številne podobne zaščitne ukrepe za varstvo podatkov, kot jih vključujeta Direktiva 95/46/ES in Konvencija št. 108. Čeprav mednarodni standardi še niso zavezujoči, zagotavljajo uporabne napotke glede načel varstva podatkov, ki jih lahko tretje države prostovoljno uporabljajo, tako da je njihov pravni okvir združljiv s standardi EU. ENVP verjame, da bi morali podpisniki sporazuma ACTA pri obdelavi osebnih podatkov iz EU upoštevati tudi načela, določena v mednarodnih standardih.

### V.3 **Potreba po izvajanju ustreznih zaščitnih ukrepov za varovanje prenosa podatkov iz EU v tretje države**

*Kakšno obliko naj imajo zaščitni ukrepi, da bi učinkovito varovali prenos podatkov v tretje države?*

76. Če se dokaže nujnost prenosa osebnih podatkov v tretje države, ENVP poudarja, da se mora Evropska unija pogajati s prejemniki iz tretje države – poleg samega sporazuma ACTA – o posebnih instrumentih, ki vsebujejo ustrezna jamstva za varstvo podatkov, da se ureja izmenjava osebnih podatkov.

77. Ustrezne zaščitne ukrepe za varstvo podatkov je treba običajno določiti z zavezujočim sporazumom med EU in prejemnikom iz tretje države, s katerim se stranka prejemnica zaveže, da bo spoštovala zakonodajo EU o varstvu podatkov ter posameznikom zagotovila enake pravice in pravna sredstva, kot so zagotovljeni v skladu s pravom EU. Potreba po zavezujočem sporazumu izhaja iz člena 26(2) Direktive 95/46/ES in člena 13(3)(b) Okvirnega sklepa ter je nadalje podprta z obstoječo prakso EU o sklepanju posebnih sporazumov, da se omogoči poseben prenos podatkov v tretje države ([46]).

78. Podobno se od prejemnika na podlagi osnutka mednarodnih standardov lahko zahteva, naj zagotovi, da bo omogočil zahtevano raven varstva za izvedbo prenosa. Ta jamstva bi lahko dobila tudi obliko pogodbene obveznosti.

*Vsebina zaščitnih ukrepov, ki jih podpisniki sporazuma ACTA navedejo v zvezi s prenosi osebnih podatkov*

79. ENVP še posebej poudarja, da so mednarodne izmenjave informacij za namene izvrševanja zakonodaje še posebno občutljive z vidika varstva podatkov, saj bi s takim okvirom lahko uzakonili ogromne prenose podatkov na področju,

([42]) Konvencija Sveta Evrope o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov, ki je bila sestavljena 28. januarja 1981 v Strasbourgu, ter dodatni protokol h Konvenciji o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov v zvezi z nadzornimi organi in čezmejnim prenosom podatkov, ki je bil podpisan 8. novembra 2001.

([43]) Okvirni sklep Sveta 2008/977/PNZ z dne 27. novembra 2008 o varstvu osebnih podatkov, ki se obdelujejo v okviru policijskega in pravosodnega sodelovanja v kazenskih zadevah, UL L 350, 30.12.2008, str. 60.

([44]) Glej odgovore na vprašalnik Evropskega parlamenta za kandidatko za komisarja Viviane Reding, str. 5, http://www.europarl.europa.eu/hearings/static/commissioners/answers/reding_replies_en.pdf

([45]) Resolucija, ki je bila sprejeta v Madridu novembra 2009.

([46]) Na primer sporazumi Europola in Eurojusta z ZDA, sporazum PNR, sporazum Swift, sporazum med Evropsko unijo in Avstralijo o obdelavi in posredovanju podatkov iz evidence podatkov o potnikih (PNR) Evropske unije s strani letalskih prevoznikov avstralski carinski službi.

na katerem bi bil vpliv na posameznike še posebno resen in na katerem so vse večje potrebe po strogih in zanesljivih zaščitnih ukrepih.

80. ENVP poudarja, da se posebni pogoji in zaščitni ukrepi lahko opredelijo samo za vsak primer posebej glede na vse parametre izmenjave podatkov. Za namen napotkov pa bi rad v nadaljevanju poudaril nekatera načela in zaščitne ukrepe, ki jih morajo navesti tretje osebe prejemnice, da se prenos podatkov lahko izvede.

