

I

(Rezoliucijos, rekomendacijos ir nuomonės)

NUOMONĖS

EUROPOS DUOMENŲ APSAUGOS PRIEŽIŪROS
PAREIGŪNASEuropos duomenų apsaugos priežiūros pareigūno nuomonė dėl šiuo metu vykstančių Europos
Sąjungos derybų dėl Kovos su klastojimu prekybos susitarimo (ACTA)

(2010/C 147/01)

EUROPOS DUOMENŲ APSAUGOS PRIEŽIŪROS PAREIGŪNAS,

atsižvelgdamas į Sutartį dėl Europos Sąjungos veikimo, ypač į jos 16 straipsnį,

atsižvelgdamas į Europos Sąjungos pagrindinių teisių chartiją, ypač į jos 8 straipsnį,

atsižvelgdamas į 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyvą 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ⁽¹⁾,

atsižvelgdamas į 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyvą 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje ⁽²⁾,

atsižvelgdamas į 2000 m. gruodžio 18 d. Europos Parlamento ir Tarybos reglamentą (EB) Nr. 45/2001 dėl asmens apsaugos Bendrijos institucijoms ir įstaigoms tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo, ypač į jo 41 straipsnį ⁽³⁾,

PRIĖMĖ ŠIĄ NUOMONĘ:

I. ĮVADAS

1. Europos Sąjunga dalyvauja derybose dėl Kovos su klastojimu prekybos susitarimo (ACTA) projekto. Šias derybas 2007 m. pradėjo suinteresuotųjų šalių iniciatyvinė grupė, o vėliau tęsė daugiau dalyvių; tarp jų yra Australija, Kanada, Europos Sąjunga, Japonija, Korėja, Meksika, Marokas,

Naujoji Zelandija, Singapūras, Šveicarija ir Jungtinės Valstijos. Europos Komisija gavo Tarybos įgaliojimus pradėti šias derybas 2008 m.

2. Europos duomenų apsaugos priežiūros pareigūnas (EDAPP) pripažįsta, kad tarptautinė prekyba suklastotomis ir piratinėmis prekėmis, kuri dažnai susijusi su nusikaltėlių tinklais, kelia vis didesnį susirūpinimą, todėl, siekiant kovoti su šios rūšies nusikalstamumu, tarptautiniu lygmeniu reikia taikyti atitinkamus bendradarbiavimo mechanizmus.
3. EDAPP pabrėžia, kad dėl Europos Sąjungos derybų dėl daugiašalio susitarimo, kurio pagrindinis dalykas – intelektinės nuosavybės teisių įgyvendinimas, kyla svarbių klausimų, susijusių su priemonių, kurių imtasi kovai su klastojimu ir piratavimu, poveikiu asmenų pagrindinėms teisėms, visų pirma jų teisei į privatumą ir duomenų apsaugą.
4. Šiuo atžvilgiu EDAPP ypač apgailestauja, kad Europos Komisija su juo nepasikonsultavo dėl šio susitarimo turinio. Todėl EDAPP, veikdamas savo iniciatyva, priėmė šią nuomonę, pagrįstą Reglamento (EB) Nr. 45/2001 41 straipsnio 2 dalimi, kad patartų Komisijai su privatumu ir duomenų apsauga susijusiais aspektais, į kuriuos reikėtų atsižvelgti derybose dėl ACTA.

II. ESAMA PADĖTIS IR NUMATOMAS ACTA TURINYS

5. 7-asis derybų raundas siekiant 2010 m. sudaryti susitarimą įvyko 2010 m. sausio 26–29 d. Meksikoje. Tačiau iki šiol oficialus susitarimo projektas dar nepaskelbtas.

⁽¹⁾ OL L 281, 1995 11 23, p. 31.

⁽²⁾ OL L 201, 2002 7 31, p. 37.

⁽³⁾ OL L 8, 2001 1 12, p. 1.

6. Derybomis siekiama priimti naują daugiašalį susitarimą, skirtą stiprinti intelektinės nuosavybės teisių (INT) įgyvendinimą ir kovoti su klastojimu bei piratavimu. Jei šis naujas susitarimas bus priimtas, juo bus sukurti geresni tarptautiniai standartai, kuriais nustatoma, kaip kovoti su didelio masto INT pažeidimais. Europos Komisijos Prekybos generalinis direktoratas visų pirma pabrėžė, kad „daugiausia dėmesio ketinama skirti reikšmingos įtakos prekybos interesams turinčiai klastojimo ir piratavimo, o ne eilinių piliečių veiklai“⁽⁴⁾.

7. Kalbant apie susitarimo turinį, 2009 m. lapkričio mėn. Europos Komisijos Prekybos generalinio direktorato išleistoje „Pagrindinių aptariamų dalykų santraukoje“ matyti, kad ACTA kovos su piratavimu ir klastojimu tikslo bus siekiama trimis pagrindinėmis priemonėmis: i) tarptautiniu bendradarbiavimu; ii) įgyvendinimo praktika ir iii) INT įgyvendinimui skirtos teisinės bazės apibrėžimu keliose nustatytose srityse, visų pirma skaitmeninėje aplinkoje⁽⁵⁾. Numatytomis priemonėmis visų pirma bus reglamentuojamos teisinės procedūros (pvz., draudimai, laikinosios priemonės), interneto paslaugų teikėjų (IPT) vaidmuo bei išpaigojimai atgrasant nuo autorių teisių pažeidimų internete ir tarptautinio bendradarbiavimo priemonės siekiant užkirsti prekių vežimą iš vienos šalies į kitą. Tačiau paviešinta informacija susijusi tik su bendrais susitarimo ypatumais ir jokios specifinės bei konkrečios priemonės joje nedetalizuojamos.

8. EDAPP pažymi, kad net jei numatytas ACTA tikslas – kovoti tik su didelio masto INT pažeidimais, negalima atmesti, kad į ACTA taikymo sritį gali patekti ir eilinių piliečių veikla, visų pirma dėl to, kad įgyvendinimo priemonės taikomos skaitmeninėje aplinkoje. EDAPP pažymi, kad tam reikės nustatyti tinkamas pagrindinių asmenų teisių apsaugos garantijas. Be to, duomenų apsaugos teisės aktai apima visus asmenis, įskaitant ir tuos, kurie gali būti susiję su klastojimo ir piratavimo veikla; kova su didelio masto pažeidimais neabejotinai taip pat bus susijusi su asmens duomenų tvarkymu.

9. Šiuo atžvilgiu EDAPP labai rekomenduoja Europos Komisijai vesti viešą ir skaidrų dialogą dėl ACTA, galbūt surengti viešą konsultaciją, nes tai taip pat padėtų užtikrinti, kad priemonės, kurių bus imtasi, atitinka ES privatumo ir duomenų apsaugos teisės reikalavimus.

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

⁽⁵⁾ Žr. 2 išnašą.

III. EDAPP PASTABŲ TAIKYMO SRITIS

10. EDAPP aktyviai ragina ES, visų pirma Europos Komisiją, gavusią įgaliojimus sudaryti susitarimą, užtikrinti tinkamą pusiausvyrą tarp reikalavimų apsaugoti intelektinės nuosavybės teises ir asmenų privatumo bei duomenų apsaugos teisių.

11. EDAPP pabrėžia, kad privatumas ir duomenų apsauga yra pagrindinės Europos Sąjungos vertybės, pripažįstamos EŽTK 8 straipsnyje bei ES pagrindinių teisių chartijos⁽⁶⁾ 7 ir 8 straipsniuose, ir šių vertybių būtina paisyti vykdam bet kokią politiką ir taikant visas taisykles, kurias ES priėmė vadovaudamasi Sutarties dėl Europos Sąjungos veikimo (SESV) 16 straipsniu.

12. Be to, EDAPP pabrėžia, kad bet koks Europos Sąjungos susitarimas dėl ACTA privalo atitikti privatumo ir duomenų apsaugos teisės srityje Europos Sąjungai nustatytus įpareigojimus, visų pirma įtvirtintus Direktyvoje 95/46/EB, Direktyvoje 2002/58/EB⁽⁷⁾ ir Europos Žmogaus Teisių Teismo⁽⁸⁾ bei Teisingumo Teismo⁽⁹⁾ jurisprudencijoje.

13. Į privatumą ir duomenų apsaugą būtina atsižvelgti nuo pat derybų pradžios, o ne tada, kai schemos ir procedūros jau apibrėžtos ir suderintos ir todėl per vėlu ieškoti alternatyvių, privatumą atitinkančių, sprendimų.

14. Atsižvelgdamas į tai, kad viešai prieinama labai nedaug informacijos, EDAPP pažymi, kad negali pateikti konkrečių ACTA nuostatų analizės. Todėl šioje nuomonėje EDAPP daugiausia dėmesio skirs aprašyti tikėtinas grėsmes saugumui ir duomenų apsaugai, kurių gali kilti dėl galimų konkrečių susitarimo priemonių, šiose dvejose srityse: intelektinės nuosavybės teisių įgyvendinimo skaitmeninėje aplinkoje (IV skyrius) ir tarptautinio bendradarbiavimo mechanizmų (V skyrius).

⁽⁶⁾ Europos Sąjungos pagrindinių teisių chartija, OL C 303, 2007 12 14, p. 1.

⁽⁷⁾ 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių) OL L 201, 2002 7 31, p. 37.

⁽⁸⁾ 1950 m. lapkričio 4 d. Romoje priimtos Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos (EŽTK) 8 straipsnyje nustatytų pagrindinių elementų ir sąlygų aiškinimas pagal tai, kaip jie taikomi įvairiose srityse. Visų pirma žr. toliau šioje nuomonėje nurodytą teismo praktiką.

⁽⁹⁾ Visų pirma žr. bylą C-275/06, *Productores de Música de España (Promusicae)*, Rink. p. I-271, [2008] ir bylą C-557/07, *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten*, dar nepaskelbtą Rinkinyje.

