I

(Rezolūcijas, ieteikumi un atzinumi)

ATZINUMI

EIROPAS DATU AIZSARDZĪBAS UZRAUDZĪTĀJS

Eiropas Datu aizsardzības uzraudzītāja atzinums par notiekošajām Eiropas Savienības sarunām saistībā ar Nolīgumu par viltotu preču tirdzniecības apkarošanu *(ACTA)*

(2010/C 147/01)

EIROPAS DATU AIZSARDZĪBAS UZRAUDZĪTĀJS,

ņemot vērā Līgumu par Eiropas Savienības darbību un jo īpaši tā 16. pantu,

ņemot vērā Eiropas Savienības Pamattiesību hartu un jo īpaši tās 8. pantu,

ņemot vērā Eiropas Parlamenta un Padomes 1995. gada 24. oktobra Direktīvu 95/46/EK par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti [1],

ņemot vērā Eiropas Parlamenta un Padomes Direktīvu 2002/58/EK (2002. gada 12. jūlijs) par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē [2],

ņemot vērā Eiropas Parlamenta un Padomes Regulu (EK) Nr. 45/2001 (2000. gada 18. decembris) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Kopienas iestādēs un struktūrās un par šādu datu brīvu apriti [3] un jo īpaši tās 41. pantu,

IR PIEŅĒMIS ŠO ATZINUMU.

I. IEVADS

1. Eiropas Savienība piedalās sarunās attiecībā uz Nolīguma par viltotu preču tirdzniecības apkarošanu *(ACTA)* projektu. Šīs sarunas 2007. gadā uzsāka sākotnējā ieinteresēto pušu grupa un pēc tam turpināja plašāka dalībnieku grupa; patlaban sarunas notiek starp Austrāliju, Kanādu, Eiropas Savienību, Japānu, Koreju, Meksiku, Maroku, Jaunzēlandi, Singapūru, Šveici un Amerikas Savienotajām Valstīm. Padome piešķīra Eiropas Komisijai mandātu pievienoties šīm sarunām 2008. gadā.

2. EDAU atzīst, ka starptautiskā tirdzniecība ar viltotām un pirātiskām precēm rada arvien lielākas bažas un tā nereti ir saistīta ar organizētās noziedzības grupējumiem, tādēļ šā noziedzības veida apkarošanai ir nepieciešams izveidot atbilstošus starptautiskās sadarbības mehānismus.

3. EDAU norāda, ka Eiropas Savienības sarunas par daudzpusējiem nolīgumiem, kuru pamata mērķis ir intelektuālā īpašuma tiesību īstenošana, rada nozīmīgus jautājumus attiecībā uz viltošanas un pirātisma apkarošanas nolūkā veikto pasākumu ietekmi uz personu pamattiesībām un jo īpaši viņu tiesībām uz privātumu un datu aizsardzību.

4. Šajā saistībā EDAU jo īpaši nožēlo, ka Eiropas Komisija nav ar viņu konsultējusies par šāda nolīguma saturu. Tādēļ EDAU, rīkojoties pēc savas iniciatīvas, ir pieņēmis šo atzinumu, pamatojoties uz Regulas (EK) Nr. 45/2001 41. panta 2. punktu, ar mērķi sniegt Komisijai vadlīnijas par saistītajiem privātuma un datu aizsardzības aspektiem, kurus vajadzētu ņemt vērā *ACTA* sarunās.

II. PAŠREIZĒJĀ SITUĀCIJA UN PAREDZEMAIS *ACTA* SATURS

5. Septītā sarunu kārta notika 2010. gada 26.–29. janvārī Mehiko nolūkā noslēgt nolīgumu 2010. gada laikā. Tomēr līdz pat šim brīdim nav pieejams neviens oficiāls nolīguma projekts.

[1] OV L 281, 23.11.1995., 31. lpp.
[2] OV L 201, 31.7.2002., 37. lpp.
[3] OV L 8, 12.1.2001., 1. lpp.

6. Sarunu mērķis ir pieņemt jaunu daudzpusēju nolīgumu, lai stiprinātu intelektuālā īpašuma tiesību īstenošanu, kā arī apkarotu viltošanu un pirātismu. Pieņemšanas gadījumā šis jaunais nolīgums izveidos uzlabotus starptautiskus standartus attiecībā uz to, kā rīkoties liela apmēra intelektuālā īpašuma tiesību pārkāpumu gadījumos. Eiropas Komisijas Tirdzniecības ģenerāldirektorāts jo īpaši uzsver, ka "ir paredzēts koncentrēties uz tādu viltošanas un pirātisma darbību, kas būtiski skar ekonomiskās intereses, nevis uz vienkāršo pilsoņu darbību" ([4]).

7. Ciktāl tas attiecas uz nolīguma saturu, "Galveno apspriežamo tematu kopsavilkumā", kuru Eiropas Komisijas Tirdzniecības ģenerāldirektorāts publicēja 2009. gada novembrī, ir minēts, ka *ACTA* mērķis apkarot pirātismu un viltošanu tiks sasniegts šādos trīs galvenajos veidos: i) starptautiskā sadarbība, ii) īstenošanas prakse, un iii) tiesiskā regulējuma formulēšana intelektuālā īpašuma tiesību īstenošanai vairākās apzinātajās nozarēs, jo īpaši elektroniskajā vidē. ([5]) Paredzētie pasākumi jo īpaši būs veltīti tiesiskajai kārtībai (piemēram, tiesību aizsardzības līdzekļi, pagaidu pasākumi), interneta pakalpojumu sniedzēju nozīmei un pienākumiem, lai nepieļautu autortiesību pārkāpumus internetā, un starptautiskās sadarbības pasākumiem, lai novērstu viltotu preču pārvietošanu pāri robežām. Tomēr publiskotajā informācijā ir sniegtas tikai vispārīgas ziņas par nolīgumu un tajā nav sīkāk aplūkoti nekādi īpaši vai konkrēti pasākumi.

8. EDAU norāda, ka pat tad, ja *ACTA* iecerētais mērķis ir apkarot tikai liela apmēra intelektuālā īpašuma tiesību pārkāpumus, nevar izslēgt, ka *ACTA* skars arī vienkāršo pilsoņu darbības, jo īpaši tad, ja īstenošanas pasākumi notiks elektroniskajā vidē. EDAU uzsver, ka personu pamattiesību aizsardzības nolūkā būs jānosaka atbilstošas garantijas. Turklāt datu aizsardzības tiesību akti aptver visas personas, tostarp personas, kuras, iespējams, var būt iesaistītas viltošanas un pirātisma darbībās; liela apmēra pārkāpumu apkarošanas mērķiem noteikti būs jāapstrādā arī personu dati.

9. Šajā saistībā EDAU stingri mudina Eiropas Komisiju nodrošināt atklātu un pārredzamu dialogu par *ACTA*, iespējams, rīkojot atklātas konsultācijas, kas palīdzētu arī nodrošināt veicamo pasākumu atbilstību ES privātuma un datu aizsardzības tiesību aktu prasībām.

III. **EDAU KOMENTĀRU MĒRĶIS**

10. EDAU stingri aicina ES un jo īpaši Eiropas Komisiju, kurai ir piešķirts nolīguma parakstīšanas mandāts, rast pareizu līdzsvaru starp intelektuālā īpašuma tiesību aizsardzības prasībām un personas tiesībām uz privātuma un datu aizsardzību.

11. EDAU uzver, ka privātums un datu aizsardzība ir Eiropas Savienības pamatvērtības, kuras ir atzītas Eiropas Cilvēktiesību konvencijas 8. pantā un Eiropas Pamattiesību hartas ([6]) 7. un 8. pantā un kuras ir jāievēro visos ES saskaņā ar Līguma par Eiropas Savienības darbību *(TFEU)* 16. pantu pieņemtajos politikas un noteikumu dokumentos.

12. Papildus EDAU uzsver, ka jebkādās vienošanās, kuras Eiropas Savienība panākusi saistībā ar *ACTA*, ir jāievēro tiesiskie pienākumi, kas noteikti ES attiecībā uz privātuma un datu aizsardzības tiesību normām, jo īpaši, kā paredz Direktīva 95/46/EK, Direktīva 2002/58/EK ([7]) un Eiropas Cilvēktiesību tiesas ([8]) un Eiropas Kopienu Tiesas ([9]) prakse.

13. Privātums un datu aizsardzība ir jāņem vērā jau pašā sarunu sākumā, nevis tad, kad ir izstrādāti plāni un kārtība un ir panākta vienošanās par to, jo tad jau ir pārāk vēlu meklēt alternatīvus privātuma aizsardzības interesēm atbilstošus risinājumus.

14. Ņemot vērā nelielo publiski pieejamās informācijas daudzumu, EDAU atzīmē, ka viņš nevar sniegt konkrētu *ACTA* noteikumu analīzi. Tādēļ šajā atzinumā EDAU vērsīs uzmanību uz konkrētu pasākumu iespējamo draudu privātumam un datu aizsardzībai raksturošanu, kurus nolīgums, kā jau minēts, var izraisīt šādās divās jomās: intelektuālā īpašuma tiesību īstenošana elektroniskajā vidē (IV nodaļa) un starptautiskās sadarbības mehānismi (V nodaļa).

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

([5]) Skatīt iepriekš zemteksta piezīmi Nr. 2.

([6]) Eiropas Savienības Pamattiesību harta, OV C 303, 14.12.2007., 1. lpp.

([7]) Eiropas Parlamenta un Padomes Direktīva 2002/58/EK (2002. gada 12. jūlijs) par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (direktīva par privāto dzīvi un elektronisko komunikāciju), OV L 201, 31.7.2002., 37. lpp.

([8]) Interpretācija par to, kā galvenie 1950. gada 4. novembrī Romā pieņemtās Eiropas Cilvēktiesību un pamatbrīvību aizsardzības konvencijas 8. panta noteikumi un normas ir piemērojami dažādām jomām. Jo īpaši skatīt tiesas praksi, uz kuru ir atsauces citās šā atzinuma daļās.