— Preveriti je treba, kakšna je pravna utemeljitev, na podlagi katere potekajo dejavnosti obdelave podatkov (tj. ali postopki obdelave temeljijo na pravni obveznosti, soglasju posameznika, na katerega se osebni podatki nanašajo, ali kateri koli drugi veljavni utemeljitvi), in ali se s prenosi podatkov spoštuje prvotni namen zbiranja podatkov. Prenosa zunaj področja uporabe opredeljenega namena ne sme biti;

— jasno je treba opredeliti količino in vrste osebnih podatkov, ki se bodo izmenjali, ter jih zmanjšati na obseg, ki je nujno potreben za to, da se doseže namen prenosa. Zbrani in preneseni osebni podatki lahko vključujejo predvsem naslove IP uporabnikov interneta, datum in čas suma kršitve ter vrsto kršitve. ENVP priporoča, naj se podatki med preiskavo ne povezujejo z nobenim konkretnim posameznikom, in opozarja, da se lahko osumljenec identificira le v skladu z zakonom in pod nadzorom sodnika. ENVP v zvezi s tem poudarja, da so podatki v zvezi s kršitvami pravic intelektualne lastnine in sumov kršitev posebna kategorija podatkov, katerih obdelava je po navadi omejena na organe kazenskega pregona in zahteva dodatne zaščitne ukrepe. Osebe, ki so pooblaščene za obdelavo podatkov v zvezi s kršitvami pravic intelektualne lastnine in sumi kršitve, ter pogoji za obdelavo teh podatkov morajo biti zato posebej opredeljeni v skladu z veljavno zakonodajo o varstvu podatkov;

— osebe, ki si lahko izmenjujejo podatke, morajo biti jasno določene, nadaljnji prenosi drugim prejemnikom pa morajo biti načelno prepovedani, če niso nujni za določeno preiskavo. Ta omejitev je še posebno pomembna zato, ker imenovani prejemniki ne smejo neupravičeno deliti informacij z nepooblaščenimi prejemniki;

— ENVP domneva, da v sporazumu ACTA ne bo predvideno samo sodelovanje med javnimi organi, ampak da bodo z njim tudi naloge izvrševanja podeljene zasebnim organizacijam (kot so ponudniki internetnih storitev, organizacije imetnice avtorskih pravic itd.). V zadnjem primeru je treba pogoje in raven vključenosti zasebnih organizacij pri uveljavljanju pravic intelektualne lastnine natančno oceniti, da ukrepi sporazuma ACTA ponudnikom internetnih storitev in organizacijam imetnikov avtorskih pravic ne bi dali dejanske pravice, da spremljajo vedenje uporabnikov na spletu. Poleg tega bi morala obdelava osebnih podatkov s strani zasebnih organizacij v okviru izvrševanja zakonodaje potekati na podlagi ustrezne pravne podlage. Prav tako je pomembno pojasniti, ali bodo zasebne organizacije morale sodelovati s policijo, in opredeliti obseg takega sodelovanja. Vsekakor bi to moralo biti omejeno samo na „huda kazniva dejanja“, katerih opredelitev bo morala biti tudi natančno določena, saj vse kršitve pravic intelektualne lastnine ne morejo biti opredeljene kot huda kazniva dejanja;

— način izmenjave osebnih podatkov mora biti jasno izbran, še zlasti je treba navesti, ali bo šlo za sistem „push“ – tj. ponudniki internetnih storitev in organizacije imetnikov pravic bi številne podatke, ki jih imajo pod svojim nadzorom, prenesle tretjim osebam, kot so policija in organi kazenskega pregona v tujini – ali za sistem „pull“ – tj. policija in organi kazenskega pregona bi imeli neposreden dostop do baze podatkov zasebnih strank ali baz podatkov, v katerih so zbrane informacije. Kot je bilo že očrtano v okviru PNR, je sistem „push“ edina možnost, ki je skladna z načeli varstva podatkov z evropskega vidika varstva podatkov, saj daje pošiljatelju iz EU, ki je zelo verjetno tudi upravljavec podatkov, pravico, da izvaja nadzor nad prenosom podatkov ([47]);

— določiti je treba obdobje, v katerem bodo prejemniki lahko hranili osebne podatke, in namen, ki upravičuje nujnost take hrambe. Tako obdobje hrambe mora biti sorazmerno glede na namen, ki naj bi bil dosežen, kar pomeni, da je treba podatke odstraniti ali izbrisati, ko niso več potrebni za doseganje navedenega namena;

— obveznosti, naložene upravljavcem podatkov v tretjih državah, morajo biti jasno določene; nadzorni mehanizmi in/ali izvršljivi mehanizmi odgovornosti morajo biti zagotovljeni, tako da obstajajo učinkoviti viri in sankcije zoper upravljavce podatkov v primeru neupravičene obdelave ali drugih pomembnih dogodkov; poleg tega bi bilo treba vzpostaviti pravna sredstva, tako da bi

([47]) Glej Mnenje 4/2003 o ravni varstva, zagotovljeni v Združenih državah za prenos podatkov o potnikih, DS 78, sprejeto 13. junija 2003.