IV. INTELEKTINĖS NUOSAVYBĖS TEISIŲ ĮGYVENDINIMAS SKAITMENINĖJE APLINKOJE

IV.1. Poreikis nagrinėti „interneto atjungimo po trijų įspėjimų politikos“ poveikį privatumui ir (arba) duomenų apsaugai

15. Europos Komisijos teigimu, ACTA pagrindu bus sukurta kovos su piratavimu skaitmeninėje aplinkoje teisinė bazė⁽¹⁰⁾. Šioje bazėje bus nustatytos sąlygos, kuriomis IPT ir kiti interneto tarpininkai⁽¹¹⁾ gali būti laikomi atsakingais dėl to, kad per jų įrenginius pateikiama medžiaga, kurios autorių teisės saugomos ir pažeistos. Šioje bazėje taip pat gali būti numatytos priemonės ir teisių įgyvendinimo mechanizmai, taikytini interneto naudotojams pažeidžiant autorių teises išsiuntus ar parsisiuntus medžiagos. Nors išsamiai apie šią bazę oficialiai dar neskelbiama, atsižvelgiant į iš įvairių šaltinių prieinamą informaciją galima numatyti, kad ji gali apimti įpareigojimų nustatymą IPT taikyti „interneto atjungimo po trijų įspėjimų“ politiką, dar vadinamą „laispniškos reakcijos“ schema. Dėl tokių schemų autorių teisių turėtojai galės kontroliuoti interneto naudotojus ir nustatyti įtariamus autorių teisių pažeidėjus. Susisiekus su įtariamo pažeidėjo IPT, šis įspėtų naudotoją, kuris nustatytas kaip pažeidėjas; po pirmųjų trijų įspėjimų jam būtų atjungta interneto prieiga.

16. Tuo metu, kai vyksta derybos dėl ACTA, kai kuriose valstybėse narėse, pavyzdžiui, Prancūzijoje, įgyvendinama interneto atjungimo po trijų įspėjimų politika. Ši politika taip pat aptariama įvairiuose ES forumuose, kaip antai Suinteresuotųjų asmenų dialoge dėl neteisėto įkėlimo ir parsisiuntimo, šiuo metu šių forumų moderatorius yra Vidaus rinkos ir paslaugų generalinis direktoratas, ir jie susiję su Komisijos komunikato dėl didesnės intelektinės nuosavybės teisių apsaugos vidaus rinkoje⁽¹²⁾ priėmimu. Šia tema diskutuojama ir Europos Parlamente, tebevykstant debatams dėl Europos Parlamento rezoliucijos dėl didesnės intelektinės nuosavybės teisių apsaugos vidaus rinkoje projekto (vadinamos M. Gallo pranešimu).

17. Tokia praktika itin kišamasi į privačią asmens sritį. Ji susijusi su bendru interneto naudotojų veiklos stebėjimu, įskai-

⁽¹⁰⁾ Žr. 2 išnašą.

⁽¹¹⁾ Įvairūs interneto tarpininkai gali būti apibrėžiami pagal jų vykdomas funkcijas. Tačiau tikrovėje tarpininkai paprastai vykdo kelias tokias funkcijas. Interneto tarpininkai apima: a) *prieigos teikėjus*: naudotojai prie tinklo prisijungia, prisijungdami prie prieigos teikėjo serverio; b) *tinklo teikėjus*: šie pateikia maršruto parinktuvus, t. y. duomenims perduoti būtiną techninę įrangą; c) *serverio teikėjus*: jie nuomoja vietą savo serveryje, kur naudotojai ar turinio teikėjai gali įkelti turinį. Naudotojai gali įkelti ir parsisiųsti medžiagą naudodamiesi interneto paslauga, pvz., elektronine skelbimų lenta arba P2P tinklais.

⁽¹²⁾ Komisijos komunikatas Tarybai, Europos Parlamentui ir Europos ekonomikos ir socialinių reikalų komitetui. Didesnė intelektinės nuosavybės teisių apsauga vidaus rinkoje, Briuselis, 2009 m. rugsėjo 11 d., COM(2009) 467 galutinis.

tant visiškai teisėtą veiklą. Ji turi įtakos milijonams įstatymų besilaikančių interneto naudotojų, įskaitant daugelį vaikų ir paauglių. Šią veiklą atlieka privatus asmenys, o ne teisėsaugos institucijos. Be to, dabar beveik visose šiuolaikinio gyvenimo srityse interneto vaidmuo yra svarbiausias, todėl atjungimo nuo interneto pasekmės gali būti neįtikėtinais liūdnomis, asmenys gali būti atskirti nuo darbo, kultūros, e. valdžios programų ir kt.

18. Tokiomis aplinkybėmis svarbu įvertinti, kiek ši politika atitinka ES duomenų apsaugos ir privatumo teisės aktus, be to, ar interneto atjungimo po trijų įspėjimų politika yra būtina intelektinės nuosavybės teisių įgyvendinimo priemonė. Tokiomis aplinkybėmis dar reikėtų išanalizuoti, ar yra kitų, ne tokių agresyvių, metodų.

19. Vis dar neaišku, ar interneto atjungimo po trijų įspėjimų politika bus įtraukta į ACTA. Tačiau ši politika svarstoma ir kitose srityse, ir ji gali turėti didžiulį poveikį asmens duomenų ir privatumo apsaugai. Dėl šių priežasčių EDAPP mano, kad šioje nuomonėje reikia aptarti šią politiką. Prieš atlikdamas minėtą analizę, EDAPP trumpai apibūdins taikytinus duomenų apsaugos ir privatumo teisės aktus.

20. Reikėtų pažymėti, kad, be duomenų apsaugos ir privatumo, interneto atjungimo po trijų įspėjimų politika kelia rūpestį dėl kitų vertybių, kaip antai tinkamo proceso ir žodžio laisvės. Tačiau šioje nuomonėje bus išnagrinėti tik tie klausimai, kurie susiję su asmens duomenų ir asmens privatumo apsauga.

IV.2. Interneto atjungimo po trijų įspėjimų politika bei ES duomenų apsaugos ir (arba) privatumo teisės aktų taikymas

Kaip gali būti suformuluota interneto atjungimo po trijų įspėjimų politika

21. Trumpai tariant, pagal interneto atjungimo po trijų įspėjimų politiką autorių teisių turėtojai, naudodamiesi automatinėmis techninėmis priemonėmis, kurias galbūt teiktų tretieji asmenys, galėtų įtariamą autorių teisių pažeidimą nustatyti stebėdami interneto naudotojų veiklą, pavyzdžiui, forumus,

tinklaraščius, arba apsimetę rinkmenų bendrintojais lygiaranguose tinkluose, kad nustatytų rinkmenų bendrintojus, kurie, kaip įtariama, keičiasi autorių teisių saugoma medžiaga⁽¹³⁾.

22. Surinkę interneto naudotojų, kaip įtariama, pažeidžiančių autorių teises, interneto protokolo adresus (IP adresus) ir taip juos nustatę, autorių teisių turėtojai išsiųstų šių naudotojų IP adresus atitinkamam (-iems) interneto paslaugų teikėjui (-ams), kuris (-ie) abonentą, kuriam priklauso IP adresas, išpėtų, jog jis gali būti pažeidęs autorių teises. Gavus tam tikrą skaičių IPT išpėjimų, IPT automatiškai nutraukia arba sustabdo abonto interneto ryšį⁽¹⁴⁾.

Taikytini duomenų apsaugos ir (arba) privatumo ES teisės aktai

23. Interneto atjungimo po trijų išpėjimų politika turi atitikti reikalavimus, kylančius iš teisės į privatumą, nustatytos EŽTK 8 straipsnyje bei Pagrindinių teisių chartijos 7 straipsnyje, ir iš teisės į duomenų apsaugą, nustatytos Pagrindinių teisių chartijos 8 straipsnyje bei SESV 16 straipsnyje ir išsamiai apibrėžtos Direktyvoje 95/46/EB bei Direktyvoje 2002/58/EB.

24. EDAPP nuomone, interneto naudotojų elgesio stebėjimas ir paskesnis jų IP adresų surinkimas prilygsta jų teisės į privataus gyvenimo gerbimą ir susirašinėjimo slaptumą ribojimui, kitaip tariant, ribojama jų teisė į privatų gyvenimą. Šis požiūris atitinka Europos Žmogaus Teisių Teismo praktiką⁽¹⁵⁾.

25. Direktyva 95/46/EB yra taikytina⁽¹⁶⁾, nes interneto atjungimo po trijų išpėjimų politika susijusi su IP adresų, kurie bet kuriuo atveju atitinkamomis aplinkybėmis turėtų būti

⁽¹³⁾ P2P technologija – tai paskirstytoji programinės įrangos sistema, kurią naudojant atskiri kompiuteriai gali prisijungti prie kitų kompiuterių ir palaikyti su jais tiesioginį ryšį.

⁽¹⁴⁾ Tarp alternatyvių sankcijų galėtų būti interneto ryšio funkcijos ribojimas, pvz., ryšio greičio, apimties ir kt. ribojimas.

⁽¹⁵⁾ Visų pirma žr. 2006 m. birželio 26 d. EŽTT sprendimo *Weber and Saravia v. Germany* (dec.), Nr. 54934/00, 77 punktą ir 2008 m. liepos 1 d. EŽTT sprendimą *Liberty and others v the UK*, Nr. 58243/00.

⁽¹⁶⁾ Teisingumo Teismas laikosi plataus požiūrio į Direktyvos 95/46/EB taikytinumą, šios direktyvos nuostatos turi būti aiškinamos atsižvelgiant į EŽTK 8 straipsnį. Savo 2003 m. gegužės 20 d. sprendimo *Rundfunk*, sujungtos bylos C-465/00, C-138/01 ir C-139/01, Rink. p. I-4989, 68 punkte Teisingumo Teismas nurodė, kad „Direktyvos Nr. 95/46/EB nuostatos, reglamentuojančios asmens duomenų, galinčių pažeisti pagrindines laisves, ypač teisę į privatų gyvenimą, tvarkymą, turi būti būtinai aiškinamos atsižvelgiant į pagrindines teises, kurios pagal nusistovėjusią teismo praktiką yra bendrų teisės principų, kurių laikymąsi užtikrina Teisingumo Teismas, dalis“.

laikomi asmens duomenimis, tvarkymu. IP adresai – tai identifikatoriai, kurie atrodo kaip taškais atskirtų skaičių serija, pvz., 122.41.123.45. Prisiregistravęs pas interneto prieigos teikėją abonentas įgyja galimybę naudotis internetu. Kiekvieną kartą abonentui prisijungiant prie interneto per jo naudojamą prisijungimo prie interneto įrenginį (pvz., kompiuterį) jam bus priskiriamas IP adresas⁽¹⁷⁾.

