

29 STRAIPSNIO duomenų apsaugos darbo grupė

xxx/05/EN

WP 104

Darbinis dokumentas dėl duomenų apsaugos klausimų, susijusių su intelektinės nuosavybės teisėmis

2005 m. sausio 18 d.

Ši Darbo grupė buvo sudaryta pagal Direktyvos 95/46/EC 29 straipsnį. Ji yra Europos savarankiška patariamoji duomenų apsaugos ir privatumo institucija. Jos tikslai nubrėžti Direktyvos 95/46/EC 30 straipsnyje ir Direktyvos 2002/58/EC 15 straipsnyje.

Sekretoriatas yra išlaikomas Europos Komisijos E direktorato (paslaugos, autorių teisės, pramoninė nuosavybė ir duomenų apsauga), Vidaus rinkos pagrindinis direktoratas, B-1049 Briuselis, Belgija, įstaigos Nr. C100-6/136.

Tinklapis: www.europa.eu.int/comm/privacy

DARBO GRUPĖ DĖL ASMENŲ APSAUGOS TVARKANT ASMENS DUOMENIS

**sudaryta pagal Europos Parlamento ir Tarybos Direktyvą 95/46/EB
1995 m. spalio 24 d.¹,**

atsižvelgdama į aukščiau nurodytos Direktyvos 29 straipsnį, 30(1)(c) straipsnį ir 30(3) straipsnį,
atsižvelgdama į jos tvarkos nurodymus ir ypač į 12 ir 14 straipsnius,

PRIĖMĖ ŠĮ darbinį dokumentą dėl:

Duomenų apsaugos klausimų susijusių su intelektinės nuosavybės teisėmis

1. ĮVADAS

Darbo grupė pažymi, kad augant su interneto plėtote susijusiam apsikeitimui informacija, vis labiau aštrėja subtilus klausimas dėl autorinės informacijos valdymo. Problemų kyla teisėms ir prievolėms tų veikėjų, kuriems rūpi autoriaus teisės ginama informacija ir tiems, kurie yra įtraukti į skaitmeninį teisių tvarkymą.

Darbo grupė pripažįsta būtinybę įgyvendinti apsaugos priemones, siekiant apsaugoti teisėtus intelektinės nuosavybės savininkų interesus nuo galimų sukčiavimų. Be to, Darbo grupė (DG) nustatė, jog dalis šių priemonių, užtikrinančių veiksmingą kai kurios autorinės medžiagos apsaugą nuo galimų neteisėtų apsikeitimų, vykdomų įvairiais autoriaus teisių valdytojų lygiais, įtraukia asmenų asmens duomenų tvarkymą. Pirmasis aspektas, kurį Darbo grupė ketina nagrinėti, yra susijęs su skaitmeniniu teisių valdymu („STV“), pastaruoju metu išitvirtinančiu tiek, kiek „STV“ leidžia indentifikuoti ir sekti asmenis, turinčius prieigą prie įstatymais saugomos informacijos (pvz., dainos, programinė įranga) internete. Kitas aspektas nušviečia galimybes, kuriomis gali naudotis autoriaus teisių valdytojai, priversdami asmenis, įtariamus autoriaus teisės pažeidimu, laikytis jų teisių.

Atsižvelgiant į skirtingus duomenų apsaugos klausimų atsiradimo lygmenis, šiuo dokumentu siekiama priminti pagrindinius teisinius principus, kurių privaloma laikytis ne tik autoriaus teises turintiems ir jomis besinaudojantiems, bet ir kitiems, su skaitmeninio tvarkymo sritimi susijusiems asmenims, kaip antai pramonės ir paslaugų teikėjai, siūlantys skaitmeninę teisių valdymo technologiją.

a. Skaitmeninis teisių valdymas

Dėl besiplėtojančio skaitmeninio teisių valdymo, DG pažymi, kad naujosios technologijos, taikomos identifiukuoti ir/arba sekti vartotojus yra nustatomos informacijos apsikeitimo lygmenyje bei platformos lygmenyje (t.y., techninės įrangos/programinės įrangos patikrinimas).