([9]) Jo īpaši skatīt: lieta C-275/06, *Productores de Música de España (Promusicae)*, *ECR* (2008), I–271. lpp., un lieta C-557/07, *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten, nyr.*

IV. INTELEKTUĀLĀ ĪPAŠUMA TIESĪBU ĪSTENOŠANA ELEKTRONISKAJĀ VIDĒ

IV.1. Nepieciešamība analizēt "interneta atslēgšanas par trim pārkāpumiem kārtības" ietekmi uz privātumu/datu aizsardzību

15. Kā norāda Eiropas Komisija, *ACTA* izveidos tiesisku regulējumu pirātisma apkarošanai elektroniskajā vidē ([10]). Šis regulējums nodrošinās noteikumus, saskaņā ar kuriem interneta pakalpojumu sniedzējus un citus tiešsaistes starpniekus ([11]) varēs saukt pie atbildības par autortiesību pārkāpumiem attiecībā uz tādiem materiāliem, kurus izplata ar viņu tehnisko līdzekļu palīdzību. Regulējums var nodrošināt arī pasākumus un tiesību aizsardzības līdzekļus, kurus var piemērot interneta lietotājiem, ja viņi augšupielādē vai lejupielādē ar autortiesībām aizsargātus materiālus, pārkāpjot autortiesības. Lai gan detalizēta informācija par šādu regulējumu nav oficiāli publicēta, ņemot vērā no dažādiem avotiem pieejamo informāciju, var secināt, ka tas var iekļaut pienākuma noteikšanu interneta pakalpojumu sniedzējiem pieņemt "interneta atslēgšanas par trim pārkāpumiem kārtību", kuru dēvē arī par "pakāpeniskas reaģēšanas" plāniem. Šādi plāni ļaus autortiesību turētājiem uzraudzīt interneta lietotājus un noskaidrot iespējamos autortiesību pārkāpējus. Pēc sazināšanās ar iespējamā pārkāpēja interneta pakalpojumu sniedzēju interneta pakalpojumu sniedzējs brīdinātu lietotāju, kas ir atzīts par pārkāpēju, un pēc trīs brīdinājumu saņemšanas šādam lietotājam atslēgtu piekļuvi internetam.

16. Līdztekus *ACTA* sarunām "interneta atslēgšanas par trim pārkāpumiem" kārtību dažas dalībvalstis jau ievieš, piemēram, Francija. To patlaban apspriež arī dažādos ES forumos, piemēram, "Ieinteresēto pušu dialogs par nelegālu augšupielādi un lejupielādi", kas patlaban notiek pēc *DG MARKT* ierosmes saistībā ar Komisijas paziņojuma pieņemšanu, lai veicinātu intelektuālā īpašuma tiesību īstenošanu iekšējā tirgū ([12]). Arī Eiropas Parlaments diskutē par šo tēmu saistībā ar notiekošajām debatēm par Eiropas Parlamenta rezolūcijas attiecībā uz intelektuālā īpašuma tiesību īstenošanu iekšējā tirgū stingrākas piemērošanas projektu (ko dēvē arī par "Gallo" *(Gallo)* ziņojumu).

17. Šāda prakse ir liela iejaukšanās personu privātajā dzīvē. Tā ietver vispārēju interneta lietotāju darbības (tostarp pilnībā likumīgas) uzraudzību. Tā ietekmē miljoniem likumpaklausīgo interneta lietotāju, tostarp daudzus bērnus un pusaudžus. Šādu uzraudzību veic privātpersonas, nevis tiesībaizsardzības iestādes. Turklāt patlaban internetam ir liela nozīme gandrīz visos mūsdienu dzīves aspektos, tādēļ interneta piekļuves atslēgšanas sekas var būt ļoti nopietnas, nošķirot cilvēkus no darba, kultūras dzīves, e-pārvaldes lietojumprogrammām utt.

18. Ņemot to vērā, ir ieteicams novērtēt, cik lielā mērā šāda kārtība atbilst ES datu aizsardzības un privātuma tiesību aktiem, un jo īpaši, vai "interneta atslēgšanas par trim pārkāpumiem kārtība" ir vajadzīgs pasākums intelektuālā īpašuma tiesību īstenošanai. Šajā kontekstā ir jāanalizē, vai nav citu – mazāk agresīvu – metožu.

19. Joprojām nav skaidrs, vai "interneta atslēgšanas par trim pārkāpumiem kārtība" būs iekļauta *ACTA*. Tomēr šo kārtību izvērtē arī citās jomās un tai ir potenciāli liela ietekme uz personas datu un privātuma aizsardzību. Šo iemeslu dēļ EDAU uzskata, ka tā ir jāapspriež šajā atzinumā. Pirms iepriekš minētās analīzes veikšanas EDAU īsumā raksturos piemērojamo datu aizsardzības un privātuma tiesisko regulējumu.

20. Jāpiebilst, ka papildus datu aizsardzībai un privātumam interneta atslēgšanas par trim pārkāpumiem kārtība rada bažas attiecībā uz tādām vērtībām kā taisnīgs process un vārda brīvība. Tomēr šajā atzinumā tiks skatīti tikai tie jautājumi, kas ir saistīti ar personas datu un personu privātuma aizsardzību.

IV.2. Interneta atslēgšanas par trim pārkāpumiem kārtība un ES datu aizsardzības/privātuma tiesiskā regulējuma piemērošana

Kā var noteikt interneta atslēgšanas par trim pārkāpumiem kārtību

21. Īsumā saskaņā ar interneta atslēgšanas par trim pārkāpumiem kārtību autortiesību turētāji ar automatizētu tehnisko līdzekļu palīdzību, kurus, iespējams, nodrošinās trešās puses, atklās iespējamos autortiesību pārkāpumus, iesaistoties interneta lietotāju darbības uzraudzībā, piemēram,

([10]) Skatīt iepriekš zemteksta piezīmi Nr. 2.

([11]) Dažādus tiešsaistes starpniekus var definēt atbilstīgi viņu funkcionālajai nozīmei. Tomēr realitātē starpnieki parasti uzņemas vairākas no šīm funkcijām. Tiešsaistes starpnieki ietver: a) *piekļuves pakalpojumu sniedzēji*: lietotāji pieslēdzas tīklam, pieslēdzoties *piekļuves pakalpojumu sniedzēja* serverim; b) *tīkla pakalpojumu sniedzēji*: nodrošina maršrutētājus, t. i., datu pārraidei vajadzīgos tehniskos līdzekļus; c) *resursu pakalpojumu sniedzēji*: iznomā vietu savā serverī, kurā lietotāji vai satura pakalpojumu sniedzēji var augšupielādēt saturu. Lietotāji var augšupielādēt vai lejupielādēt materiālus tiešsaistes pakalpojumā, kā biļetens vai P2P tīkli.

([12]) Komisijas paziņojums Padomei, Eiropas Parlamentam un Eiropas Ekonomikas un sociālo lietu komitejai par intelektuālā īpašuma tiesību stingrāku piemērošanu iekšējā tirgū, Briselē, 2009. gada 11. septembrī, COM(2009) 467 galīgā redakcija.

uzraugot forumus, emuārus vai iekļaujoties kā datņu koplietotāji vienādranga tīklos, lai atklātu datņu koplietotājus, kuri, iespējams, apmainās ar materiāliem, kurus aizsargā autortiesības. ([13])

22. Pēc tam, kad ir atklāts interneta lietotājs, kas, iespējams, ir iesaistīts autortiesību pārkāpumā, apkopojot šādu lietotāju interneta protokola adreses (IP adreses), autortiesību turētāji nosūtīs šādu lietotāju IP adreses attiecīgajiem interneta pakalpojumu sniedzējiem, kuri brīdinās IP adreses abonenta īpašnieku par viņa iespējamo līdzdalību autortiesību pārkāpumā. Pēc tam, kad interneta pakalpojumu sniedzējs būs nosūtījis noteiktu skaitu brīdinājumu, interneta pakalpojumu sniedzējs automātiski pārtrauks sniegt pakalpojumus vai atslēgs abonentam interneta pieslēgumu. ([14])

Piemērojamais ES datu aizsardzības/privātuma tiesiskais regulējums

23. Interneta atslēgšanas par trim pārkāpumiem kārtībai ir jāatbilst prasībām, kas izriet no tiesībām uz privātumu, kā noteikts Eiropas Cilvēktiesību konvencijas 8. pantā un Pamattiesību hartas 7. pantā, kā arī, kas izriet no tiesībām uz datu aizsardzību, kā noteikts Pamattiesību hartas 8. pantā un *TFEU* 16. pantā un ka iestrādāts Direktīvā 95/46/EK un Direktīvā 2002/58/EK.

24. EDAU skatījumā interneta lietotāju rīcības uzraudzība un papildus viņu IP adrešu vākšana ir iejaukšanās viņu tiesībās uz privātās dzīves un sarakstes neaizskaramību, tas ir, iejaukšanās viņu tiesībās uz privāto dzīvi. Šis uzskats sakrīt ar Eiropas Cilvēktiesību tiesas praksi ([15]).

25. Ir piemērojama Direktīva 95/46/EK, ([16]) jo interneta atslēgšanas par trim pārkāpumiem kārtība ietver IP adrešu apstrādi, kuras jebkurā gadījumā attiecīgos apstākļos uzskata par personas datiem. IP adreses ir identifikatori, kas ir ar punktiem atdalītu skaitļu rinda, piemēram, 122.41.123.45. Abonēšanas noformēšana pie interneta pakalpojuma sniedzēja nodrošinās abonentam piekļuvi internetam. Ikreiz, kad abonents vēlēsies piekļūt internetam, viņam tiks piešķirta IP adrese ar iekārtas (piemēram, datora), kuru viņš izmanto, lai piekļūtu internetam, starpniecību. ([17])

26. Ja lietotājs iesaistās noteiktā darbībā, piemēram, augšupielādē internetā materiālus, trešās puses var atpazīt lietotāju pēc viņa izmantotās IP adreses. Piemēram, lietotājs ar IP adresi 122.41.123.45 ir augšupielādējis, iespējams, autortiesības pārkāpjošu materiālu P2P pakalpojumā plkst. 3:00 2010. gada 1. janvārī. Interneta pakalpojumu sniedzējs pēc tam varēs sasaistīt šādu IP adresi ar abonenta vārdu, kuram šī adrese ir piešķirta, un attiecīgi noskaidrot viņa personību.