26. Jei naudotojas užsiima konkrečia veikla, pvz., įkelia medžiagą į internetą, tretieji asmenys gali ją nustatyti pagal jo naudotą IP adresą. Pavyzdžiui, naudotojas, kurio IP adresas yra 122.41.123.45, 2010 m. sausio 1 d. 15 val., pasinaudodamas P2P paslauga, kaip įtariama, įkėlė medžiagą, kurios autorių teisės yra pažeistos. Tuomet IPT galės prijungti tokį IP adresą prie abonto, kuriam jis priskyre šį adresą, vardo ir taip išsiaiškinti jo tapatybę.

27. Jei atsižvelgtume į Direktyvos 95/46/EB 2 straipsnyje pateiktą asmens duomenų apibrėžtį, asmens duomenys reiškia „bet kurią informaciją, susijusią su asmeniu (duomenų subjektu), kurio tapatybė yra nustatyta arba gali būti nustatyta; asmuo, kurio tapatybė gali būti nustatyta, yra tas asmuo, kurio tapatybė gali būti nustatyta tiesiogiai ar netiesiogiai, ypač pasinaudojus nurodytu asmens identifikavimo kodu“⁽¹⁸⁾, galima padaryti tik tokią išvadą, kad IP adresai ir informacija apie su tokiais adresu susietą veiklą yra asmens duomenys visais šioje nuomonėje aktualiais atvejais. Iš tikrųjų IP adresas yra identifikacinis numeris, pagal kurį galima sužinoti abonto, kuriam priskirtas šis IP adresas, vardą. Be to, apie tokį IP adresą turintį abonentą surinkta informacija („2010 m. sausio 1 d. 15.00 val. jis įkėlė tam tikrą medžiagą į ZS interneto svetainę“) susijusi su asmens, kurio tapatybę galima nustatyti (IP adreso turėtojo), veiklą, t. y. neabejotinai yra apie jo veiklą, todėl taip pat turi būti laikoma asmens duomenimis.

⁽¹⁷⁾ IP adresas, kurį IPT priskiria asmeniui, kiekvieną kartą jam naršant internete gali būti tas pats (vadinamasis statinis IP adresas). Kiti IP adresai yra dinaminiai, tai reiškia, kad interneto prieigos teikėjas kiekvieną kartą, kai jo klientai prisijungia prie interneto, jiems priskiria vis kitokį IP adresą. Akivaizdu, kad IPT gali prijungti IP adresą prie abonto paskyros, kuriai IPT priskyre (dinaminį arba statinį) IP adresą.

⁽¹⁸⁾ 26 konstatuojamojoje dalyje ši apibrėžtis papildyta: „kadangi apsaugos principai turi būti taikomi visai informacijai apie asmenį, kurio tapatybė yra nustatyta arba gali būti nustatyta; kadangi norint nustatyti, ar asmens tapatybė gali būti nustatyta, reikėtų atsižvelgti į visas priemones, kuriomis galėtų pasinaudoti duomenų valdytojas ar bet kuris kitas asmuo minėto asmens tapatybei nustatyti; kadangi apsaugos principai netaikomi duomenims, kurie paversti anoniminiais tokiu būdu, kad duomenų subjekto tapatybė nebegalų būti nustatyta; ...“.

28. Šiai nuomonei visiškai pritaria 29 straipsnio darbo grupė, kuri dokumente duomenų apsaugos klausimais, susijusiais su intelektinės nuosavybės teisėmis, nurodė, kad IP adresai, surinkti siekiant apginti intelektinės nuosavybės teises, t. y. nustatyti interneto naudotojų, kurie įtariamai pažeidę intelektinės nuosavybės teises, tapatybę, yra asmens duomenys, jei konkretaus asmens atžvilgiu jie naudojami tokioms teisėms ginti⁽¹⁹⁾.
29. Direktyva 2002/58/EB taip pat taikytina, nes interneto atjungimo po trijų išpėjimų politika susijusi su srauto ir ryšių duomenų rinkimu. Direktyvoje 2002/58/EB reglamentuojamas tokių duomenų naudojimas ir nustatomas viešųjų ryšių tinklais perduodamų pranešimų ir šiuose pranešimuose esančių duomenų konfidencialumo principas.

vyrą, vertinant ją demokratinėje visuomenėje apskritai⁽²²⁾. Be to, pagal šį principą būtina įvertinti, ar yra galimybė taikyti alternatyvias mažiau ribojančias priemones.

31. Nors EDAPP pripažįsta intelektinės nuosavybės teisių įgyvendinimo svarbą, jis mano, kad tokia interneto atjungimo po trijų išpėjimų politika, kokia žinoma dabar, susijusi su tam tikrais visuotinai taikomais elementais, yra neproporcinga priemonė ir todėl negali būti laikoma būtina. Be to, EDAPP yra įsitikinęs, kad yra alternatyvių mažiau ribojančių sprendimų arba kad numatyta politika gali būti įgyvendinama ne taip ribojant arba būti mažesnės aprėpties. Teisiniu išsamesnio reglamentavimo lygmeniu trijų išpėjimų metodas taip pat kelia problemų. Šios išvados bus paašškintos toliau.

Trijų išpėjimų metodo politika yra neproporcinga

32. EDAPP nori pabrėžti platų nustatytų priemonių poveikį. Šiuo atžvilgiu reikėtų paminėti tokius dalykus:

IV.3. Ar interneto atjungimo po trijų išpėjimų politika yra būtina priemonė

30. EŽTK 8 straipsnyje įtvirtintas būtinumo principas, pagal kurį bet kuri priemonė, kuria pažeidžiama asmenų teisė į privatumą, leidžiama tik tuo atveju, jei tai yra demokratinėje visuomenėje būtina priemonė, atsižvelgiant į šia priemone siekiamą teisėtą tikslą⁽²⁰⁾. Būtinumo principą taip pat galima rasti Direktyvos 7 ir 13 straipsniuose bei Direktyvos 2002/58/EB 15 straipsnyje⁽²¹⁾. Pagal šį principą reikalaujama priemonės proporcingumo analizės, ir ši priemonė turi būti įvertinta atsižvelgiant į susijusių interesų pusiaus-

i) stebėjimas (nepastebėtas) turėtų įtakos milijonams asmenų ir visiems naudotojams, nepaisant to, ar jie yra įtariamieji.

ii) Stebėjimas būtų susijęs su sisteminiu duomenų įrašymu, dėl to žmonės gali būti paduoti į civilinius ar net baudžiamuosius teismus; be to, dėl to kai kuri surinkta informacija būtų vertinama kaip neskelbtina pagal Direktyvos 95/46/EB 8 straipsnį, pagal kurį reikalaujama patikimesnių garantijų.

iii) Dėl stebėjimo gali atsirasti daug klaidingos informacijos atvejų. Autorių teisių pažeidimas nenustatomas taip paprastai, atsakant į klausimą „taip“ arba „ne“. Teismai dažnai turi nagrinėti labai daug techninių ir teisinių duomenų, kad nustatytų, ar pažeidimas buvo padarytas⁽²³⁾.

⁽¹⁹⁾ 29 straipsnio darbo grupė. Darbinis dokumentas dėl duomenų apsaugos klausimų, susijusių su intelektinės nuosavybės teisėmis (WP 104), priimtas 2005 m. sausio 18 d. Ši darbo grupė įkurta pagal Direktyvos 95/46/EB 29 straipsnį. Tai yra nepriklausoma patariamoji Europos institucija duomenų apsaugos ir privatumo klausimais. Jos uždaviniai aprašyti Direktyvos 95/4/EB 6 30 straipsnyje ir Direktyvos 2002/58/EB 15 straipsnyje. Taip pat žr. Darbo grupės nuomonę 4/2007 dėl asmens duomenų sąvokos (WP 136), priimtą 2007 m. birželio 20 d., visų pirma p. 16.

⁽²⁰⁾ EŽTK 8 straipsnyje aiškiai nurodomas reikalavimas, kad bet koks ribojimas turi būti „būtinai demokratinėje visuomenėje“.

⁽²¹⁾ Direktyvos 95/46/EB 13 straipsnyje ribojimas leidžiamas tik jei tai reikalinga priemonė norint užtikrinti: „a) nacionalinį saugumą; b) gynybą; c) visuomenės saugumą; d) kriminalinių nusikaltimų bei reglamentuojamų profesijų etikos pažeidimų prevenciją, tyrimą, išaiškinimą ir persekiojimą; e) svarbius ekonominius ar finansinius valstybės narės ar Europos Sąjungos interesus, įskaitant ir monetarinius, biudžeto ar mokesčių klausimus; f) kontrolės, tikrinimo ar taisyklių nustatymo funkciją, kuri susijusi, bent atsitiktinai, su įgaliojimų vykdymu c, d ir e punktuose nurodytais atvejais; g) duomenų subjekto apsaugą arba kitų asmenų teisių ir laisvių apsaugą“. Direktyvos 2002/58/EB 15 straipsnyje nustatyta, kad „toks ribojimas yra būtina, tinkama ir adekvati demokratinės visuomenės priemonė, skirta apsaugoti nacionalinį saugumą (t. y. valstybės saugumą), gynybą, visuomenės saugumą, taip užkardant, tiriant ir nustatant baudžiamąsias veikas ar neteisėtą elektroninių ryšių sistemos naudojimą, kaip nurodyta Direktyvos 95/46/EB 13 straipsnio 1 dalyje“.