¹ Official Journal L 281, 23.11.1995, p. 31, galima rasti:
<http://europa.eu.int/comm/internal-market/privacy/law-fr.htm>

Dėl informacijos atsisiuntimo iš vienos sistemos dalies į kitą internetu, jei perduodama autorinė informacija, norint gauti tokią informaciją vis dažniau atliekamas išankstinis vartotojo tapatybės patikrinimas, kuris užbaigiamas tęsiant tos informacijos sekimą per žymenis arba skaitmeninius ženklus. Pavyzdžiui, vartotojai dažnai turės įrodyti savo tapatybę prieš atsisiųsdami dainą iš oficialaus tiekėjo, ir jų tapatybė bus visiškai nustatyta, surinkus informaciją per kiekvieno vartotojo atsisiunčiamo muzikos kūrinio unikalų indentifikatorių. Be skelbiamo tikslo kontroliuoti asmens naudojamą informaciją, pagal „STV“, žymenys pritvirtinami dažnai dar ir tam, kad skelbimai vartotojams būtų profilijuojami ir adresuojami. Kaip teigia Tarptautinė telekomunikacijų darbo grupė, „Elektroninės autoriaus teisės valdymo sistemos (EATVS) yra sukuriamos ir siūlomos tokios, kurios gali įtvirtinti platų vartotojų stebėjimą skaitmeniniais prietaisais. Kai kurios EATVS kontroliuoja kiekvieną atskirą vartotojų skaitymo, klausymo ir stebėjimo internete veiksmą tokiu būdu kaupdamos ypatingą informaciją apie duomenų subjektą“².

Dėl bazinės įrangos lygmens, Darbo grupė atidžiai sekė kai kurių pramonės projektų raidą, įskaitant TCG, skirtą užtikrinti patikimumą informacijos, kuri įtraukta į bazinę kompiuterio įrangą ir gaunama iš jos. Jei tokios sistemos, kaip pripažįsta Darbo grupė, gali turėti teigiamos įtakos informacijos saugumo lygmeniui, jų taikymas gali būti labai plėtojamas ir leisti per nuotolį patikrinti ar kompiuterio bazinės įrangos sudedamosios dalys atitinka autoriaus teises. Savo 2004 m. sausio 23 d. dariniame dokumente Darbo grupė pažymėjo, kad „TPM grindžiama įranga galėtų būti [...] pavyzdžiui, turinio pramonės naudojama, kad atgautų tiekimo ir skaitmeninio turinio (įskaitant programinę įrangą) naudojimo kontrolę, kurią jie prarado atsiradus internetui ir tiesioginio sujungimo (peer-to-peer) įrangai.“ Tokie tikrinimai galėtų vykti įprastine tvarka, pagal bet kokio ryšio tarp bazinių įrangų struktūrą, kadangi „TPM naudojimas, plačiai skatinamas pramonės, veikiausiai taps de facto norma, neišvengiama dalyvavimo informacinėje visuomenėje ypatybe.“

b. Autoriaus teisės įgyvendinimas

Kadangi tikrinimas ir sekimas vyksta prie šaltinio siekiant patikrinti „a priori“ kiekvieną vartotoją, internetu teisėtai atsisiunčiantį informaciją, autorinės informacijos apsauga reikalauja iš daugelio autoriaus teisių vykdytojų imtis „a posteriori“ (vėlesnių) veiksmų ir atlikti tyrimus dėl pažeidimais įtariamų vartotojų.

Darbo grupė išskiria tokias teisių valdytojų naudotinas priemones:

Stebėjimo priemonės (tiesioginio sujungimo), veikiančios internete, buvo nustatytos kaip pagrindinis būdas surasti informaciją apie asmenis, galinčius prisijungti tiesiogiai arba atsisiunčiančius saugotiną informaciją. Autoriaus teisių vykdytojų atliekami tyrimai paprastai remiasi vartotojų IP adresų kaupimu³. Toliau ši informacija jungiama su vartotojų duomenimis, aptiktais IPT (internetų paslaugų tiekėjų) (anglų k. ISP -Internet Service Providers). Kai kuriais atvejais teisių vykdytojai tiesiogiai kreipiasi dėl vartotojo tapatybės į IPT, norėdami pasiūsti vartotojams įspėjimo dėl tokios veiklos liovimosi ar nutraukimo raštus. Kitais atvejais autoriaus teisės vykdytojai kreipiasi dėl bendradarbiavimo į IPT, reikalaudami, kad jie patys siųstų tokiems

² Tarptautinė Darbo grupė dėl duomenų apsaugos telekomunikacijose, "Bendra nuomonė dėl privatumo ir autoriaus teisės apsaugos valdymo", priimtas Darbo grupės susitikime, vykusiame 2000 m. gegužės 27 d.