27. Izvērtējot Direktīvas 95/46/EK 2. pantā paredzēto personas datu definīciju: "jebkura informācija attiecībā uz identificētu vai identificējamu fizisku personu ("datu subjektu"); identificējama persona ir tā, kuru var identificēt tieši vai netieši, norādot reģistrācijas numuru;" ([18]), var secināt, ka IP adreses un informācija par darbību, kas saistīta ar šādām adresēm, ir personas dati visos gadījumos, kuri attiecas uz šeit minēto. Patiesībā IP adreses ir identifikācijas numurs, kas ļauj noskaidrot tā abonenta vārdu, kuram šī IP adrese ir piešķirta. Turklāt informācija, kas ir savākta par abonentu, kuram ir piešķirta šāda IP adrese ("viņš augšupielādēja noteiktus materiālus tīmekļa vietnē ZS 2010. gada 1. janvārī, plkst. 15.00"), *attiecas uz šādu personu*, t. i., skaidri norāda uz identificējamas personas (IP adreses turētāja) rīcību un attiecīgi arī ir uzskatāma par personas datiem.

([13]) P2P tehnoloģija ir sadalīta datorizētas programmatūras arhitektūra, kas ļauj atsevišķiem datoriem tiešā veidā pieslēgties citiem datoriem un sazināties ar tiem.

([14]) Alternatīvas sankcijas ietver interneta pieslēguma funkciju ierobežošanu, piemēram, pieslēguma ātruma, apjoma samazināšana utt.

([15]) Jo īpaši skatīt ECT 2006. gada 26. jūnija spriedumu lietā *Weber and Saravia v. Germany* (dec.), Nr. 54934/00, 77. punkts, un ECT 2008. gada 1. jūlija spriedumu lietā *Liberty and others v the UK*, Nr. *58243/00*.

([16]) Eiropas Kopienu Tiesai ir plaša pieeja attiecībā uz Direktīvas 95/46/EK piemērojamību. Tās normas ir jāinterpretē Eiropas Cilvēktiesību konvencijas 8. panta izpratnē. Eiropas Kopienu Tiesa 2003. gada 20. maija spriedumā *Rundfunk* apvienotajās lietās C-465/00, C-138/01 un C-139/01, *ECR* (2003), I–4989. lpp., 68. punkts, konstatēja, ka "Direktīvas 95/46 noteikumi tiktāl, ciktāl tie nosaka personas datu apstrādi, kas var radīt pamattiesību, jo īpaši tiesību uz privātumu, pārkāpumu, ir obligāti jāinterpretē pamattiesību kontekstā, kuras saskaņā ar pastāvošo tiesas praksi ir neatņemama daļa no vispārējiem likumības principiem, kuru uzraudzību nodrošina Tiesa".

([17]) IP adrese, kuru interneta pakalpojumu sniedzējs piešķir personai, vienmēr var būt viena un tā pati ikreiz, kad viņš piekļūst internetam (to dēvē arī par statisko IP adresi). Citas IP adreses ir dinamiskas, kas nozīmē, ka interneta pakalpojumu sniedzējs piešķir saviem klientiem dažādas IP adreses ikreiz, kad viņi pieslēdzas internetam. Neapšaubāmi, interneta pakalpojumu sniedzējs var piesaistīt IP adresi tā abonenta kontam, kuram ir piešķirta (dinamiskā vai statiskā) IP adrese.

([18]) Šo definīciju papildina preambulas 26. punkts: "Tā kā aizsardzības principi ir jāpiemēro jebkurai informācijai par identificētu vai identificējamu personu; tā kā, lai noteiktu, vai persona ir identificējama, būtu jāņem vērā visi līdzekļi, kurus, iespējams, pamatoti izmantotu personas datu apstrādātājs vai jebkura cita persona, lai identificētu minēto personu; tā kā aizsardzības principus nepiemēro anonīmi iesniegtiem datiem, ja datu subjekts vairs nav identificējams; (…)".

28. Šo uzskatu pilnībā atbalsta 29. panta darba grupa, kura dokumentā par datu aizsardzības jautājumiem saistībā ar intelektuālā īpašuma tiesībām ir norādījusi, ka IP adreses, kuras vāc, lai īstenotu intelektuālā īpašuma tiesības, t. i., atklātu interneta lietotājus, kuri, iespējams, pārkāpj intelektuālā īpašuma tiesības, ir personas dati tiktāl, ciktāl tos izmanto šādu tiesību īstenošanai attiecībā uz konkrēto personu ([19]).

29. Tāpat arī ir piemērojama Direktīva 2002/58/EK, jo interneta atslēgšanas par trim pārkāpumiem kārtība nozīmē arī datu plūsmas informācijas un sakaru datu vākšanu. Direktīva 2002/58/EK reglamentē šādu datu izmantošanu un paredz saziņas konfidencialitātes principu sabiedriskajos sakaru tīklos un attiecībā uz datiem, kas attiecas uz šādu saziņu.

IV.3. **Vai interneta atslēgšanas par trim pārkāpumiem kārtība ir vajadzīgs pasākums?**

30. Eiropas Cilvēktiesību konvencijas 8. pants nosaka vajadzības principu, saskaņā ar kuru jebkādi pasākumi, kas pārkāpj personu privātumu, ir pieļaujami tikai gadījumā, ja tie ir vajadzīgi demokrātiskā sabiedrībā, lai īstenotu tās leģitīmos mērķus. ([20]) Vajadzības princips ir paredzēts arī Direktīvas 95/46/EK 7. un 13. pantā un Direktīvas 2002/58/EK 15. pantā. ([21]) Šis princips nozīmē, ka ir jāizanalizē pasākuma samērīgums, kas jānovērtē, pamatojoties uz skarto interešu līdzsvaru, ņemot to vērā visas demokrātiskās sabiedrības kontekstā. ([22]) Tāpat arī tas nozīmē, ka ir jāizvērtē, vai nepastāv mazāk agresīvi alternatīvi pasākumi.

31. Lai gan EDAU atzīst intelektuālā īpašuma tiesību īstenošanas svarīgumu, viņš tomēr uzskata, ka interneta atslēgšanas par trim pārkāpumiem kārtība tās pašreizējā formā, kas ietver noteiktus vispārējas piemērošanas elementus, ir nesamērīgs pasākums un tādēļ to nevar uzskatīt par vajadzīgu pasākumu. Tāpat arī EDAU ir pārliecināts, ka ir alternatīvi mazāk agresīvi risinājumi vai arī paredzēto politiku var īstenot mazāk agresīvā veidā vai ierobežotākā apmērā. Interneta atslēgšanas par trim pārkāpumiem pieeja rada sarežģījumus arī plašākā tiesiskā izpratnē. Šie secinājumi tiks aplūkoti turpmāk.

Trīs pārkāpumu pieeja nav samērīga

32. EDAU vēlas uzsvērt ierosināto pasākumu pārāk plašo mērogu. Šajā saistībā jāmin šādi apsvērumi:

i) apstāklis, ka (nepaziņota) uzraudzība ietekmētu miljoniem cilvēku un *visus* lietotājus neatkarīgi no tā, vai viņus tur aizdomās;

ii) uzraudzība nozīmētu datu sistemātisku reģistrēšanu; dažu šādu datu dēļ cilvēki var nonākt civillietu tiesā vai pat krimināltiesā, turklāt noteiktu savākto informāciju var klasificēt kā sensitīvus datus saskaņā ar Direktīvas 95/46/EK 8. pantu, kurai attiecīgi vajadzīga stingrāka aizsardzība;

iii) uzraudzība var izraisīt daudzus kļūdainus lēmumus. Autortiesību pārkāpums nenozīmē tikai vienkāršu "Jā" vai "Nē" atbildi uz jautājumu. Lai konstatētu, vai ir noticis pārkāpums, tiesām nereti ir jāizskata ļoti liels tehniskās un juridiskās informācijas daudzums, izlasot desmitiem lappušu; ([23])

([19]) 29. panta darba grupas darba dokuments par datu aizsardzības jautājumiem saistībā ar intelektuālā īpašuma tiesībām (WP 104), kas pieņemts 2005. gada 18. janvārī. Šī darba grupa tika izveidota saskaņā ar Direktīvas 95/46/EK 29. pantu. Tā ir neatkarīga Eiropas konsultatīvā organizācija datu aizsardzības un privātuma jautājumos. Tās uzdevumi ir izklāstīti Direktīvas 95/46/EK 30. pantā un Direktīvas 2002/58/EK 15. pantā. Skatīt arī darba grupas 2007. gada 20. jūnijā pieņemto atzinumu 4/2007 par personas datu jēdzienu (WP 136), jo īpaši 16. lpp.

([20]) Eiropas Cilvēktiesību konvencijas 8. pantā ir nepārprotami norādīts, ka iejaukšanās vai ierobežojumi var būt "nepieciešami demokrātiskā sabiedrībā".

([21]) Direktīvas 95/46/EK 13. pants pieļauj ierobežojumu tikai gadījumā, ja tas ir "ir nepieciešams aizsargpasākums: a) valsts drošībai; b) aizsardzībai; c) sabiedrības drošībai; d) krimināls odāmu noziedzīgu nodarījumu vai reglamentētu profesiju ētikas pārkāpumu profilaksei, izziņai, atklāšanai un krimināl vajāšanai; e) dalībvalsts vai Eiropas Savienības svarīgās ekonomiskās vai finansiālās interesēs, tostarp monetāros, budžeta un nodokļu jautājumus; f) ar oficiālo pilnvaru īstenošanu c), d) un e) apakšpunktā minētajos gadījumos pat laiku pa laikam saistītajai uzraudzībai, pārbaudei un reglamentējošām funkcijām; g) datu subjekta aizsardzībai vai citu personu tiesību un brīvību aizsardzībai". Direktīvas 2002/58/EK 15. pants paredz (…)" ja šādi ierobežojumi ir vajadzīgi saskaņā ar nepieciešamiem, atbilstīgiem un samērīgiem pasākumiem demokrātiskā sabiedrībā, lai garantētu valsts drošību, aizsardzību, sabiedrības drošību un krimināl pārkāpumu vai elektroniskās komunikācijas sistēmas nevēlamas izmantošanas novēršanu, izmeklēšanu, noteikšanu un krimināl vajāšanu, kā noteikts Direktīvas 95/46/EK 13. panta 1. punktā".