⁽²²⁾ Taip pat žr. 1984 m. rugpjūčio 2 d. EŽTT sprendimo *Malone v. the United Kingdom*, A serija, Nr. 82, p. 32, 81 ir tolesnius punktus, ir 2008 m. gruodžio 4 d. EŽTT sprendimo *Marper v. the United Kingdom* [GC], Nr. 30562/04 ir Nr. 30566/04, 101 ir tolesnius punktus.

⁽²³⁾ Teismams gali tekti įvertinti, ar medžiagai iš tikrųjų taikoma autorių teisių apsauga, kokios teisės buvo pažeistos, ar naudojimas gali būti laikomas sąžiningu, nustatyti taikytiną teisę, žalą ir kt.

- iv) Galimos stebėjimo pasekmės, dėl kurių galėtų būti nutraukta interneto prieiga. Taip būtų ribojamos asmens teisės į nuomonės reiškimo laisvę, informacijos laisvę ir galimybę susipažinti su kultūra, naudotis e. valdžios programomis, forumais, e. paštu, ir kai kuriais atvejais – vykdyti su darbu susijusią veiklą. Šiomis aplinkybėmis ypač svarbu suvokti, kad pasekmes pajus ne tik įtariamasis pažeidėjas, bet ir visi šeimos nariai, kurie naudojami tuo pačiu interneto ryšiu, įskaitant mokyklinio amžiaus vaikus, besinaudojančius internetu savo mokyklinei veiklai.
- v) Paprastai vertinimą atliks ir sprendimą priims privatus subjektas (t. y. autorių teisių turėtojai arba IPT). EDAPP savo ankstesnėje nuomonėje jau išreiškė rūpestį dėl privataus sektoriaus (pvz., IPT ar autorių teisių turėtojų) atliekamo asmenų stebėjimo srityse, kurios iš esmės yra teisės saugos institucijų kompetencija ⁽²⁴⁾.
33. EDAPP nėra įsitikinęs, kad priemonių nauda nusveria poveikį pagrindinėms asmenų teisėms. Autorių teisių apsauga yra teisių turėtojų ir visuomenės interesas. Tačiau pagrindinių teisių ribojimai neatrodo pateisinami, jei būtų palygintas ribojimo dydis, t. y. privatumo ribojimo mastas, kurį parodo pirmiau minėti dalykai, ir numatoma nauda – atgrasymas nuo intelektualinės nuosavybės teisių pažeidimų, kai šie pažeidimai daugiausia yra nedidelio masto. Kaip generalinė advokatė J. Kokott nurodė savo išvadoje byloje *Promusicae*: „... nėra aišku, ar keitimasis rinkmenomis tarp privačių subjektų, ypač kai jie veikia nesiekdami pelno, kelia tokią grėsmę autorių teisėms, kad pateisintų šios išimties taikymą. Iš esmės nesutariama, kiek iš tikrųjų žalos padaro keitimasis rinkmenomis tarp privačių subjektų“ ⁽²⁵⁾.
34. Šiomis aplinkybėmis taip pat vertėtų priminti Europos Parlamento reakciją į „trijų išpėjimų schemas“ persvarstant telekomunikacijų teisės aktų paketą, visų pirma Paminėtos direktyvos 138 pakeitimą ⁽²⁶⁾. Šiame pakeitime buvo nustatyta, kad bet kokios pagrindinių teisių ar laisvių ribojimo priemonės gali būti nustatytos tik tuo atveju, jei jos yra tinkamos, proporcingos ir būtinos demokratinėje visuomenėje ir jų įgyvendinimui taikomos tinkamos procedūrinės
- apsaugos garantijos, atitinkančios EŽTK ir bendruosius Bendrijos teisės principus, įskaitant veiksmingą teismingą apsaugą ir teisingą procesą ⁽²⁷⁾.
35. Be to, EDAPP pabrėžia, kad kiekvienas pagrindinių teisių ribojimas bus atidžiai tikrinamas ES ir nacionaliniu lygmenimis. Šiomis aplinkybėmis galima palyginti su Duomenų saugojimo direktyva 2006/24/EB ⁽²⁸⁾, kurioje nukrypstama nuo bendrojo duomenų apsaugos principo – duomenų ištrynimo principo, kai duomenys tampa nebereikalingi tam tikslui, kuriam buvo surinkti. Pagal šią direktyvą reikalaujama, kad srauto duomenys būtų saugomi kovai su sunkiais nusikaltimais. Reikia pažymėti, kad saugojimas leidžiamas tik „sunkių nusikaltimų“ atveju, jis apribojamas tik „srauto duomenimis“, į kuriuos iš esmės nepatenka informacija apie pranešimų turinį, ir kad taikomos griežtos garantijos. Vis dėlto buvo suabejota jos suderinamumu su pagrindinių teisių standartais; Rumunijos Konstitucinis Teismas nusprendė, kad bendras saugojimas nedera su pagrindinėmis teisėmis ⁽²⁹⁾, o Vokietijos Konstituciniame Teisme šiuo metu yra nagrinėjama byla ⁽³⁰⁾.
- Kitų, mažiau ribojančių, priemonių egzistavimas*
36. Pirmiau pateiktas išvadas patvirtina ir tai, kad tam pačiam tikslui pasiekti yra mažiau ribojančių priemonių. EDAPP primygtinai reikalauja iširti ir išbandyti tokias mažiau ribojančias priemones.
- ⁽²⁷⁾ Galutinai vadinamasis 138 pakeitimas suformuluotas taip: „1 straipsnio 3a dalis. Priemonėmis, kurių valstybės narės imasi nustatydamos galutinių paslaugų vartotojų prieigą prie paslaugų bei programinės įrangos ir galimybes jas naudoti elektroninių ryšių tinkluose, gerbiamos fizinį asmenų pagrindinės teisės ir laisvės, garantuojamos Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija ir bendraisiais Bendrijos teisės principais. Šias galutinių paslaugų vartotojų prieigą prie paslaugų bei programinės įrangos ir galimybes jas naudoti elektroninių ryšių tinkluose nustatančias priemones, galinčias apriboti tas pagrindines teises ar laisves, galima nustatyti tik tuo atveju, jei jos yra tinkamos, proporcingos ir būtinos demokratinėje visuomenėje, ir jų įgyvendinimui turi būti taikomos tinkamos procedūrinės apsaugos priemonės, atitinkančios nustatytą Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijoje ir bendruosius Bendrijos teisės principus, įskaitant veiksmingą teismingą apsaugą ir teisingą procesą. Atitinkamai šių priemonių galima imtis tik deramai laikantis nekaltumo prezumpcijos principo ir užtikrinant teisę į privatumą. Turi būti garantuojamas išankstinis teisingas ir nešališkas procesas, įskaitant atitinkamo asmens ar asmenų teisę būti išklausytiems, esant būtinybei – tinkamai pagrįstais skubos atvejais turi būti taikomos atitinkamos sąlygos ir procedūrinės priemonės, atitinkančios nustatytą Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijoje. Turi būti garantuojama veiksminga ir tinkamu laiku atlika teisminė peržiūra.“
- ⁽²⁸⁾ 2006 m. kovo 15 d. Europos Parlamento ir Tarybos direktyva 2006/24/EB, OL L 105, 2006 4 13, p. 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>
- ⁽²⁴⁾ 2008 m. birželio 23 d. EDAPP nuomonė dėl pasiūlymo dėl sprendimo, kuriuo nustatoma daugiametė internetu ir kitomis ryšių technologijomis besinaudojančių vaikų apsaugos Bendrijos programa, OL C 2, 2009 1 7, p. 2.
- ⁽²⁵⁾ Žr. 8 išnašoje nurodytos bylos 106 punktą.
- ⁽²⁶⁾ Žr. 2009 m. lapkričio 25 d. Europos Parlamento ir Tarybos direktyvą 2009/140/EB, OL L 337, 2009 12 18, p. 37.

37. Šiomis aplinkybėmis EDAPP primena, kad iš dalies pakeistoje Direktyvoje 2002/22/EB dėl universaliųjų paslaugų ir paslaugų gavėjų teisių, susijusių su elektroninių ryšių tinklais ir paslaugomis (toliau – Piliiečių teisių direktyva), kuri yra neseniai reformuoto telekomunikacijų teisės akto paketo dalis, yra numatytos tam tikros taisyklės ir procedūros, skirtos riboti nedidelio masto autorių teisių pažeidimus tarp vartotojų⁽³¹⁾. Tokios procedūros apima valstybių narių pareigą pateikti standartizuotą viešojo intereso informaciją įvairiomis temomis, visų pirma paminėti autorių ir gretutinių teisių pažeidimai ir jų teisiniai padariniai⁽³²⁾. Tuomet valstybės narės gali prašyti IPT išplatinti šią informaciją visiems savo klientams ir įtraukti ją į sutartis.

38. Ši sistema skirta informuoti asmenis ir atgrasyti juos nuo autorių teisių saugomos informacijos platinimo bei dalyvavimo neteisėtoje veikloje, kartu išvengiant interneto naudojimo stebėjimo ir su privatumu bei duomenų apsauga susijusių rūpesčių. Piliiečių teisių direktyva turi būti įgyvendinta 2011 m. gegužės mėn.; taigi šios procedūros dar neįgyvendintos. Todėl dar nebuvo galimybių išmėginti jų naudą. Taigi atrodo per anksti neatsižvelgti į galimą šių naujų procedūrų naudą ir vietoj to taikyti „internetu atjungimo po trijų išpėjimų“ politiką, kuri gerokai labiau riboja pagrindines teises.

39. Be to, kas nurodyta pirmiau, reikėtų priminti, kad 2004 m. balandžio 28 d. Direktyvoje 2004/48/EB dėl intelektinės nuosavybės teisių įgyvendinimo numatytos įvairios intelektinės nuosavybės teisių įgyvendinimo teisumuose priemonės (aptartos šios nuomonės 43 ir tolesniuose punktuose)⁽³³⁾.

40. INTI direktyva tik neseniai perkelta į valstybių narių teisę. Iki šiol dar nebuvo pakankamai laiko įvertinti, ar jos nuostatos yra tinkamos intelektinės nuosavybės teisėms

⁽³¹⁾ Žr. 2009 m. lapkričio 25 d. Europos Parlamento direktyvą 2009/136/EB, OL L 337, 2009 12 18, p. 11.