³ Dar prieš keletą metų daugeliui vartotojų vis dar būdavo priskiriami dinamiški adresai, beisikeičiantys kaskart prisijungiant prie interneto. Kabelinis ar asinchroninės skaitmeninės abonentinės linijos sujungimas leido priskirti nuolatinį IP adresą vartotojams. Todėl, jei yra nuolatinis IP adresas, o tai turėtų tapti reikalavimu, pritaikius naują IPv6 protokolą, palengvės interneto vartotojo sekimas (šiuo klausimu plačiau išdėstyta Darbo grupės 2002 m. gegužės 30 d. Nuomonėje 2002/2 apie unikalų identifikavimo priemonių telekomunikacijų galiniuose įrenginiuose naudojimą: pavyzdys IPv6, DG 58, 10750/02/EN).

vartotojams laiškus, prašydami juos išimti įtariamą pažeidimu medžiagą arba priešingu atveju vartotojams bus nutrauktas interneto paslaugų teikimas.

Kokiu mastu teisių valdytojai gali naudotis detalioja informacija apie vartotojus skiriasi kiekvienoje šalyje. Pavyzdžiui, Belgijoje teisių valdytojai kreipiasi dėl bendradarbiavimo į Interneto paslaugų teikėjus, kad šie siųstų išpėjimo laiškus vartotojams. Jungtinėse Valstijose, Interneto paslaugų teikėjų buvo prašoma perduoti savo klientų ID *tiesiogiai* muzikos industrijos atstovams be teismo potvarkio⁴. Tai lėmė keletą teismo nutarčių atsiradimą (pvz., Verizon byla - 2003 m. gruodis), kuriose toks tiesioginis informacijos perdavimas teisės valdytojams teismo buvo pripažinta neteisėtu. Pagal kitą pavyzdį, Australijos įstatymai (pagal „Anton Pilar įsakymą“) leidžia atlikti užklausų paiešką, įskaitant vizitus į namus tokių privačių asmenų kaip intelektualinės nuosavybės teisių valdytojai.

Siekdami susieti įtariamus pažeidimus su atsakingais vartotojais ir gauti visą vartotojo vaizdą, teisių valdytojai deda pastangas, kad galėtų pasinaudoti esamais viešaisiais registrais, pvz., „Whois“ duomenų bazėmis, kuriose saugomi detalūs asmens duomenys tų, kurie yra užregistravę domeno pavadinimą. Juose saugoma ypatinga informacija: kontaktiniai domeno duomenys, įskaitant telefono numerį, elektroninio pašto adresą bei kitus asmens duomenis. Kai kurią informaciją galima naudoti tiesiogiai prisijungus, o kitos detalės yra nematomos ir jų reikia prašyti duomenų bazės valdytojo.

Pagaliau Darbo grupė pažymi, jog, atsižvelgiant į tą faktą, kad teisių valdytojų atliekamą asmens informacijos rinkimą reglamentuoja duomenų apsaugos principai, keliose šalyse vyksta diskusijos su suinteresuotais teisių valdytojais, kad jiems būtų suteikta daugiau lankstumo tvarkant asmens duomenis. Prancūzijos duomenų apsaugos įstatymai, pavyzdžiui, šiuo metu įvedė išimtį, kuri specialiai leidžia įstatymu⁵ nustatytiems konkrečioms teisių valdytojams tvarkyti juridinius duomenis tam tikromis aplinkybėmis ir iš anksto gavus Prancūzijos DAI⁶ - duomenų apsaugos institucijos leidimą.

Darbo grupė šioje permainų situacijoje išvelgia būtinybę priminti pagrindinius duomenų apsaugos principus ir jų taikymo ribas, apimančias skaitmeninį teisės valdymą ir autoriaus teisės įgyvendinimą.

II. Intelektinės nuosavybės teisių valdymas

- Teisėtas teisių valdytojų tikslas užkirsti kelią saugomos informacijos naudojimui neretai apsiriboja vartotojų sekimu ir kontroliavimu to, kam jie teikia pirmenybę. Konkrečiai unikalių identifikatorių, susietų su surinkta asmenine informacija naudojimas lemia detalių asmens duomenų tvarkymą. Duomenų apsaugos direktyva 95/46 nustato keletą principų, kurių privaloma laikytis bet kokiam teisės valdytojui tokiu atveju, kai tvarkomi asmens duomenys. Direktyvos 2004/48/EB 2(3) (a) straipsnis dėl intelektualinės nuosavybės teisių vykdymo

⁴ Autoriaus teisės valdytojai savo prašymuose rėmėsi Skaitmeninio tūkstantmečio autoriaus teisės aktu dėl Teisinio apribojimo, susijusio su tiesiogiai internete prieinama medžiaga. Pagal šias nuostatas, bet kuris autoriaus teisės valdytojas arba jo/jos atstovas gali prašyti federalinio teismo teisėjo padėjėjo pateikti IPT įsakymą, kuriame prašoma nurodyti tapatybę vartotojo, įtariamo veikla, pažeidžiančia autoriaus teises. Ši procedūra yra itin lanksti, kadangi leidžia gauti asmens duomenis, susijusius su vartotoju nepradedant viso juridinio proceso.