([22]) Skatīt arī ECT 1984. gada 2. augusta lietu *Malone* v. *the United Kingdom, Series A* no. *82*, 32. lpp., *paras 81 un* s., un ECT 2008. gada 4. decembra lietu *Marper* v. *the United Kingdom* (GC), nos. 30562/04 un 30566/04, *paras* 101 un *s.*

([23]) Tiesām jāizvērtē, vai konkrētos materiālus tiešām aizsargā autortiesības, kādas tiesības ir tikušas pārkāptas, vai izmantošanu var uzskatīt par taisnīgas izmantošanas gadījumu, piemērojamās tiesību normas, zaudējumus utt.

iv) iespējamās uzraudzības *sekas*, kuras var iestāties piekļuves internetam atslēgšanas dēļ. Tas var nozīmēt iejaukšanos personu tiesībās uz vārda brīvību, informācijas brīvību un piekļuvi kultūras dzīvei, e-pārvaldes lietojumprogrammām, interneta veikaliem, elektroniskajam pastam un dažos gadījumos arī darba iespējām. Šajā saistībā ir jo īpaši svarīgi apzināties, ka šādas sekas izjutīs ne tikai iespējamais pārkāpējs, bet arī visi ģimenes locekļi, kas izmanto to pašu interneta pieslēgumu, tostarp skolas vecuma bērni, kuri izmanto internetu mācību nolūkiem;

v) tas apstāklis, ka parasti izvērtējumu veiks un lēmumu pieņems privāta organizācija (t. i., autortiesību turētāji vai interneta pakalpojumu sniedzēji). EDAU iepriekšējā atzinumā jau ir minējis bažas par personu uzraudzību, ko veic privātas organizācijas (piemēram, interneta pakalpojumu sniedzēji vai autortiesību turētāji) jomās, kuras būtībā ietilpst tiesībaizsardzības iestāžu kompetencē. ([24])

33. EDAU nav pārliecināts, vai šādu pasākumu nodrošinātie ieguvumi būs lielāki par sekām, kuras tie radīs personu pamattiesībām. Autortiesību aizsardzība ir paredzēta šādu tiesību turētāju un sabiedrības interesēs. Tomēr pamattiesību ierobežojumi nešķiet pamatoti, salīdzinot iejaukšanās pakāpi, t. i., iejaukšanās privātajā dzīvē mērogu, kā minēts iepriekš, ar paredzamajiem ieguvumiem, atturot no intelektuālā īpašuma tiesību pārkāpumiem, kuru lielākā daļa ir maznozīmīgi intelektuālā īpašuma tiesību pārkāpumi. Ģenerāladvokāts *Kokott* atzinumā *Promusicae* norāda: "Nav (…) skaidrs, vai privāta rakstura datņu apmaiņa, jo īpaši tad, ja tā notiek bez jebkāda nodoma gūt peļņu, apdraud autortiesību aizsardzību tādā mērā, lai attaisnotu šādus izņēmuma līdzekļus. Patiesībā tas ir strīdīgs jautājums, cik lielā mērā privāta datņu apmaiņa patiešām rada zaudējumus". ([25])

34. šajā saistībā ir vērts arī atgādināt Eiropas Parlamenta reakciju attiecībā uz "trīs pārkāpumu plānu" telekomunikāciju paketes pārskatīšanas kontekstā, jo īpaši Pamatdirektīvas 138. labojumu. ([26]) Šajā labojumā tika noteikts, ka jebkādus ierobežojumus pamattiesībām vai brīvībām var noteikt tikai tajā gadījumā, ja tie ir atbilstoši, samērīgi un vajadzīgi demokrātiskā sabiedrībā, savukārt to īstenošanai piemēro atbilstošas procesuālās garantijas atbilstīgi Eiropas Cilvēktiesību konvencijai un Kopienas tiesību normu vispārīgajiem principiem, tostarp efektīvu tiesisko aizsardzību un taisnīgu tiesu. ([27])

35. šajā saistībā EDAU papildus uzsver, ka jebkādi pamattiesību ierobežojumi ir rūpīgi jāizvērtē gan ES, gan attiecīgajās valstīs. Šajā kontekstā var saskatīt līdzības ar datu saglabāšanas Direktīvu 2006/24/EK ([28]), kurā ir atkāpe no vispārīgā datu aizsardzības principa saistībā ar datu dzēšanu, ja tie vairs nav vajadzīgi mērķim, kuram tie tika vākti. Šī direktīva paredz, ka datu plūsmas informāciju saglabā smagu noziedzīgu nodarījumu apkarošanas nolūkā. Jāpiebilst, ka datu saglabāšana ir atļauta tikai saistībā ar smagiem noziedzīgiem nodarījumiem un attiecas tikai uz datu plūsmas informāciju, kas būtībā izslēdz informāciju par saziņas saturu, un tāpat arī ir paredzētas stingrākas garantijas. Tomēr ir radušās šaubas par tās atbilstību pamattiesību standartiem; Rumānijas Konstitucionālā tiesa ir nolēmusi, ka visaptveroša saglabāšana neatbilst pamattiesībām ([29]), turklāt šobrīd tāda pati lieta ir iesniegta izskatīšanai arī Vācijas Konstitucionālajā tiesā. ([30])

Citu mazāk agresīvu līdzekļu esamība

36. Iepriekš minētos konstatējumus pastiprina apstāklis, ka ir mazāk agresīvi līdzekļi šā paša mērķa sasniegšanai. EDAU uzstāj, ka vajadzētu izpētīt un izmēģināt šādus mazāk agresīvus līdzekļus.

([24]) EDAU 2008. gada 23. jūnija atzinums par priekšlikumu lēmumam, ar kuru izveido daudzgadu Kopienas programmu par bērnu aizsardzību, izmantojot internetu un citas sakaru tehnoloģijas, OV C 2, 7.1.2009., 2. lpp.

([25]) Skatīt 8. zemteksta piezīmē minētās lietas 106. daļu.

([26]) Skatīt Eiropas Parlamenta un Padomes 2009. gada 25. novembra Direktīvu 2009/140/EK, OV L 337, 18.12.2009., 37. lpp.

([27]) Tā dēvētā 138. labojuma galīgā redakcija ir izteikta šādi: "1. panta 3. punkta a) apakšpunkts. Pasākumi, ko dalībvalstis veic attiecībā uz lietotāju piekļuvi pakalpojumiem un lietojumprogrammām vai to lietošanu, izmantojot elektronisko komunikāciju tīklus, respektē fizisko personu pamattiesības un pamatbrīvības, kas garantētas Eiropas Cilvēktiesību un pamatbrīvību aizsardzības konvencijā, un Kopienas tiesību aktu vispārīgajiem principiem. Jebkuru no minētajiem pasākumiem attiecībā uz lietotāju piekļuvi pakalpojumiem un lietojumprogrammām vai to lietošanu, izmantojot elektronisko komunikāciju tīklus, kurš varētu ierobežot šīs pamattiesības un pamatbrīvības, var veikt vienīgi tad, ja tas ir piemērots, samērīgs un vajadzīgs demokrātiskā sabiedrībā, un uz to īstenošanu attiecina piemērotus procedūras aizsardzības pasākumus atbilstīgi Eiropas Cilvēktiesību un pamatbrīvību aizsardzības konvencijai un Kopienas tiesību aktu vispārīgajiem principiem, tostarp efektīvu tiesisko aizsardzību un taisnīgu tiesu. Tātad šos pasākumus var veikt vienīgi tad, ja tiek pienācīgi respektēts nevainīguma prezumpcijas princips un tiesības uz privātumu. Nodrošina iepriekšēju taisnīgu un objektīvu procedūru, tostarp iesaistītās personas vai iesaistīto personu tiesības tikt uzklausītam, ņemot vērā vajadzību pienācīgi pamatotos gadījumos nodrošināt atbilstīgus apstākļus un procedūras pasākumus atbilstīgi Eiropas Cilvēktiesību un pamatbrīvību aizsardzības konvencijai. Garantē tiesības uz efektīvu un savlaicīgu tiesas izskatīšanu."

([28]) Eiropas Parlamenta un Padomes 2006. gada 15. marta Direktīva 2006/24/EK, OV L 105,13.4.2006., 54. lpp.

([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. Šajā saistībā EDAU atgādina grozīto Direktīvu 2002/22/EK par universālo pakalpojumu un lietotāju tiesībām attiecībā uz elektronisko sakaru tīkliem un pakalpojumiem (ko dēvē arī par "pilsoņu tiesību direktīvu"), kas ir nesen pārskatītās telekomunikāciju paketes daļa un iekļauj atsevišķus noteikumus un kārtību nolūkā ierobežot neliela apmēra autortiesību pārkāpumus no patērētāju puses. ([31]) Šī kārtība ietver pienākumu dalībvalstīm nodrošināt standartizētu sabiedrību interesējošu informāciju par dažādām tēmām, jo īpaši skaidrojot autortiesību un blakustiesību pārkāpumus un to tiesiskās sekas ([32]). Dalībvalstis var pēc tam pieprasīt interneta pakalpojumu sniedzējiem izplatīt informāciju visiem klientiem un iekļaut to klientu līgumos.

38. Sistēma ir paredzēta, lai informētu cilvēkus un pārliecinātu viņus neizplatīt ar autortiesībām aizsargātu informāciju un neiesaistīties nelikumīgās darbībās, vienlaikus izvairoties no interneta izmantošanas uzraudzības un bažām par datu aizsardzību. Pilsoņu tiesību direktīvai ir jābūt ieviestai 2011. gada maijā; tātad minētā kārtība vēl nepastāv. Tādēļ vēl nav bijusi iespēja pārbaudīt tās sniegtos ieguvumus. Tātad ir pāragri neņemt vērā iespējamos šīs jaunās kārtības nodrošinātos ieguvumus un tā vietā pieņemt "atslēgšanas par trim pārkāpumiem" kārtību, kas ierobežo pamattiesības daudz lielākā mērā.