⁽³²⁾ Visų pirma Direktyvos 2009/136/EB 21 straipsnio 4 dalyje numatyta, kad „valstybės narės gali reikalauti, kad 3 dalyje nurodyti ūkio subjektai tam tikrais atvejais esamiems ir būsimiems abonentams nemokamai platintų informaciją apie viešuosius interesus tomis pačiomis priemonėmis, kurias jie paprastai taiko ryšiams su abonentais palaikyti. Tokiu atveju tokią informaciją rengia atitinkamos viešosios institucijos; ji yra standartinės formos ir, *inter alia*, apima šias temas: a) dažniausi elektroninių ryšių paslaugų naudojimo būdai, siekiant dalyvauti neteisėtoje veikloje ar platinti žalingą turinį, ypač jei tokiu būdu gali būti pažeistos kitų asmenų teisės ir laisvės, įskaitant autorių ir gretutinių teisių pažeidimus bei jų teises pasekmes; ...“. Be to, pagal 20 straipsnio 1 dalį „valstybės narės taip pat gali reikalauti, kad sutartyje būtų pateikta 21 straipsnio 4 dalyje nurodyta ir su teikiama paslauga susijusi informacija, kurią šiuo tikslu gali teikti atitinkamos viešosios institucijos, apie elektroninių ryšių tinklų ir paslaugų naudojimą dalyvaujant neteisėtoje veikloje ar platinant žalingą turinį bei apie apsaugos priemones, skirtas nuo pavojų apsaugoti asmenį, jo privatumą ir asmens duomenis“.

⁽³³⁾ OL L 157, 2004 4 30, p. 45 (toliau – INTI direktyva).

ginti. Todėl bet koks poreikis pakeisti dabartinę teismų procesais grindžiamą sistemą, kuri dar neišbandyta, yra bent jau abejotinas. Dėl to neišvengiamai kyla klausimas, kodėl su esamais pažeidimais negalima tinkamai kovoti taikant esamas civilines ir baudžiamąsias sankcijas už autorių teisių pažeidimus. Todėl prieš siūlydama tokias politines priemones Komisija turėtų pateikti patikimą informaciją, įrodančią, kad dabartiniai teisės aktai nepateisino lūkesčių.

41. Be to, neaišku, ar kaip nors rimtai apsvarstyti alternatyvūs ekonominės veiklos modeliai, nesusiję su reguliariu asmenų stebėjimu. Pavyzdžiui, jei dėl P2P naudojimo autorių teisių turėtojai įrodytų savo nuostolius, teisių turėtojai ir IPT galėtų, pavyzdžiui, išbandyti įvairius interneto prieigos abonementus, kai dalis kainos už abonentinę sutartį su neribota interneto prieiga atitenka autorių teisių turėtojams.

Galimybė atlikti tikslinį stebėjimą mažiau ribojančiomis priemonėmis

42. Be visiškai skirtingų modelių, kurie, kaip nurodyta, turėtų būti ištirti ir išbandyti, naudojimo tikslinis stebėjimas bet kuriuo atveju galėtų būti atliekamas mažiau ribojančiomis priemonėmis.

43. Intelektinės nuosavybės teisių įgyvendinimo tikslas taip pat gali būti pasiektas stebint tik ribotą skaičių asmenų, kurie, kaip įtariama, dalyvauja darant ne smulkius autorių teisių pažeidimus. INTI direktyvoje šiuo atžvilgiu pateikiamos tam tikros gairės. Joje nustatytos sąlygos, kuriomis institucijos gali įpareigoti interneto prieigos teikėjus intelektinės nuosavybės teisių įgyvendinimo tikslais atskleisti jų turimus asmens duomenis. 8 straipsnyje numatyta, kad kompetentingos teisminės institucijos, reaguodamos į pagrįstą ir proporcingą prašymą, pažeidimų *komerciniu mastu* atveju gali įpareigoti IPT pateikti jų turimus įtariamų pažeidėjų asmens duomenis (pvz., informaciją apie intelektinės nuosavybės teises pažeidžiančių prekių ar paslaugų kilmę ir platinimo tinklus)⁽³⁴⁾.

44. Taigi „komercinio masto“ kriterijus yra lemiamas. Pagal šį kriterijų stebėjimas gali būti proporcingas ribotais, konkrečiais, *ad hoc* atvejais, kai yra pagrįstų piktnaudžiavimo autorių teisėmis komerciniu mastu įtarimų. Pagal šį

⁽³⁴⁾ Tai tik patvirtinama INTI direktyvos 14 konstatuojamojoje dalyje.

kriterijų tai galėtų apimti aiškias privačių asmenų piktnaudžiavimo autorių teisėmis atvejus, kai siekiama gauti tiesioginės ar netiesioginės ekonominės komercinės naudos.

45. Praktiškai siekiant, kad pirmiau minėta sistema veiktų veiksmingai, autorių teisių turėtojai galėtų vykdyti tikslinį kai kurių IP adresų stebėjimą, kad patikrintų autorių teisių pažeidimo mastą. Tai reikštų, kad autorių teisių turėtojams taip pat būtų leidžiama tokiu pačiu tikslu fiksuoti pranešimus apie įtariamus pažeidimus. Tokia informacija turėtų būti panaudota tik patikrinus pažeidimo reikšmingumą. Pavyzdžiui, taip būtų aiškiais šiurkščių pažeidimų ir nereikšmingų, bet tęstinių pažeidimų, padarytų per tam tikrą laiką siekiant komercinės ar finansinės naudos, atvejais. Tęstinumo tam tikrais laikotarpiais būtinybė pabrėžiama ir išsamiau paaiškinama toliau aptariant saugojimo principą.
46. Tai reikštų, kad tokiais atvejais informacijos rinkimas siekiant įrodyti įtariamą piktnaudžiavimą internetu gali būti laikomas proporcingu ir būtinu siekiant pasirengti teisiniui procesui, įskaitant bylinėjimąsi.
47. EDAPP mano, kad, taikant papildomą garantiją, duomenų tvarkymo operacijos, kuriomis siekiama surinkti tokius įrodymus, turėtų būti iš anksto patikrintos nacionalinių duomenų apsaugos institucijų ir šios turėtų suteikti joms leidimus. Ši nuomonė grindžiama tuo, kad duomenų tvarkymo operacijos keltų konkrečią grėsmę asmenų teisėms ir laisvėms atsižvelgiant į jų tikslus, t. y. teisių gynimą, kuris galėtų būti įgyvendinamas ir baudžiamosiomis priemonėmis, ir atsižvelgiant į neskelbtiną surinktų duomenų pobūdį. Tai, kad tvarkymas susijęs su elektroninių pranešimų stebėjimu, yra dar vienas veiksnys, dėl kurio reikalinga didesnė priežiūra.
48. EDAPP mano, kad INTĮ direktyvoje nustatytas „komercinis mastas“ yra labai tinkamas būdas nustatyti stebėjimo ribas, kad būtų paisoma proporcingumo principo. Be to, neatrodo, kad yra patikimų įrodymų, pagal INTĮ nustatytus kriterijus patvirtinančių, kad realūs teisiniai veiksmai dėl autorių teisių pažeidimo yra neįmanomi ar neveiksmingi. Pavyzdžiui, atrodo, kad Vokietijos pateikta informacija, pagal kurią nuo 2008 m., po INTĮ direktyvos perkėlimo į nacionalinę teisę, išduota maždaug 3 000 teismo įsakymų, pagal kuriuos IPT atskleidė teismams 300 000 abonentų informaciją, rodo priešingai.
49. Apskritai, kadangi INTĮ direktyva galioja dar tik dvejus metus, sunku suvokti, kodėl teisės aktų leidėjai turėtų atsakyti šioje direktyvoje nustatytų kriterijų ir imti taikyti labiau ribojančius metodus, kai ES dar tik pradeda bandyti neseniai patvirtintus metodus. Dėl tos pačios priežasties

sunku suprasti, kam reikia dabartinę teismais grindžiamą sistemą keisti kitomis priemonėmis (be to, kad kyla tinkamo proceso klausimų, kurie čia neaptariami).

IV.4. Interneto atjungimo po trijų įspėjimų politikos atitikties išsamesnėms duomenų apsaugos nuostatoms

50. Yra kitų, konkretesnių, teisinių priežasčių, dėl kurių trijų įspėjimų metodas duomenų apsaugos požiūriu yra problemiškas. EDAPP norėtų pabrėžti abejotiną tvarkymo teisinių pagrindą, kurio reikalaujama Direktyvoje 95/46/EB, ir Direktyvoje 2002/58/EB įtvirtintą pareigą naikinti registracijos bylas.

Tvarkymo teisinis pagrindas

51. Trijų įspėjimų metodo schemas susijusios su asmens duomenų tvarkymu, kai kurie iš šių duomenų bus panaudoti teisinėse ar administracinėse procedūrose siekiant pakartotiniams pažeidėjams atjungti interneto prieigą. Šiuo požiūriu tokie duomenys pagal Direktyvos 95/46/EB 8 straipsnį laikytini neskelbtiniais. 8 straipsnio 5 dalyje nustatyta, kad „duomenys, susiję su nusikaltimais, nuteisimais ar valstybės saugumo priemonėmis, gali būti tvarkomi tik tuo atveju, jeigu tai kontroliuoja oficiali valdžios institucija arba jeigu nacionaliniai įstatymai užtikrina tinkamas saugumo priemones ...“.
52. Šiomis aplinkybėmis svarbu priminti jau minėtą 29 straipsnio darbo grupės dokumentą, kuriame aptariamas teisminių duomenų tvarkymo klausimas⁽³⁵⁾. Darbo grupė teigia, kad „nors kiekvienas asmuo neabejotinai turi teisę tvarkyti teisminius duomenis savo paties bylinėjimosi procese, šis principas neapima tiek, kad leistų tretiesiems asmenims atlikti išsamų asmens duomenų tyrimą, rinkimą ir centralizavimą, įskaitant visų pirma sisteminių bendro pobūdžio tyrimą, pvz., interneto stebėjimą Tokių tyrimų atlikti priklauso teisminių institucijų kompetencijai“⁽³⁶⁾. Nors tikslinių, konkrečių įrodymų rinkimas, visų pirma šiurkščių pažeidimų byloje, gali būti būtinas norint suformuluoti ir įgyvendinti teisinius reikalavimus, EDAPP visiškai pritaria 29 straipsnio darbo grupės nuomonei dėl plataus masto tyrimų, susijusių su didžiulio interneto naudotojų duomenų kiekio tvarkymu, teisėtumo stoka.
53. Pirmiau aprašyta diskusija dėl proporcingumo principo ir „komercinio masto“ kriterijaus yra svarbi siekiant nustatyti, kokiomis sąlygomis bus įteisintas IP adresų ir susijusių informacijos rinkimas.