lahko posamezniki vložili pritožbo na neodvisni organ za varstvo podatkov in iskali učinkovito pravno sredstvo pred neodvisnim in nepristranskim sodiščem ([48]);

— v instrumentu, ki ga sklenejo stranke, morajo biti jasno opredeljene pravice posameznika, na katerega se nanašajo osebni podatki, v zvezi z obdelavo takih podatkov s strani tretje osebe prejemnice, navedeno pa mora biti tudi, da imajo učinkovito sredstvo za uveljavljanje svojih pravic v zvezi z obdelavo, ki se izvaja v tujini;

— ključnega pomena je tudi preglednost, in stranke instrumenta za varstvo podatkov se morajo dogovoriti, kako bodo obveščale posameznike, na katere se nanašajo osebni podatki, o poteku obdelave podatkov, njihovih pravicah in načinu njihovega uveljavljanja.

## VI. **SKLEPNE UGOTOVITVE**

81. ENVP zato resno poziva Evropsko komisijo, naj začne javen in pregleden dialog o sporazumu ACTA, morda z javnim posvetovanjem, ki bi pomagal zagotoviti, da bodo sprejeti ukrepi v skladu z zahtevami zakonodaje EU o varstvu zasebnosti in podatkov.

82. V okviru pogajanj, ki potekajo o sporazumu ACTA, ENVP poziva Evropsko komisijo, naj poišče pravo ravnovesje med zahtevami za varovanje pravic intelektualne lastnine ter pravico do varstva zasebnosti in podatkov. ENVP poudarja, da je bistveno zlasti, da se varstvo zasebnosti in podatkov upošteva od samega začetka pogajanj, preden je dogovorjeno o kakršnem koli ukrepu, tako da pozneje ne bo treba iskati drugih rešitev v skladu z načeli zasebnosti.

83. Medtem ko je intelektualna lastnina pomembna za družbo in jo je treba varovati, se ne sme postaviti nad temeljne pravice posameznika do zasebnosti, varstva podatkov in druge pravice, kot so domneva nedolžnosti, učinkovito sodno varstvo in svoboda izražanja.

84. Če sedanji osnutek sporazuma ACTA vključuje ali si vsaj posredno prizadeva za politiko treh napak pred odklopom interneta, bi sporazum ACTA močno omejil temeljne pravice in svoboščine evropskih državljanov, zlasti glede varstva osebnih podatkov in zasebnosti.

85. ENVP meni, da politika treh napak pred odklopom interneta ni nujna, da se doseže namen uveljavljanja pravic intelektualne lastnine. Prepričan je, da obstajajo druge manj intruzivne rešitve ali da je vsaj predvidene politike mogoče izvajati manj intruzivno ali v omejenem obsegu, predvsem s ciljno usmerjenim *ad hoc* spremljanjem.

86. Politika treh napak pred odklopom interneta je problematična tudi na podrobnejši pravni ravni, zlasti ker mora obdelava pravosodnih podatkov, predvsem s strani zasebnih organizacij, temeljiti na ustrezni pravni podlagi. Delovanje shem treh napak ima lahko za posledico dodatno dolgoročnejše shranjevanje dnevnikov, kar bi bilo v nasprotju z veljavno zakonodajo.

87. Če sporazum ACTA vključuje izmenjavo osebnih podatkov med organi in/ali zasebnimi organizacijami znotraj držav podpisnic, ENVP poleg tega poziva Evropsko unijo, naj izvaja ustrezne zaščitne ukrepe. Ti zaščitni ukrepi morajo veljati za vse prenose podatkov na podlagi sporazuma ACTA – za podatke na področju pregona civilnega, kazenskega ali digitalnega kriminala – in morajo biti v skladu z načeli varstva podatkov, ki so določeni Konvenciji št. 108 in Direktivi 95/46/ES. ENVP priporoča, naj bodo taki zaščitni ukrepi v obliki zavezujočih sporazumov med pošiljatelji iz EU in prejemniki iz tretje države.

88. ENVP si želi tudi, da bi se v nadaljevanju z njim posvetovali o ukrepih, ki se bodo izvajali v zvezi s prenosom podatkov, ki bo potekal na podlagi sporazuma ACTA, da bo lahko preveril njihovo sorazmernost, in da bi ti ukrepi zagotavljali ustrezno raven varstva podatkov.

V Bruslju, 22. februarja 2010

Peter HUSTINX

*Evropski nadzornik za varstvo podatkov*

([48]) Glej Mnenje Evropskega nadzornika za varstvo podatkov o končnem poročilu Kontaktne skupine na visoki ravni EU-ZDA za izmenjavo informacij ter varstvo zasebnosti in osebnih podatkov, 11.11.2008.