39. Papildus iepriekš minētajam ir jāatgādina, ka 2004. gada 28. aprīļa Direktīva 2004/48/EK par intelektuālā īpašuma tiesību piemērošanu paredz dažādus līdzekļus intelektuālā īpašuma tiesību īstenošanai tiesās (aplūkots tālāk, sākot ar 43. punktu). ([33])

40. *IPRE* direktīva ir tikai nesen pārņemta dalībvalstu tiesību aktos. Tādēļ nav bijis pietiekami daudz laika, lai novērtētu, vai tās noteikumi ir piemēroti intelektuālā īpašuma tiesību īstenošanas mērķiem. Attiecīgi jebkāda vajadzība aizstāt pašreizējo uz tiesas procesu balstīto sistēmu, kas vēl nav pārbaudīta, ir vismaz apšaubāma. Iepriekš minētais rada neizbēgamu jautājumu – kādēļ šobrīd izdarītos pārkāpumus nevar pienācīgi atrisināt, piemērojot pastāvošās civiltiesiskās un krimināltiesiskās sankcijas par autortiesību pārkāpumiem. Tādēļ pirms šādu politikas pasākumu ierosināšanas Komisijai vajadzētu sagatavot uzticamu informāciju, apliecinot, ka pašreizējais tiesiskais regulējums nespēj nodrošināt paredzēto mērķu sasniegšanu.

41. Turklāt nav skaidrs, vai ir nopietni apsvērti jebkādi alternatīvi ekonomiskie uzņēmējdarbības modeļi, kuros nebūtu nepieciešama sistemātiska personu uzraudzība. Piemēram, ja autortiesību turētāji ir konstatējuši zaudējumus, kurus izraisa P2P izmantošana, tiesību turētāji un interneta pakalpojumu sniedzēji varētu, piemēram, izmēģināt diferencētu piekļuves internetam abonēšanu, kurā daļa no ienākumiem par neierobežotas piekļuves abonēšanu tiktu sadalīta autortiesību turētājiem.

Iespēja veikt mērķtiecīgu uzraudzību mazāk agresīvā veidā

42. Līdztekus pilnīgi atšķirīgiem modeļiem, kurus, kā minēts, vajadzētu izpētīt un izmēģināt, jebkurā gadījumā var izmantot mērķtiecīgu uzraudzību mazāk agresīvā veidā.

43. Intelektuālā īpašuma tiesību īstenošanas mērķi var sasniegt, uzraugot tikai ierobežotu personu loku, par kurām ir aizdomas, ka tās ir iesaistītas nopietnā autortiesību pārkāpumā. *IPRE* direktīvā šajā saistībā ir paredzētas dažas vadlīnijas. Tajā ir paredzēti nosacījumi, saskaņā ar kuriem varas iestādes var pieprasīt, lai piekļuves internetam pakalpojumu sniedzēju rīcībā esošie dati tiktu atklāti intelektuālā īpašuma tiesību īstenošanas mērķiem. Direktīvas 8. pants paredz, ka kompetentas tiesu iestādes var pieprasīt interneta pakalpojumu sniedzējiem sniegt personas datus, kuri ir viņu rīcībā par iespējamajiem pārkāpējiem (piemēram, informācija par preču vai pakalpojumu, kas pārkāpj intelektuālā īpašuma tiesības, izcelsmi un izplatīšanas tīkliem), reaģējot uz pamatotu un samērīgu pieprasījumu gadījumā, ja pārkāpums ir izdarīts *komercnolūkā*. ([34])

44. Tātad izšķiroša nozīme ir komercnolūka kritērijiem. Saskaņā ar šiem kritērijiem uzraudzība var būt samērīga ierobežotu, konkrētu un īpašu situāciju kontekstā, ja pastāv

([31]) Eiropas Parlamenta un Padomes 2009. gada 25. novembra Direktīva 2009/136/EK, OV L 337, 18.12.2009., 11. lpp.

([32]) Jo īpaši Direktīvas 2009/136/EK 21. panta 4. punkts paredz, ka "Dalībvalstis var prasīt, lai 3. punktā minētie uzņēmumi pašreizējiem un jauniem abonentiem vajadzības gadījumā bez maksas sniegtu informāciju, kas sabiedrībā rada plašu ieinteresētību, izmantojot tos pašus līdzekļus, kurus uzņēmumi lieto ikdienas saziņā ar abonentiem. Šādā gadījumā šo informāciju nodrošina attiecīgās valsts iestādes standartformā, un tā attiecas, *inter alia*, uz šādiem tematiem: a) parastākie elektronisko komunikāciju pakalpojumu lietojumi, iesaistoties nelikumīgās darbībās vai izplatot kaitīgu saturu, jo īpaši, ja tas var skart citu cilvēku tiesību un brīvību respektēšanu, arī autortiesību un blakustiesību pārkāpumus, un to tiesiskās sekas; (…)." Turklāt saskaņā ar 20. panta 2. punktu "Dalībvalstis var arī prasīt, lai līgumā būtu ietverta visa informācija, ko attiecīgas valsts iestādes šajā saistībā varētu sniegt par elektronisku komunikāciju tīklu un pakalpojumu lietojumu, lai nodarbotos ar nelikumīgām darbībām vai izplatītu kaitīgu saturu, un par aizsardzības līdzekļiem pret personiskas drošības, privātās dzīves vai personas datu apdraudējumiem, kā norādīts 21. panta 4. punktā, un kas ir atbilstīga sniegtajam pakalpojumam."

([33]) OV L 157, 30.4.2004., 45. lpp. (turpmāk tekstā – "*IPRE* direktīva").

([34]) Tas ir papildus apstiprināts *IPRE* direktīvas preambulas 14. apsvērumā.

pamatotas aizdomas par autortiesību ļaunprātīgu izmantošanu komerciālos nolūkos. Šie kritēriji var ietvert situācijas, kurās notiek nepārprotama autortiesību ļaunprātīga izmantošana, ko veic privātpersonas ar mērķi gūt tiešus vai netiešus materiālos labumus.

45. Praksē, lai nodrošinātu iepriekš minēto pasākumu efektivitāti, autortiesību turētāji varētu iesaistīties mērķtiecīgā noteiktu IP adrešu uzraudzībā, lai pārliecinātos par autortiesību pārkāpuma apmēru. Tas nozīmē, ka autortiesību turētājiem būtu arī atļauts tajos pašos nolūkos sekot līdzi ziņojumiem par iespējamo pārkāpumu. Šādu informāciju vajadzētu izmantot tikai pēc tam, kad ir pārbaudīta pārkāpuma smaguma pakāpe. Piemēram, acīmredzami lieli pārkāpumi, kā arī maznozīmīgi, taču pastāvīgi pārkāpumi noteiktā laikposmā materiāla labuma gūšanas vai finansiālas iedzīvošanās nolūkā. Sistemātiskuma noteiktā laikposmā nepieciešamība ir uzsvērta un detalizēti skaidrota tālāk apsvērumos par saglabāšanas principu.

46. Tas nozīmē, ka šādos gadījumos informācijas vākšanu nolūkā pierādīt iespējamo ļaunprātīgo interneta izmantošanu var uzskatīt par samērīgu un vajadzīgu, lai sagatavotos juridiskam procesam, tostarp tiesvedībai.

47. EDAU uzskata, ka ir nepieciešama papildu garantija – pirms datu apstrādes, lai iegūtu šāda veida pierādījumus, to vispirms vajadzētu pārbaudīt un atļaut valstu datu aizsardzības iestādēm. Šie uzskati ir balstīti uz apstākli, ka datu apstrādes operācijas var radīt konkrētus riskus personu tiesībām un brīvībām apstrādes mērķu kontekstā, t. i., tādu tiesību īstenošanas darbību veikšana, kuras pēc tam var izrādīties krimināli sodāmas, ņemot vērā savākto datu sensitivitāti. Fakts, ka apstrāde ietver elektronisko sakaru uzraudzību, ir papildfaktors, kas prasa pastiprinātu kontroli.

48. EDAU uzskata, ka *IPRE* direktīvā paredzētais komercnolūks ir ļoti atbilstošs nosacījums, lai noteiktu uzraudzības robežas samērīguma principa ievērošanai. Turklāt šķiet, ka nav ticamu pieradījumu, kas liecinātu, ka, ievērojot *IPRE* direktīvā noteiktos kritērijus, nav iespējami efektīvi tiesiski pretpasākumi autortiesību pārkāpumiem. Turklāt šķiet, ka ziņojumi, piemēram, no Vācijas, kur kopš 2008. gada, kad tika pārņemta *IPRE* direktīva, ir izdoti apmēram 3 000 tiesas rīkojumi, saskaņā ar kuriem interneta pakalpojumu sniedzēji ir atklājuši tiesām abonēšanas informāciju par 300 000 abonentu, pierāda pretējo.

49. Kopumā var secināt – tā kā *IPRE* direktīva ir spēkā tikai divus gadus, ir grūti izprast, kādēļ likumdevējiem vajadzētu atteikties no šajā direktīvā paredzētajiem kritērijiem un noteikt daudz agresīvākas metodes, ja ES tikai sāk pārbaudīt nesen pieņemtās metodes. Šā paša iemesla dēļ ir arī grūti izprast vajadzību aizstāt pašreizējo uz tiesu balstīto sistēmu ar cita veida pasākumiem (papildus rodas arī jautājums par likumīgu procesu, kas šeit nav minēts).

IV.4. **Interneta atslēgšanas par trim pārkāpumiem kārtības atbilstība detalizētākiem datu aizsardzības noteikumiem**

50. Ir citi konkrētāki tiesiski iemesli, kādēļ trīs pārkāpumu pieeja ir problemātiska datu aizsardzības izpratnē. EDAU vēlas uzsvērt apšaubāmo juridisko pamatu apstrādei, kuru paredz Direktīva 95/46/EK, un Direktīvā 2002/58/EK paredzēto *log* datņu iznīcināšanas pienākumu.

Apstrādes tiesiskais pamats

51. Trīs pārkāpumu pieejas plāns paredz apstrādāt personas datus, no kuriem daži tiks izmantoti tiesiskajā vai administratīvajā procesā, lai atslēgu piekļuvi internetam par atkārtotiem pārkāpumiem. Šajā saistībā šādus datus klasificē kā sensitīvus datus saskaņā ar Direktīvas 95/46/EK 8. pantu. Direktīvas 8. panta 5. punktā ir noteikts: "Uz noziedzīgiem nodarījumiem, kriminālas vajāšanas gadījumiem vai drošības pasākumiem attiecināmu datu apstrādi var veikt tikai valsts iestādes kontrolē vai, ja saskaņā ar attiecīgās valsts tiesībām ir paredzētas piemērotas speciālas garantijas (…)".