⁽³⁵⁾ Žr. šios išvados 28 punktą.

⁽³⁶⁾ Kursyvu išskirta mano.

54. IPT gali mėginti įteisinti autorių teisių turėtojų atliekamą tvarkymą, į savo klientų sutartis įrašę sąlygas, pagal kurias būtų leidžiama stebėti jų duomenis ir nutraukti abonementus. Sudarant tokias sutartis būtų tariama, kad klientai sutiko su stebėjimu. Tačiau ši praktika visų pirma susijusi su pagrindiniu klausimu dėl to, ar asmenys gali duoti IPT sutikimą dėl duomenų tvarkymo, kurį atliks ne IPT, o tretieji asmenys, kurių atžvilgiu IPT neturi jokių „igaliojimų“.

55. Antra, kyla sutikimo galiojimo klausimas. Direktyvos 95/46/EB 2 straipsnio h punkte sutikimas apibrėžiamas kaip reiškiantis „bet kurį savanoriškai ir žinomai duotą konkretų duomenų subjekto pareiškimą, kuriuo duomenų subjektas nurodo savo sutikimą, kad būtų tvarkomi su juo susiję duomenys“. Svarbus aspektas yra tas, kad norint, kad sutikimas galiootų, nepaisant jo davimo aplinkybių, jis turi būti duotas savanoriškai ir žinomai, turi būti konkreti duomenų subjekto valios išraiška, kaip apibrėžta direktyvos 2 straipsnio h punkte. EDAPP turi rimtų abejonių dėl to, ar asmenys, paprašyti duoti sutikimą dėl jų veiklos internete stebėjimo, iš tikrųjų turės galimybę pasirinkti, visų pirma todėl, kad alternatyva bus interneto prieigos neturėjimas ir todėl galimas pakenkimas daugeliui kitų jų gyvenimo sričių.

56. Trečia, labai abejotina, ar toks stebėjimas apskritai galėtų būti laikomas *būtinu* sutarčiais, kurios šalis yra duomenų subjektas, įvykdyti, kaip to reikalaujama Direktyvos 95/46/EB 7 straipsnio b punkte, nes akivaizdu, kad stebėjimas yra ne duomenų subjekto sudarytos sutarties dalykas, o tik priemonė IPT kitiems interesams tenkinti.

Registracijos bylų naikinimas

57. Pagal Direktyvą 2002/58/EB, visų pirma jos 6 straipsni, srauto duomenys, kaip antai IP adresai, gali būti renkami ir saugomi tik dėl priežasčių, tiesiogiai susijusių su pačiu pranešimu, įskaitant sąskaitų pateikimą, srauto valdymą ir sukčiavimo prevenciją. Paskui duomenys turi būti ištrinami. Tai nepažeidžia išipareigojimų pagal Duomenų saugojimo direktyvą, pagal kurią, kaip jau aptarta, reikalaujama saugoti srauto duomenis ir policijai ir prokurorams juos perduoti **tik** siekiant padėti tirti **sunkius nusikaltimus** ⁽³⁷⁾.

58. Remiantis tuo, kas išdėstyta pirmiau, interneto paslaugų teikėjai turėtų sunaikinti visas interneto naudotojų veiklą atskleidžiančias registracijos bylas, kurių nebereikia minėtiems tikslams pasiekti. Atsižvelgiant į tai, kad registracijos

bylos nėra būtinos sąskaitoms pateikti, atrodytų, kad srauto valdymo tikslais IPT turėtų pakakti trijų ar keturių savaitių ⁽³⁸⁾.

59. Tai reiškia, kad autorių teisių turėtojams susisiekus su IPT, nebent jie tai padarytų per minėtą ribotą laikotarpį, IPT neturėtų turėti registracijos bylų, pagal kurias IP adresai susiejami su atitinkamais abonentais. Registracijos bylos ilgiau nei nurodyta galėtų būti saugomos tik dėl pateisintų priežasčių siekiant teisės aktuose nustatytų tikslų.

60. Praktiškai tai reiškia, kad IPT skirti autorių teisių turėtojų prašymai negalėtų būti tenkinami, nebent jie būtų perduodami labai greitai, nes IPT tiesiog nebeturėtų informacijos. Taip savaime nustatomos ribos tam, kas laikoma pirmesniame skyriuje aprašyta priimtina stebėjimo praktika.

Šalutinio poveikio grėsmė

61. Be to, EDAPP kelia rūpestį ne tik interneto atjungimo po trijų išpėjimų politikos poveikis privatumui ir duomenų apsaugai, bet ir jos šalutinis poveikis. Jei interneto atjungimo po trijų išpėjimų politika būtų patvirtinta, ji galėtų tapti pavojingu pagrindu įteisinti dar masiškesnį interneto naudotojų veiklos stebėjimą įvairiose srityse ir įvairiais tikslais.

62. EDAPP ragina Komisiją užtikrinti, kad ACTA neišplėstų ir nepažeistų dabar ES galiojančios INT įgyvendinimo tvarkos, kuria paisoma pagrindinių teisių ir laisvių bei piliečių laisvių, kaip antai asmens duomenų apsaugos.

V. RŪPESTĮ DUOMENŲ APSAUGOS POŽIŪRIU KELIANTYS KLAUSIMAI, SUSIJĘ SU TARPTAUTINIO BENDRADARBIAVIMO MECHANIZMAIS

63. Viena iš ACTA dalyvių nurodytų priemonių INT įgyvendinimo klausimui spręsti yra tarptautinio bendradarbiavimo aktyvinimas taikant įvairias priemones, kurias panaudojus

⁽³⁷⁾ Žr. šios nuomonės 35 punktą.

⁽³⁸⁾ Srauto valdymas apima kompiuterio tinklo srauto analizę siekiant optimizuoti ar užtikrinti veikimą, mažesnę delną ir (arba) didesnę siuntimo spartą.

ACTA pasirašiusių šalių jurisdikcijose būtų galima veiksmingai įgyvendinti intelektinės nuosavybės teises.

64. Atsižvelgiant į turimą informaciją, galima numatyti, kad daugelis planuojamų priemonių, skirtų užtikrinti intelektinės nuosavybės teisių įgyvendinimą, bus susijusios ne tik su tarptautiniais valstybės institucijų (pvz., muitinės, policijos ir teisingumo), bet ir valstybinių bei privačių subjektų (pvz., IPT ir IN teisių turėtojų organizacijų) informacijos apie įtariamus INT pažeidimus mainais. Dėl tokio duomenų perdavimo duomenų apsaugos požiūriu kyla įvairių klausimų.

V.1. Ar pagal ACTA numatytas keitimasis duomenimis yra teisėtas, būtinas ir proporcingas?

65. Dabartiniame derybų proceso etape, kai daug konkrečių duomenų tvarkymo elementų tebėra neapibrėžti ar nežinomi, neįmanoma patikrinti, ar siūloma priemonių sistema atitinka pagrindinius duomenų apsaugos principus ir ES duomenų apsaugos teisę.

66. Pirmiausia galima kelti klausimą, ar duomenų perdavimas trečiosioms šalims pagal ACTA yra teisėtas. Klausimas, ar šioje srityje būtina taikyti tarptautinio lygio priemones, gali būti keliamas, kol tarp ES valstybių narių nėra susitarimo dėl įgyvendinimo priemonių skaitmeninėje aplinkoje suderinimo ir taikytinų baudžiamųjų sankcijų rūšių⁽³⁹⁾.

67. Atsižvelgiant į tai, kas išdėstyta pirmiau, atrodo, kad duomenų perdavimo pagal ACTA būtinumo ir proporcingumo principų būtų lengviau paisyti, jei susitarime būtų griežtai apsiribojama kova su sunkiausiais INT pažeidimo atvejais, užuot leidus bendrai perduoti duomenis, susijusius su bet koku INT pažeidimo įtarimu. Tam reikės tiksliai apibrėžti, kas yra „sunkiausi INT pažeidimai“, su kuriais gali būti siejamas duomenų perdavimas.

68. Be to, ypatingą dėmesį reikėtų atkreipti į duomenimis besikeičiančius asmenis, ir tai, ar duomenimis keisis tik valdžios institucijos, ar taip pat ir privatūs asmenys ir valdžios institucijos. Kaip anksčiau nurodyta šioje nuomonėje, privačių subjektų dalyvavimas tokioje srityje, kuri iš esmės priklauso teisėsaugos institucijų kompetencijai, kelia nemažai rūpesčių⁽⁴⁰⁾. Sąlygos, kuriomis privatūs subjektai dalyvaus

renkant su INT pažeidimais susijusius asmens duomenis ir keičiantis jais su valdžios institucijomis, turėtų būti griežtai susietos tik su konkrečiomis aplinkybėmis, taikant atitinkamas garantijas.

V.2. Taikytini duomenų apsaugos teisės aktai, kuriuose reglamentuojamas duomenų perdavimas pagal ACTA

Bendra duomenų perdavimo tvarka

69. Bendra ES taikoma duomenų apsaugos sistema reglamentuojama Direktyvoje 95/46/EB. Direktyvos 95/46/EB 25 ir 26 straipsniuose apibrėžiama duomenų perdavimui trečiosioms šalims taikoma tvarka. 25 straipsnyje reikalaujama, kad duomenys būtų perduodami tik toms šalims, kurios užtikrina adekvatų apsaugos lygį, kitaip toks perdavimas iš esmės yra draudžiamas.