⁵ Išimtis taikoma juridiniams asmenims, kaip išsamiai išvardinta Intelektinės nuosavybės kodekso straipsniuose L.321-1 ir L.331-1, ir turi tikslą ginti teisių valdytojų interesus.

⁶ CNIL privalės patikslinti juridinės informacijos, įtrauktos į bylas, kokybę bei jos saugojimo trukmę. Ji taip pat privalės užtikrinti, kad toks tvarkymas atitiktų tai, kas griežtai būtina kovoje su sukčiavimu (2004 m. liepos 29 d. „Conseil Constitutionnel“ sprendimas Nr.2004-499 DC). Pažymėtina, kad pagal Konstitucinį teismą, vartotojų tapatybės nustatymas pagal jų IP adresus galimas tik atliekant teisinę procedūrą.

patvirtino principą, jog Direktyva 2004/48/EB nesikerta su Direktyva 95/46 ir todėl neturi poveikio duomenų apsaugos principų taikymui.

Esminė šio dokumento mintis yra iškelti būtinybės principą ir anoniminės prieigos prie tinklo paslaugų reikalingumą, laikantis skaidrumo principo, derinant tikslą ir duomenų saugojimo apribojimus.

➤ Būtinybės ir (arba) anonimiškumo principai

Darbo grupė dar kartą patvirtina būtinybę leisti anoniminius ir pseudoniminius veiksmus internete. Šį principą Darbo grupė kėlė ne vieną kartą,⁷ kol jos Rekomendacijos „Anonimiškumas internete“ buvo patvirtintas 1997 m. gruodžio 3 d., kuriose DG jau pareiškė, tvarkant asmens duomenis internete reikia laikytis duomenų apsaugos principų, kaip ir kitose srityse. „Vartotojai privalo turėti galimybę naudotis internetu neatskleidžiant savo tapatybės tais atvejais, kai asmens duomenys nereikalingi tam tikrai paslaugai teikti“⁸. Šį principą pateisina būtinybės principas, nurodytas Duomenų apsaugos direktyvos 6 c) straipsnyje, pagal kurį asmens duomenys turi atitikti jų rinkimo ir (arba) vėlesnio tvarkymo temą, tikslą ir apimtį.

Šiuo požiūriu Darbo grupė pabrėžia, kad naudojant STV technologijas konkrečiai informacijai apsaugoti turėtų būti naudojami ir įrankiai vartotojo anonimiškumui išlaikyti. Todėl daugiau dėmesio vertėtų skirti privatumą stiprinančioms technologijoms, plėtojant ir diegiant šiuos naujus įrankius.

➤ Unikalių identifikatorių naudojimas

Unikalių identifikatorių naudojimas leidžia sujungti duomenis, susijusius su atskiru asmeniu, ir lengvina jų profiliavimą. Skaitmeninio teisių valdymo struktūroje jie leidžia profiliuoti vartotojus, remiantis dokumentų, kuriuose jis ir (arba) ji ieško informacijos, kokybe ir kiekybe. Pavyzdžiui, kompanija, siūlydama teisėto turinio tiesioginį ryšį, turės galimybę sekti tokių unikalais identifikatoriais pažymėtų dokumentų srautą per stebimuosius tinklus ir nustatyti vartotoją prie šaltinio, šiam pradėjus teisėtą atsiuntimą kaip ir toliau galbūt neteisėtai naudojant dokumentą. Darbo vietoje muzikos ar filmų industrijos atstovai turės galimybę susekti savo darbuotojus besinaudojant jiems patikėta saugoma informacija. Darbo grupė pagrįstai abejoja dėl identifikatorių naudojimo „a priori“ kiekvieno vartotojo sekimui, siekiant atpažinti konkretų asmenį įtarus jį autoriaus teisės pažeidimu. Dokumento ženklėjimas specialiomis žymomis neturi būti sietinas su asmeniu, išskyrus tada, kai ši sąsaja yra būtina paslaugų atlikimui, ar jei asmuo prieš tai buvo informuotas ir davė tam savo sutikimą.