52. Šajā saistībā ir lietderīgi atgādināt iepriekš minēto 29. panta darba grupas dokumentu, kurā ir aplūkoti tiesu datu apstrādes jautājumi. ([35]) Darba grupa norāda, ka "Lai gan ikvienai personai neapšaubāmi ir tiesības apstrādāt tiesas datus šādas personas lietas iztiesāšanas procesā, šis princips tomēr nenozīmē, ka trešām pusēm ir atļauta personas datu padziļināta izpēte, vākšana un centralizācija, tostarp jo īpaši sistemātiska vispārīga izpēte, piemēram, interneta skenēšana (…). Šāda izmeklēšana ir tiesu iestāžu kompetencē". ([36]) Lai gan noteiktu un konkrētu pierādījumu vākšana, jo īpaši smagu pārkāpumu gadījumā, var būt vajadzīga, lai formulētu un izpildītu juridisku prasību, EDAU pilnībā atbalsta 29. panta darba grupas viedokli par leģitimitātes trūkumu plaša mēroga izmeklēšanai, kas ietver liela interneta lietotāju datu apjoma apstrādi.

53. Iepriekš izklāstītās diskusijas par samērīguma principu un komercnolūka kritērijiem ir piemērotas, lai noteiktu, kādi IP adrešu un saistītās informācijas vākšanas nosacījumi ir leģitīmi.

([35]) Skatīt šā atzinuma 28. punktu.
([36]) Tekstu ir pasvītrojis autors.

54. Interneta pakalpojumu sniedzēji var mēģināt legalizēt autortiesību turētāju veikto apstrādi, iekļaujot attiecīgus pantus klientu līgumos, kas ļauj uzraudzīt klientu datus un atslēgt abonentu. Ja klients paraksta šādu līgumu, var uzskatīt, ka viņš ir piekritis uzraudzībai. Tomēr šāda prakse rada pamatjautājumu par to, vai persona var sniegt piekrišanu interneta pakalpojumu sniedzējam par datu apstrādi, kuru veiks nevis interneta pakalpojumu sniedzējs, bet gan trešās puses, kuras neatrodas interneta pakalpojumu sniedzēja kontrolē.

55. Otrkārt, pastāv jautājums par piekrišanas derīgumu. Direktīvas 95/46/EK 2. panta h) apakšpunktā piekrišana ir definēta kā "jebkurš labprātīgi sniegts šīs personas vēlmju konkrēts un paziņots norādījumu, ar kuru datu subjekts izsaka savu piekrišanu uz viņu attiecināmu personas datu apstrādei". Ir svarīgi atcerēties, ka, lai piekrišana būtu derīga neatkarīgi no apstākļiem, kādos tā ir dota, tai ir jābūt labprātīgam, konkrētam un paziņotam norādījumam par datu subjekta vēlmēm, kā ir definēts direktīvas 2. panta h) apakšpunktā. EDAU ir nopietnas šaubas par to, vai personām, kad tām tiks lūgta piekrišana viņu darbības internetā uzraudzībai, būs iespēja izdarīt īstu izvēli, jo īpaši tādēļ, ka alternatīva būs interneta pieslēguma neesamība, kas tādējādi var apdraudēt daudzas viņu dzīves jomas.

56. Treškārt, pastāv jautājums par to, vai jebkādu šādu uzraudzību vispār var uzskatīt par *vajadzīgu* līguma, kurā datu subjekts ir līgumslēdzēja puse, izpildei, kā nosaka Direktīvas 95/46/EK 7. panta b) apakšpunkts, jo uzraudzība acīmredzami nav datu subjekta parakstītā līguma mērķis, bet gan tikai līdzeklis interneta pakalpojumu sniedzējam, kuru viņš izmanto citu personu interesēs.

Log datņu dzēšana

57. Saskaņā ar Direktīvu 2002/58/EK, proti, tās 6. pantu, tādu plūsmas informāciju kā IP adreses var vākt un glabāt tikai tādu iemeslu dēļ, kas ir tieši saistīti ar pašu saziņu, tostarp rēķinu kārtošanu, datu plūsmas informācijas pārvaldību un krāpšanas novēršanu. Pēc tam dati ir jāizdzēš. Tas nenodara kaitējumu datu saglabāšanas direktīvā paredzētajiem pienākumiem, saskaņā ar kuriem, kā jau minēts, ir jāglabā datu plūsmas informāciju un to var atklāt policijai un prokuratūrai, **tikai** lai palīdzētu **smagu noziedzīgu nodarījumu** izmeklēšanai. ([37])

58. Saskaņā ar iepriekš minēto interneta pakalpojumu sniedzējiem vajadzētu izdzēst visas *log* datnes, kuras var atklāt interneta lietotāju darbības, ja datnes vairs nav vajadzīgas iepriekš minētajiem mērķiem. Ņemot vērā to, ka *log* datnes nav vajadzīgas rēķinu apstrādes vajadzībām, var pieņemt, ka trīs vai četras nedēļas varētu būt pietiekams laiks, kurā interneta pakalpojumu sniedzējs varētu tās izmantot datu plūsmas informācijas pārvaldības mērķiem. ([38])

59. Tas nozīmē, ka, saņemot pieprasījumu no autortiesību turētāja, ja vien šāds pieprasījums nav iesniegts iepriekš norādītajā laikposmā, interneta pakalpojumu sniedzēja rīcībā nevajadzētu būt *log* datnēm, kuras sasaista IP adreses ar konkrētiem abonentiem. *Log* datņu glabāšana ilgāk par šādu laikposmu ir pieļaujama tikai pamatotu iemeslu dēļ, ievērojot likumā paredzētos mērķus.

60. Tas nozīmē, ka autortiesību turētāju pieprasījumus interneta pakalpojumu sniedzējiem nevarēs izpildīt vienkārši tādēļ, ka interneta pakalpojumu sniedzējam šādas informācijas vairs nebūs, ja vien šāds pieprasījums netiks iesniegts ļoti savlaicīgi. Tas arī nosaka pieņemamas uzraudzības prakses robežas, kā aprakstīts iepriekš.

Seku izplatīšanās risks

61. EDAU uztrauc ne tikai interneta atslēgšanas par trim pārkāpumiem kārtības ietekme uz privātumu un datu aizsardzību, bet arī tās seku izplatīšanās. Ja tiks atļauta interneta atslēgšanas par trim pārkāpumiem kārtība, tas var izraisīt risku, ka tiks legalizēta pat vēl plašāka interneta lietotāju darbības uzraudzība dažādās jomās un dažādos nolūkos.

62. EDAU aicina Komisiju pēc iespējas drīzāk nodrošināt, lai *ACTA* netiktu vēl vairāk izvērsts un nenonāktu pretrunā pašreizējam ES režīmam attiecībā uz intelektuālā īpašuma tiesību īstenošanu, kurā ir ievērotas pamattiesības, pamatbrīvības un pilsoniskās brīvības, kā personas datu aizsardzība.

V. **BAŽAS PAR DATU AIZSARDZĪBU SAISTĪBĀ AR STARPTAUTISKĀS SADARBĪBAS MEHĀNISMIEM**

63. Viens no *ACTA* sarunu dalībnieku ierosinātājiem līdzekļiem intelektuālā īpašuma tiesību īstenošanas jautājumu risināšanai ir starptautiskās sadarbības uzlabošana līdz ar

([37]) Skatīt šā atzinuma 35. punktu.

([38]) Datu plūsmas informācijas pārvaldība ietver datoru tīkla datu plūsmas informācijas analīzi, lai uzlabotu vai garantētu tā darbību, mazāku latentumu un/vai palielinātu izmantojamo joslas platumu.

daudziem pasākumiem, kas nodrošinātu efektīvu intelektuālā īpašuma tiesību īstenošanu *ACTA* parakstītāju valstu jurisdikcijās.

64. Ņemot vērā pieejamo informāciju, var secināt, ka vairāki pasākumi, kas tiek plānoti intelektuālā īpašuma tiesību īstenošanas nodrošināšanai, būs saistīti ar starptautisku informācijas apmaiņu par iespējamajiem intelektuālā īpašuma tiesību pārkāpumiem starp valsts iestādēm (kā muitas, policijas un tiesu iestādes), kā arī valsts iestādēm un privātajām organizācijām (kā interneta pakalpojumu sniedzēji un intelektuālā īpašuma tiesību turētāji). Šāda datu apmaiņa rada daudz jautājumu saistībā ar datu aizsardzību.

V.1. **Vai *ACTA* paredzētā datu apmaiņa ir likumīga, vajadzīga un samērīga?**

65. Pašreizējā sarunu procesa posmā, kurā vēl nav formulēti vai nav zināmi daudzi konkrēti datu apstrādes jautājumi, nav iespējams pārliecināties, vai ierosināto pasākumu kopums atbilst datu aizsardzības pamatprincipiem un ES datu aizsardzības tiesību aktiem.

66. Vispirms var jautāt, vai datu nodošana trešām valstīm *ACTA* nolūkā ir likumīga. Starptautisku pasākumu pieņemšanas atbilstību šajā jomā var apšaubīt tik ilgi, kamēr starp ES dalībvalstīm nav nekāda nolīguma par īstenošanas pasākumu interneta vidē saskaņošanu un piemērojamo kriminālsankciju veidiem. ([39])

67. Ņemot vērā iepriekš minēto, šķiet, ka vajadzības un samērīguma principus attiecībā uz datu nodošanu saskaņā ar *ACTA* būtu daudz vieglāk ievērot, ja nolīgumā būtu skaidri paredzēts, ka tā mērķis ir apkarot tikai vissmagākos intelektuālā īpašuma tiesību pārkāpumus, nevis atļaut masveida datu nodošanu saistībā ar jebkādām aizdomām par intelektuālā īpašuma tiesību pārkāpumiem. Tādēļ vajadzēs precīzi formulēt, kas ir "vissmagākais intelektuālā īpašuma tiesību pārkāpums", par kuru var apmainīties ar datiem.

68. Turklāt īpašu vērību vajadzētu pievērst datu apmaiņā iesaistītajām personām un tam, vai ar datiem apmainīsies tikai valsts iestādes vai arī datu apmaiņa notiks starp valsts iestādēm un privātām organizācijām. Kā minēts iepriekš šajā atzinumā, privātu organizācija iesaistīšana jomā, kas būtībā ietilpst tiesībaizsardzības iestāžu kompetencē, rada daudz bažu. ([40]) Nosacījumi, saskaņā ar kuriem privātas organizācijas var iesaistīt ar intelektuālā īpašuma tiesību pārkāpumiem saistītu personu datu vākšanā un apmaiņā ar valsts iestādēm, ir jāattiecina tikai uz stingri ierobežotiem konkrētiem apstākļiem, nosakot atbilstošas garantijas.