70. Trečiųjų šalių užtikrinamo apsaugos lygio adekvatumą kiekvienu konkrečiu atveju vertina Europos Komisija, priėmusi kelis sprendimus, kuriais pripažino adekvatumą įvairių šalių atžvilgiu, 29 straipsnio darbo grupei atlikus išsamią analizę⁽⁴¹⁾.

71. EDAPP pažymi, kad dauguma ACTA dalyvių nėra įtraukti į Komisijos parengtą šalių, užtikrinančių adekvatą apsaugą, sąrašą, išskyrus Šveicariją ir konkrečiomis aplinkybėmis – Kanadą ir JAV, visos kitos ACTA dalyvės nepripažįstamos užtikrinančiomis adekvatų apsaugos lygį. Tai reiškia, kad norint perduoti duomenis iš ES šioms šalims turi būti įvykdyta viena iš Direktyvos 95/46/EB 26 straipsnio 1 dalyje nustatytų sąlygų arba duomenų perdavimo šalys turi pateikti atitinkamas garantijas pagal direktyvos 26 straipsnio 2 dalį.

Speciali tvarka, taikoma duomenų perdavimui baudžiamosios teisės įgyvendinimo srityje

72. Nors Direktyva 95/46/EB Europos Sąjungoje yra svarbiausias duomenų apsaugos teisės aktas, šiuo metu jos taikymo sritis yra ribota, nes į ją aiškiai nepatenka veiksmai, susiję, be kita ko, su valstybės veiksmais baudžiamosios teisės srityje (3 straipsnis). Todėl keitimasis duomenimis baudžiamosios teisės įgyvendinimo tikslu nepateks į Direktyvos 95/46/EB taikymo sritį ir jiems bus taikomi Europos Tarybos konvencijoje Nr. 108 bei jos papildomame

⁽³⁹⁾ Šiuo metu Taryboje svarstomas pasiūlymas dėl baudžiamųjų sankcijų, 2006 m. balandžio 26 d. COM(2006) 168.

⁽⁴⁰⁾ Žr. šios nuomonės 32 ir 52 punktus. Taip pat žr. 2008 m. lapkričio 11 d. EDAPP nuomonę dėl ES ir JAV aukšto lygio ryšių palaikymo grupės dėl keitimosi informacija, privatumo ir asmens duomenų apsaugos galutinės ataskaitos, OL C 128, 2009 6 6, p. 1.

⁽⁴¹⁾ Žr. Europos Komisijos sprendimus dėl adekvatumo, priimtus dėl Argentinos, Kanados, Šveicarijos, JAV saugaus prieglobsčio (*Safe Harbor*) ir JAV valdžios institucijų PNR duomenų kontekste, Gernsio, Meno salos ir Džersio; juos galima rasti http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm

protokole, kurių šalys yra visos ES valstybės narės, nustatyti bendrieji duomenų apsaugos principai⁽⁴²⁾. Be to, bus taikomos ES nustatytos taisyklės, susijusios su policijos ir teismų bendradarbiavimu baudžiamosiose bylose, įtvirtintos Tarybos pamatiniame sprendime 2008/877/TVR⁽⁴³⁾.

73. Šiais teisės aktais taip pat išreiškiamas principas, kad trečiojoje šalyje, kuriai turi būti perduoti duomenys, turi būti adekvatus duomenų apsaugos lygis. Numatyta nemažai leidžiančių nukrypti nuostatų, visų pirma kai trečioji šalis pateikia atitinkamas garantijas. Todėl panašiai, kaip ir keičiantis duomenimis pagal Direktyvą 95/46/EB, norint keistis duomenimis baudžiamosios teisės įgyvendinimo srityje reikės, kad norinčios keistis duomenimis šalys pateiktų atitinkamas garantijas.

Naujos duomenų perdavimo tvarkos kūrimas

74. Galima tikėtis, kad netrukus ES pagal SESV 16 straipsnį bus priimtos naujos bendros duomenų apsaugos taisyklės, taikytinos visose ES veiklos srityse. Tai reiškia, kad po kelerių metų gali būti sukurta išsami ES duomenų apsaugos sistema, nustatanti nuoseklias duomenų apsaugos taisykles visose ES veiklos srityse ir tokio pat lygio garantijas visai duomenų tvarkymo veiklai. Kaip pabrėžė už teisingumo, pagrindinių teisių ir pilietybės klausimus atsakinga Komisijos narė Viviane Reding⁽⁴⁴⁾, ši nauja sistema turėtų veikti kaip vienas „pažangus ir išsamus teisės aktas“, kuriuo ES reglamentuojama duomenų apsauga. Tokia sistema ypač laukiama, nes suteiktų daugiau aiškumo ir nuoseklumo dėl duomenų apsaugos srityje taikomų ES taisyklių.

75. Tarptautiniame kontekste EDAPP taip pat pažymi, kad neseniai duomenų apsaugos institucijos priėmė Rezoliuciją dėl tarptautinių asmenų duomenų ir privatumo apsaugos standartų, kuri yra pirmas žingsnis nustatant pasaulinius duomenų apsaugos standartus⁽⁴⁵⁾. Tarptautiniai standartai apima įvairias duomenų apsaugos garantijas, panašias į įtvirtintąsias Direktyvoje 95/46/EB ir Konvencijoje Nr.

⁽⁴²⁾ Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu, priimta 1981 m. sausio 28 d. Strasbūre, ir Europos Tarybos konvencijos dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu papildomas protokololas dėl priežiūros institucijų ir tarptautinių duomenų srautų, 2001 m. lapkričio 8 d., Strasbūras.

⁽⁴³⁾ 2008 m. lapkričio 27 d. Tarybos pamatinis sprendimas 2008/877/TVR dėl asmens duomenų, tvarkomų vykdančios policijos ir teisminių bendradarbiavimą baudžiamosiose bylose, apsaugos, OL L 350, 2008 12 30, p. 60.

⁽⁴⁴⁾ Žr. kandidatės į Komisijos narius Vivianos Reding atsakymus į Europos Parlamento klausimą, p. 5, http://www.europarl.europa.eu/hearings/static/commissioners/answers/reding_replies_en.pdf

⁽⁴⁵⁾ 2009 m. lapkričio mėn. Madride priimta rezoliucija.

108. Nors tarptautiniai standartai kol kas nėra privalomi, juose pateikiamos naudingos gairės, susijusios su duomenų apsaugos principais, kurias trečiosios šalys gali taikyti savanoriškai, idant jų teisės aktai atitiktų ES standartus. EDAPP mano, kad ACTA pasirašiusios šalys, tvarkydamos asmens duomenis iš ES, taip pat turėtų atsižvelgti į tarptautiniuose standartuose nustatytus principus.

V.3. Būtinybė įgyvendinti atitinkamas garantijas siekiant apsaugoti duomenų perdavimą iš ES į trečiąsias šalis

Kokios formos garantijų reikėtų siekiant veiksmingai apsaugoti duomenų perdavimą į trečiąsias šalis?

76. Jei yra įrodoma būtinybė asmens duomenis perduoti į trečiąsias šalis, EDAPP pabrėžia, jog Europos Sąjunga, nepaisant to, kad yra pats ACTA susitarimas, turėtų derėtis su trečiosios šalies duomenų gavėjais dėl konkrečių priemonių, kuriose numatytos atitinkamos duomenų apsaugos garantijos, taikomos keitimuisi asmens duomenimis.
77. Atitinkamos duomenų apsaugos garantijos paprastai turėtų būti nustatomos privalomame susitarime tarp ES ir trečiosios šalies duomenų gavėjo, ir šiuo susitarimu duomenis gaunanti šalis įsipareigoja laikytis ES duomenų apsaugos teisės ir suteikti asmenims tokias pat teises ir jų įgyvendinimo priemones, kaip pagal ES teisę. Privalomo susitarimo būtinybė kyla iš Direktyvos 95/46/EB 26 straipsnio 2 dalies ir Pamatinio sprendimo 13 straipsnio 3 dalies b punkto, be to, tokio susitarimo būtinybė grindžiama esama ES praktika sudaryti specialius susitarimus siekiant leisti perduoti konkrečius duomenis trečiosioms šalims⁽⁴⁶⁾.

78. Taip pat pagal tarptautinių standartų projektą, kad duomenų perdavimas įvyktų, gavėjui gali tekti užtikrinti, jog jis suteiks reikiamą apsaugos lygį. Garantijos taip pat galėtų būti suteikiamos prisiėmus sutartinį įsipareigojimą.

Asmens duomenų perdavimo atžvilgiu ACTA pasirašiusių šalių suteiktinų garantijų turinys

79. EDAPP visų pirma pabrėžia, kad tarptautinis keitimasis informacija teisėsaugos tikslais duomenų apsaugos požiūriu yra ypač slaptas, nes pagal šią sistemą gali būti įteisinti

⁽⁴⁶⁾ Pavyzdžiui, Europolo ir Eurojusto susitarimai su JAV, PNR susitarimas, Swift susitarimas, ES ir Australijos susitarimas dėl oro vežėjų atliekamo Europos Sąjungos pateiktų keleivio duomenų įrašo (PNR) duomenų tvarkymo ir perdavimo Australijos muitinės tarnybai.

masiniai duomenų perdavimai toje srityje, kur poveikis asmenims yra ypač didelis ir kurioje juo labiau reikalingos griežtos ir patikimos garantijos.

80. EDAPP pažymi, kad konkrečios sąlygos ir garantijos gali būti nustatytos tik kiekvienu konkrečiu atveju, atsižvelgiant į visus keitimosi duomenimis parametrus. Tačiau EDAPP kaip gaires toliau pateikia kai kuriuos principus ir garantijas, kurias turi taikyti trečiųjų šalių gavėjai, kad duomenų perdavimas įvyktų:

- būtina patikrinti, koks yra duomenų tvarkymo veiklos vykdymo teisinis pagrindimas (t. y. ar tvarkymo operacijos grindžiamos teisiniu išpareigojimu, esant duomenų subjektų sutikimui, ar kitu pagrįstu pateisinimu?), ar perduodant duomenis paisoma pradinio duomenų rinkimo tikslo. Duomenys negali būti perduodami kitokiu tikslu, nei minėtas tikslas.