V.2. **Piemērojamie datu aizsardzības tiesību akti, kas regulē datu nodošanu *ACTA* kontekstā**

Vispārīgais datu nodošanas režīms

69. Vispārīgais ES piemērojamais datu aizsardzības regulējums ir noteikts Direktīvā 95/46/EK. Direktīvas 95/46/EK 25. un 26. pants nosaka režīmu, kuru piemēro, nododot datus trešām valstīm. Direktīvas 25. pants paredz, ka datus var nodot tikai tādām valstīm, kuras nodrošina atbilstošu aizsardzības līmeni, citos gadījumos šāda nodošana būtībā ir aizliegta.

70. Trešo valstu nodrošinātās aizsardzības līmeni novērtē katrā konkrētā gadījumā Eiropas Komisija, kura ir izdevusi vairākus lēmumus, atzīstot vairāku valstu atbilstību pēc visaptverošas analīzes, ko veic 29. panta darba grupa. ([41])

71. EDAU norāda, ka lielākā daļa *ACTA* dalībnieku nav iekļauti Komisijas sagatavotajā to valstu sarakstā, kuras nodrošina atbilstošu datu aizsardzību, izņemot Šveici, un īpašos apstākļos – Kanādu un ASV, savukārt pārēji *ACTA* dalībnieki nav atzīti par tādiem, kas nodrošina atbilstošu aizsardzības līmeni. Tas nozīmē, ka datu nodošanai no ES uz šīm valstīm ir jāizpilda viens no Direktīvas 95/46/EK 26. panta 1. punkta nosacījumiem vai arī pusēm datu nodošanas brīdī ir jāsniedz atbilstošas garantijas saskaņā ar Direktīvas 26. panta 2. punktu.

Īpašs datu nodošanas režīms krimināltiesiskajā jomā

72. Lai gan Direktīva 95/46/EK ir galvenais datu aizsardzības instruments ES, tās darbības joma šobrīd ir ierobežota, jo tā cita starpā skaidri izslēdz valstu sadarbību krimināltiesiskajā jomā (3. pants). Datu apmaiņa krimināltiesiskās sadarbības nolūkos attiecīgi neietilpst Direktīvas 95/46/EK darbības jomā un tai piemēro vispārīgos datu aizsardzības

([39]) Priekšlikumu par kriminālsankcijām patlaban apspriež Padomē, COM(2006) 168, 2006. gada 26. aprīlis.

([40]) Skatīt šā atzinuma 32. un 52. punktu. Skatīt arī EDAU 2008. gada 11. novembra atzinumu par ES – ASV augsta līmeņa kontaktgrupas par informācijas apmaiņu, privātuma un personas datu aizsardzību gala ziņojumu, OV C 128, 6.6.2009., 1. lpp.

([41]) Skatīt atbilstības lēmumus, kurus Eiropas Komisija ir pieņēmusi par Argentīnu, Kanādu, Šveici, ASV saistībā ar ostu drošību un ASV iestādēm pasažieru datu reģistra *(PNR)* kontekstā, Gērnsiju, Menas salu un Džērsiju. Lēmumi ir pieejami: http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm

principus, kas paredzēti Eiropas Padomes Konvencijā Nr. 108 un tās papildu protokolos, kuriem ir pievienojušās visas ES dalībvalstis. ([42]) Papildus piemēro ES pieņemtos noteikumus par policijas un tieslietu sadarbību krimināllietās, kuri ir izklāstīti Padomes Pamatlēmumā 2008/877/TI. ([43])

73. Arī šajos dokumentos ir paredzēts princips, ka trešās valstīs, kurām nodod datus, ir jābūt nodrošinātam atbilstošam aizsardzības līmenim. Ir paredzēti vairāki izņēmumi, jo īpaši, ja trešā valsts sniedz atbilstošas garantijas. Līdzīgi kā datu apmaiņai saskaņā ar Direktīvu 95/46/EK, datu apmaiņai krimināltiesiskajā sadarbībā arī ir vajadzīgas atbilstošas garantijas, kuras datu apmaiņas pusēm ir jāsniedz, lai datu apmaiņa varētu notikt.

Tiecoties uz jaunu datu apmaiņas režīmu

74. Paredzams, ka tuvākajā nākotnē uz Līguma par Eiropas Savienības darbību 16. panta pamata tiks pieņemti jauni kopīgi noteikumi par datu aizsardzību, kuri būs piemērojami visām ES darbības jomām. Tas nozīmē, ka pēc dažiem gadiem var tikt radīts pilnīgs ES datu aizsardzības regulējums, nosakot vienveidīgus datu aizsardzības noteikumus visās ES darbības jomās un paredzot vienādus tiesību aizsardzības līdzekļus un garantijas visām datu apstrādes darbībām. Kā norādījusi tiesiskuma, pamattiesību un pilsonības komisāre *Viviane Reding* ([44]), šim jaunajam regulējumam ir jāfunkcionē kā vienotam "mūsdienīgam un pilnīgam juridiskajam instrumentam" datu aizsardzības nodrošināšanai ES. Šāds regulējums ir ļoti vēlams, jo nodrošinās lielāku skaidrību un konsekvenci attiecībā uz noteikumiem, kuri piemērojami datu aizsardzībai ES.

75. Starptautiskā kontekstā EDAU vēlas minēt arī Rezolūciju par starptautiskajiem personas datu un privātuma aizsardzības standartiem, kuru nesen pieņēma datu aizsardzības iestādes un kura ir sākums pasaules datu aizsardzības standartu noteikšanai. ([45]) Starptautiskie standarti ietver virkni datu aizsardzības garantiju, kuras ir līdzīgas Direktīvā 95/46/EK un Konvencijā Nr. 108 paredzētajām. Lai gan starptautiskie standarti vēl nav saistoši, tajos ir sniegtas noderīgas vadlīnijas par datu aizsardzības principiem, kurus var brīvprātīgi piemērot trešās valstis, lai to tiesiskais regulējums atbilstu ES standartiem. EDAU uzskata, ka arī *ACTA* parakstītājām valstīm vajadzētu ņemt vērā starptautiskajos standartos paredzētos principus, apstrādājot no ES saņemtus personas datus.

V.3. **Vajadzība ieviest atbilstošas garantijas, lai aizsargātu no ES trešām valstīm nodotos datus**

Kādām vajadzētu būt garantijām, lai efektīvi aizsargātu trešām valstīm nodotus datus?

76. Ja ir konstatēta nepieciešamība nodot personas datus trešām valstīm, EDAU uzsver, ka Eiropas Savienībai papildus *ACTA* nolīgumam vajadzētu pārrunāt ar trešām valstīm saņēmējām konkrētus instrumentus, kas ietver atbilstošas datu aizsardzības garantijas, nosakot personas datu apmaiņas nosacījumus.

77. Atbilstošas datu aizsardzības garantijas parasti vajadzētu noteikt saistošā nolīgumā starp ES un trešo valsti saņēmēju, saskaņā ar kuru saņēmēja puse apņemas ievērot ES datu aizsardzības tiesību normas un nodrošināt personām tādas pašas tiesības un tiesību aizsardzības līdzekļus, kādi ir paredzēti ES tiesību aktos. Saistoša nolīguma nepieciešamība izriet no Direktīvas 95/46/EK 26. panta 2. punkta un Pamatlēmuma 13. panta 3. punkta b) apakšpunkta, kā to apliecina arī ES prakse slēgt konkrētus nolīgumus, lai atļautu noteiktu datu nodošanu trešām valstīm ([46]).

78. Tāpat arī saskaņā ar starptautisko standartu projektu saņēmējam var pieprasīt garantēt, ka viņš var nodrošināt nepieciešamo aizsardzības līmeni, lai varētu notikt datu nodošana. Šīs garantijas var noteikt arī līgumsaistību formā.

To garantiju saturs, kuras jāsniedz ACTA parakstītājām valstīm attiecībā uz personas datu nodošanu

79. EDAU īpaši uzsver, ka starptautiskajā informācijas apmaiņā tiesībaizsardzības iestāžu darbības nolūkā ir īpaši rūpīgi jāievēro datu aizsardzība, jo šāds regulējums var legalizēt

([42]) Eiropas Padomes Konvencija par personu aizsardzību attiecībā uz automātisku personas datu apstrādi, pieņemta Strasbūrā 1981. gada 28. janvārī, Konvencijas par personu aizsardzību attiecībā uz automātisku personas datu apstrādi Papildu protokols par uzraudzības institūcijām un pārrobežu datu plūsmām, Strasbūra, 2001. gada 8. novembris.

([43]) Padomes 2008. gada 27. novembra Pamatlēmums 2008/877/TI par tādu personas datu aizsardzību, kurus apstrādā policijas un tiesiskās sadarbības krimināllietās laikā, OV L 350, 30.12.2008., 60. lpp.

([44]) Skatīt atbildes uz Eiropas Parlamenta jautājumiem komisāra amata pretendentei *Viviane Reding*, 5. lpp., http://www.europarl.europa.eu/hearings/static/commissioners/answers/reding_replies_en.pdf

([45]) Rezolūcija tika pieņemta 2009. gada novembrī Madridē.

([46]) Piemēram, Eiropola un *Eurojust* nolīgums ar ASV, *PNR* nolīgums, *SWIFT* nolīgums, nolīgums starp ES un Austrāliju par pasažieru, kas izceļo no Eiropas Savienības, datu reģistra *(PNR)* apstrādi un nodošanu, ko veic gaisa pārvadātāji Austrālijas muitas dienestam.

masveida informācijas apmaiņu kādā jomā, kurā tas var ļoti nopietni ietekmēt personas un kurā vēl joprojām nav stingru un uzticamu garantiju.

80. EDAU norāda, ka konkrētus nosacījumus un garantijas var formulēt tikai katrā noteiktā gadījumā, pamatojoties uz visām datu apmaiņas īpatnībām. Vadlīniju nolūkā EDAU tomēr vēlas minēt dažus principus un garantijas, kuras būtu jāsniedz trešām pusēm saņēmējām, lai varētu notikt datu apmaiņa:

— ir jāpārbauda tiesiskais pamatojums, saskaņā ar kuru notiek datu apstrādes darbības (t. i., vai datu apstrādes pamatā ir tiesisks pienākums, datu subjektu piekrišana vai arī jebkāds cits derīgs pamatojums) un vai datu nodošana atbilst sākotnējam datu vākšanas mērķim. Datus nedrīkst nodot, ja tas neatbilst paredzētajam mērķim,

— ir skaidri jānorāda personas datu, kurus nepieciešams nodot, apjoms un veidi, un var nodot tikai tādu datu apjomu, kāds ir vajadzīgs datu nodošanas mērķa sasniegšanai. Savāktie un nodotie dati jo īpaši var ietvert interneta lietotāju IP adreses, iespējamā nodarījuma datumu un laiku, nodarījuma veidu. EDAU iesaka izmeklēšanas posmā nesasaistīt datus ar kādu konkrētu personu un atgādina, ka aizdomās turamo personības noskaidrošana var notikt tikai saskaņā ar likumu un tiesneša uzraudzībā. Šajā sakarībā EDAU norāda, ka dati saistībā ar intelektuālā īpašuma tiesību pārkāpumiem un aizdomām par pārkāpumiem ir īpaša datu kategorija, kuras apstrādi parasti var veikt tikai tiesībaizsardzības iestādes, un šādiem datiem ir jānosaka papildu garantijas. Tādēļ saskaņā ar spēkā esošajiem datu aizsardzības likumiem ir precīzi jādefinē personas, kuras ir pilnvarotas apstrādāt datus saistībā ar intelektuālā īpašuma tiesību pārkāpumiem un aizdomām par pārkāpumiem, kā arī šādu datu apstrādes nosacījumi,

— ir skaidri jānosaka personas, starp kurām var notikt datu apmaiņa, un būtībā ir jāaizliedz datu tālāknodošana citiem saņēmējiem, ja vien šāda tālāknodošana nav vajadzīga īpašai izmeklēšanai. Šis ierobežojums ir jo īpaši izšķirīgs, jo ieceltie saņēmēji nedrīkst neatļauti apmainīties ar informāciju, nododot to saņēmējiem, kuriem nav attiecīgu pilnvaru,

— EDAU pieņem, ka *ACTA* tiks noteikta ne tikai sadarbība starp valsts iestādēm, bet arī nolīguma īstenošanas uzdevumi privātām organizācijām (piemēram, interneta pakalpojumu sniedzējiem, autortiesību turētāju organizācijām utt.). Šādā gadījumā ir rūpīgi jāizvērtē privāto organizāciju iesaistīšanas intelektuālā īpašuma tiesību īstenošanā nosacījumi un apmērs, jo *ACTA* pasākumi nevar piešķirt *de facto* tiesības interneta pakalpojumu sniedzējiem un autortiesību turētāju organizācijām uzraudzīt lietotāju darbību tiešsaistē. Turklāt privātas organizācijas personas datu apstrādi tiesībaizsardzības mērķu nolūkā drīkst veikt tikai saskaņā ar atbilstošu tiesisko pamatu. Tāpat arī ir svarīgi noskaidrot, vai privātajām organizācijām būs pienākums sadarboties ar policiju, un šādas sadarbības apmēru. Šāda sadarbība jebkurā gadījumā var attiekties tikai uz smagiem noziedzīgiem nodarījumiem, kuri arī ir precīzi jādefinē, jo ne visus intelektuālā īpašuma tiesību pārkāpumus var uzskatīt par smagiem noziedzīgiem nodarījumiem,

— ir skaidri jāizvēlas personas datu apmaiņas metode, jo īpaši jānorāda, vai tā tiks veikta, izmantojot filtrēšanas sistēmu, piemēram, interneta pakalpojumu sniedzēji un autortiesību turētāju organizācijas kontrolēti nodos noteiktus datus trešām pusēm, kā policijai un citām tiesībaizsardzības iestādēm ārvalstīs, vai arī tiešās piekļuves sistēmu, piemēram, policijai un tiesībaizsardzības iestādēm, būs tieša piekļuve privātu pušu datu bāzēm vai datubāzēm, kurās centralizēti glabā informāciju. Kā jau ir minēts *PNR* kontekstā, filtrēšanas sistēma ir vienīgā iespēja, kas atbilst datu aizsardzības principiem datu aizsardzības ES kontekstā, jo tā nodrošina tiesības nosūtītājam no ES, kas, visticamāk, būs datu apstrādātājs, uzraudzīt datu nodošanu ([47]),

— ir jānorāda termiņš, cik ilgi saņēmēji var glabāt personas datus, kā arī mērķi, kādēļ ir vajadzīga šāda glabāšana. Šādam glabāšanas termiņam ir jābūt samērīgam ar sasniedzamo mērķi, kas nozīmē, ka dati ir jāizdzēš vai jāizniīcina, tiklīdz tie vairs nav vajadzīgi norādītā mērķa sasniegšanai,

— ir skaidri jānosaka pienākumi, kas jāpilda datu apstrādātājiem trešās valstīs. Ir jāgarantē kontroles un/vai īstenojami atbildības uzņemšanās pasākumi, lai datu apstrādātājiem varētu piemērot efektīvus tiesību aizsardzības līdzekļus un sankcijas nelikumīgas apstrādes vai citu attiecīgu incidentu gadījumā. Turklāt vajadzētu izstrādāt

([47]) Skatīt 29. panta darba grupas atzinumu 4/2003 par ASV nodrošināto aizsardzības līmeni pasažieru datu nodošanas nolūkā, WP78, 2003. gada 13. jūnijs.

kompensāciju mehānismus, lai personas varētu iesniegt sūdzību neatkarīgai datu aizsardzības iestādei un īstenot efektīvu tiesību aizsardzību neatkarīgā un objektīvā tiesu iestādē, ([48])

— pušu parakstītajos dokumentos vajadzētu skaidri norādīt datu subjektu tiesības attiecībā uz viņu personas datiem, ja šādus datus apstrādā saņēmējs trešā puse, lai garantētu viņiem efektīvus savu tiesību īstenošanas līdzekļus saistībā ar ārvalstīs veicamu datu apstrādi,

— ļoti svarīga ir arī pārredzamība, un datu aizsardzības vienošanās pusēm ir jāvienojas par to, kā tās informēs datu subjektus par notiekošo datu apstrādi, viņu tiesībām un to, kā tās īstenot.

VI. **SECINĀJUMI**

81. EDAU stingri mudina Eiropas Komisiju nodrošināt atklātu un pārredzamu dialogu par *ACTA*, iespējams, rīkojot atklātas konsultācijas, kas palīdzētu arī nodrošināt veicamo pasākumu atbilstību ES privātuma un datu aizsardzības tiesību aktu prasībām.

82. EDAU aicina Eiropas Komisiju sarunu par *ACTA* laikā rast pareizu līdzsvaru starp intelektuālā īpašuma tiesību aizsardzības vajadzībām un tiesībām uz privātumu un datu aizsardzību. EDAU uzsver, ka ir īpaši svarīgi ņemt vērā privātumu un datu aizsardzību jau pašā sarunu sākumā pirms vienošanās par jebkādiem pasākumiem, lai vēlāk nevajadzētu meklēt alternatīvus privātuma ievērošanai atbilstošus risinājumus.

83. Protams, intelektuālā īpašuma tiesības ir svarīgas sabiedrībai un tās ir jāaizsargā, taču tās nevar būt svarīgākas par personu pamattiesībām uz privātumu, datu aizsardzību un citām tiesībām, kā vainas prezumpcija, efektīva tiesiskā aizsardzība un vārda brīvība.

84. Tiktāl, ciktāl pašreizējais *ACTA* projekts ietver vai vismaz netieši paredz interneta atslēgšanas par trim pārkāpumiem kārtību, *ACTA* ievērojami ierobežotu Eiropas pilsoņu pamattiesības un brīvības, jo īpaši personas datu un privātuma aizsardzību.

85. EDAU neuzskata, ka interneta atslēgšanas par trim pārkāpumiem kārtība būtu vajadzīga intelektuālā īpašuma tiesību īstenošanas mērķa sasniegšanai. EDAU ir pārliecināts, ka pastāv alternatīvi mazāk agresīvi risinājumi vai vismaz paredzēto kārtību var īstenot mazāk agresīvā veidā vai ierobežotākā apmērā, jo īpaši veicot speciālu mērķtiecīgu uzraudzību.

86. Interneta atslēgšanas par trim pārkāpumiem kārtība ir problemātiska arī plašākā tiesiskā izpratnē, jo tiesu datu apstrādei, jo īpaši no privātu organizāciju puses, ir jābūt pienācīgam tiesiskam pamatojumam. Trīs pārkāpumu plāna ieviešana var radīt pamatu ilgākai *log* datņu glabāšanai, kas ir pretrunā spēkā esošajiem tiesību aktiem.

87. Turklāt EDAU aicina Eiropas Savienību ieviest atbilstošas garantijas tiktāl, ciktāl *ACTA* ietver personas datu apmaiņu starp valsts iestādēm un/vai privātām organizācijām, kas atrodas parakstītājās valstīs. Šīs garantijas ir attiecināmas uz visu datu apmaiņu saistībā ar *ACTA* neatkarīgi no tā, vai datu apmaiņa notiek civiltiesiskajā, krimināltiesiskajā vai elektroniskās uzraudzības jomā, un tām ir jāatbilst Konvencijā Nr. 108 un Direktīvā 95/46/EK paredzētajiem datu aizsardzības principiem. EDAU iesaka nodrošināt šādas garantijas, parakstot saistošus nolīgumus starp ES datu nosūtītājiem un to saņēmējiem trešās valstīs.

88. EDAU aicina turpmāk konsultēties ar viņu par pasākumiem, kas tiks veikti saistībā ar datu apmaiņu saskaņā ar *ACTA*, lai būtu iespējams pārliecināties par pasākumu samērīgumu un to, vai šie pasākumi garantē atbilstošu datu aizsardzības līmeni.

Briselē, 2010. gada 22. februārī

Peter HUSTINX

Eiropas Datu aizsardzības uzraudzītājs

([48]) Skatīt Eiropas Datu aizsardzības uzraudzītāja atzinumu par ES – ASV augsta līmeņa kontaktgrupas par informācijas apmaiņas, privātuma un personas datu aizsardzības jautājumiem gala ziņojumu, 11.11.2008.