- Asmens duomenų, kuriais planuojama keistis, kiekis ir rūšis turi būti aiškiai nurodyta ir sumažinta iki tiek, kiek yra griežtai būtina perdavimo tikslui pasiekti. Surinkti ir perduoti asmens duomenys visų pirma gali apimti interneto naudotojų IP adresus, įtariamo pažeidimo datą ir laiką ir pažeidimo rūšį. EDAPP rekomenduoja tyrimo etape nesusieti duomenų su konkrečiu asmeniu ir primena, kad įtariamojo asmens tapatybė turi būti nustatyta tik pagal įstatymą ir kontroliuojant teisėjui. Šioje nuomonėje EDAPP pabrėžia, kad su INT pažeidimais ir šių pažeidimų įtarimais susiję duomenys yra specialios kategorijos duomenys, kuriuos paprastai gali tvarkyti tik teisėsaugos institucijos ir kuriems reikia taikyti papildomas garantijas. Todėl teisę tvarkyti su INT pažeidimais ir šių pažeidimų įtarimais susijusius duomenis turintys asmenys bei šių duomenų tvarkymo sąlygos turi būti konkrečiai apibrėžti pagal esamus duomenų apsaugos teisės aktus.

- Asmenys, galintys keistis duomenimis, turi būti aiškiai nurodyti ir tolesnis perdavimas kitiems gavėjams iš esmės turėtų būti uždraustas, nebent toks perdavimas yra būtinas konkrečiam tyrimui. Šis ribojimas yra ypač svarbus, nes nustatytieji gavėjai neturėtų neteisėtai dalytis informacija su neįgalotais gavėjais.

- EDAPP daro prielaidą, kad ACTA bus ne tik numatytas valstybės institucijų bendradarbiavimas, bet ir suteiktos

autorių teisių įgyvendinimo funkcijos privačioms organizacijoms (pvz., IPT, autorių teisių turėtojų organizacijoms ir kt.). Pastaruoju atveju būtina atidžiai įvertinti privačių organizacijų dalyvavimo įgyvendinant INT sąlygas ir lygį siekiant, kad ACTA priemonėmis IPT ir IN teisių turėtojų organizacijoms *de facto* nebūtų suteikta teisė stebėti naudotojų elgesį internete. Be to, galimybė privačioms organizacijoms tvarkyti asmens duomenis teisėsaugos institucijų siekiamais tikslais turėtų būti suteikta tik pagal atitinkamą teisinį pagrindą. Taip pat svarbu išsiaiškinti, ar privačios organizacijos bus priverstos bendradarbiauti su policija ir koks bus tokio bendradarbiavimo mastas. Tai bet kuriuo atveju turėtų būti susiję tik su „sunkiais nusikaltimais“, kurių apibrėžtį taip pat reikės tiksliai nurodyti, nes ne visi INT pažeidimai laikytini sunkiais nusikaltimais.

- Keitimosi asmens duomenimis metodas turi būti aiškiai pasirinktas, visų pirma turėtų būti nurodyta, ar tai bus daroma pagal duomenų eksportavimo sistemą, pvz., IPT ir IN teisių turėtojų organizacijos perduos savo kontroliuojamus duomenis tretiesiems asmenims, pvz., užsienio policijai ir teisėsaugos institucijoms, arba duomenų importavimo sistemą, pvz., policija ir teisėsaugos institucijos turės tiesioginę prieigą prie privačių asmenų duomenų bazių ar duomenų bazių, kuriose informacija centralizuojama. Kaip jau nurodyta dėl PNR, duomenų eksportavimo sistema ES duomenų apsaugos požiūriu yra vienintelė duomenų apsaugos principus atitinkanti alternatyva, nes pagal ją ES siuntėjas, kuris, labiausiai tikėtina, yra duomenų valdytojas, įgyja teisę kontroliuoti duomenų perdavimą⁽⁴⁷⁾.

- Turi būti nurodytas laikas, kurį gavėjai saugos asmens duomenis, taip pat tokio saugojimo būtinumo tikslas. Toks saugojimo laikotarpis turėtų būti proporcingas atsižvelgiant į siektiną tikslą, t. y. duomenys turėtų būti pašalinami arba ištrinami, kai tik tampa nebereikalingi tam tikslui pasiekti.

- Turėtų būti aiškiai reglamentuoti trečiųjų šalių duomenų valdytojams nustatyti įpareigojimai. Turi būti užtikrinti priežiūros ir (arba) įgyvendinami atsakomybės mechanizmai, kad neteisėto tvarkymo ar kitų reikšmingų incidentų atveju būtų realių išteklių ir duomenų valdytojams būtų galima taikyti realias sankcijas. Be to, turėtų

⁽⁴⁷⁾ Žr. 29 straipsnio darbo grupės nuomonę Nr. 4/2003 dėl JAV užtikrinamo apsaugos lygio perduodant keleivių duomenis, WP78, 2003 m. birželio 13 d.

būti nustatyti žalos atlyginimo mechanizmai, kad asmenys galėtų pateikti skundą nepriklausomai duomenų apsaugos institucijai ir veiksmingai ginti savo teises nepriklausomame ir nešališkame teisme⁽⁴⁸⁾.

- Tarp šalių sudarytuose dokumentuose turėtų būti aiškiai nurodytos duomenų subjektų teisės dėl jų asmens duomenų, kai šiuos duomenis tvarko trečiosios šalies gavėjas, siekiant užtikrinti jiems veiksmingas priemonės ginti savo teises dėl užsienyje atlikto duomenų tvarkymo.
- Be to, ypač svarbus yra skaidrumas, ir duomenų apsaugos susitarimo šalys turėtų susitarti dėl to, kaip jos praneš duomenų subjektams apie vykstantį duomenų tvarkymą, apie jų teises ir šių teisių gynimo būdus.

VI. IŠVADOS

81. EDAPP labai rekomenduoja Europos Komisijai vesti viešą ir skaidrų dialogą dėl ACTA, galbūt surengti viešą konsultaciją, nes tai taip pat padėtų užtikrinti, kad priemonės, kurių bus imtasi, atitinka ES privatumo ir duomenų apsaugos teisės aktų reikalavimus.
82. Tebevykstant deryboms dėl ACTA EDAPP ragina Europos Komisiją užtikrinti tinkamą pusiausvyrą tarp reikalavimų apsaugoti intelektinės nuosavybės teises ir teisę į privatumą bei duomenų apsaugą. EDAPP pabrėžia, jog ypač svarbu, kad į privatumą ir duomenų apsaugą būtų atsižvelgta dar derybų pradžioje, prieš susitariant dėl bet kokių priemonių, kad vėliau netektų ieškoti alternatyvių privatumo klausimų sprendimų.
83. Nors intelektinė nuosavybė yra svarbi visuomenei ir turi būti ginama, ji neturėtų būti vertinama labiau už asmenų pagrindines teises į privatumą, duomenų apsaugą ir kitas teises, kaip antai nekaltumo prezumpciją, veiksmingą teisinę apsaugą ir nuomonės reiškimo laisvę.
84. Kadangi į dabartinį ACTA projektą įtraukta interneto atjungimo po trijų išpėjimų politika ar jame bent jau netiesiogiai raginama ją vykdyti, ACTA būtų gerokai apribotos Europos piliečių pagrindinės teisės ir laisvės, visų pirma teisė į asmens duomenų apsaugą ir privatumą.
85. EDAPP mano, kad interneto atjungimo po trijų išpėjimų politika nėra būtina intelektinės nuosavybės teisių įgyvendinimo tikslui pasiekti. EDAPP yra įsitikinęs, kad yra alternatyvių mažiau ribojančių sprendimų arba bent jau kad numatyta politika gali būti įgyvendinama ne taip ribojant arba būti mažesnės aprėpties, visų pirma taikant tikslinį *ad hoc* stebėjimą.
86. Interneto atjungimo po trijų išpėjimų politika taip pat yra probleminė išsamesniu teisiniu lygmeniu, visų pirma todėl, kad teisminių duomenų tvarkymas, visų pirma tas, kurį atlieka privačios organizacijos, turi būti paremtas atitinkamu teisiniu pagrindu. Norint, kad trijų išpėjimų sistema veiktų, gali prireikti ilgiau saugoti registracijos bylas, o tai prieštarautų esamiems teisės aktams.
87. Be to, kadangi ACTA susijęs su keitimusi asmens duomenimis tarp valdžios institucijų ir (arba) privačių organizacijų susitarimą pasirašiusiose valstybėse, EDAPP ragina Europos Sąjungą įgyvendinti atitinkamas garantijas. Šios garantijos turėtų būti taikomos visiems duomenų perdavimams pagal ACTA, nepaisant to, ar duomenys būtų perduodami įgyvendinant civilinę, baudžiamąją ar elektroninių ryšių teisę, ir turėtų atitikti Konvencijoje Nr. 108 ir Direktyvoje 95/46/EB nustatytus duomenų apsaugos principus. EDAPP rekomenduoja įforminti tokias garantijas privalomuose susitarimuose tarp ES duomenų siuntėjų ir trečiųjų šalių duomenų gavėjų.
88. Be to, EDAPP pageidauja, kad su juo būtų konsultuojamasi dėl priemonių, kurias planuojama įgyvendinti duomenų perdavimo srityje pagal ACTA, siekiant patikrinti jų proporcingumą ir tai, ar jomis užtikrinamas adekvatus duomenų apsaugos lygis.

Priimta Briuselyje 2010 m. vasario 22 d.

Peter HUSTINX

Europos duomenų apsaugos priežiūros pareigūnas

⁽⁴⁸⁾ Žr. Europos duomenų apsaugos priežiūros pareigūno nuomonę dėl ES ir JAV aukšto lygio ryšių palaikymo grupės dėl keitimosi informacija, privatumo ir asmens duomenų apsaugos galutinės ataskaitos, 2008 11 11.