➤ Duomenų subjekto informavimas

Kaip teigiama Tarptautinės telekomunikacijų darbo grupės dokumente, autoriaus teisės valdymo sistema turi veikti kaip galima skaidriau. Laikantis Direktyvos 95/46 10 straipsnio nustatytų reikalavimų, neleidžiama rinkti bet kokią informaciją, susijusią su duomenų subjektais prieš tai nepranešus jiems keleto elementų, o ypač duomenų valdytojo tapatybės, duomenų tvarkymo tikslo(-ų), duomenų gavėjų ar gavėjų kategorijų bei egzistuojančią teisę susipažinti su savo asmens duomenimis ir juos ištaisyti.

⁷ Rekomendacija 3/97 „Anonimiškumas internete“, priimta 1997.12.3;

Darbinis dokumentas: Asmens duomenų tvarkymas internete, priimtas Darbo grupės 1999 m. vasario 23 d., DG 16, 5013/99/EN/galutinis.

Rekomendacija 1/99 dėl nematomo ir automatinio asmens duomenų tvarkymo internete, atliekamo naudojant programinę ir techninę įrangą, priimta Darbo grupės 1999 m. vasario 23 d., 5093/98/EN/ galutinis, DG 17;

⁸ Tarptautinė darbo grupė duomenų apsaugai telekomunikacijose, opt. cit., p.2.

Ši informacija privalo būti skelbiama gerai matoma prieš vartotojui pateikiant asmens duomenis ar prieš jam/jai atsisiunčiant žymenimis paženklintą informaciją.⁹

➤ Tikslo apribojimo principo laikymasis (suderinamumas)

Bet koks asmens duomenų, surinktų iš vartotojo savanorišku pagrindu ar būtinų paslaugos atlikimui, panaudojimas privalo atitikti aukščiau nustatytą tikslą, kaip išdėstyta Direktyvos 6 b) straipsnyje. Iš tikrųjų, pavyzdžiui, neleidžiama rinkti vartotojo pavardės ir adreso, kai vykdomas apmokėjimas kreditine kortele, ir naudoti tuos duomenis tiesiog rinkodaros tikslams, sujungus juos su vartotojo pomėgiais, nustatytais kaupiant pažymėtą informaciją. Taip pat pagal Direktyvos dėl privatumo ir elektroninio ryšio 13 straipsnį, vartotojui privaloma suteikti informaciją ir pasirinkimą sutikti ar nesutikti su tokiu jo duomenų profiliavimu ir rinkodara. Tas pat principas galioja bet kokiam numatytam vartotojo duomenų perdavimui trečiosioms šalims. Be to, Darbo grupė pabrėžia, jog informacijos apie vartotojo pirkimo įpročius rinkimas gali lemti ypatingų duomenų tvarkymą, jei duomenų subjektai yra profiliuojami pagal jų ieškotos informacijos pobūdį (pvz., pagal religinio ar politinio turinio knygos atsiumimą ...). Toks tvarkymas gali vykti tik griežtai laikantis Direktyvos 95/46 8 straipsnio nuostatų.

➤ Asmens duomenų saugojimo apribojimai

Kaip išdėstyta Direktyvos 95/46 6 e) straipsnyje, asmens duomenys turi būti saugomi tokia forma, kuri leidžia identifikuoti duomenų subjektus ne ilgiau, negu būtina pagal tikslą, dėl kurio tie duomenys buvo surinkti ar yra toliau tvarkomi.

Bet kokie asmens duomenys, surinkti saugomo produkto ar paslaugos teikimo metu, privalo būti ištrinti, kai tik jie tampa neberekalingi sąskaitos pateikimui ar kokiam kitam vartotojo pripažintam tikslui, pavyzdžiui, komercinių ryšių palaikymui. Šis teisinis principas būtų pažeistas, jei visi vartotojo duomenys būtų saugomi bendra tvarka vien tik dėl tam tikro įtarimo, kad vartotojas piktnaudžiauja informacija, saugoma autoriaus teisės.

III. Tyrimo įgaliojimų ribos

Greta išaugusių techninių apsaugos galimybių dedant žymenis ir sekant autoriaus teisės dokumentus, jau keletą metų autoriaus teisės turėtojai imasi veiksmų, kad įtariamieji autoriaus teisės pažeidimais būtų patraukti baudžiamojon atsakomybėn. Tokie veiksmai apima informacijos rinkimą apie įtariamus vartotojus įvairiomis priemonėmis ir naudojant įvairių viešai ar ne viešai skelbtą informaciją, kaip apibūdinta skyrelyje I b.

Nors toks informacijos tvarkymas yra neginčytinai teisėtas savo paties teismo procese, vis dėlto duomenų rinkimo būdai ir surinktų duomenų pobūdis yra reglamentuojami duomenų apsaugos principais, kaip antai:

➤ Suderinamumo principas

Teisių turėtojai tyrimuose rėmėsi pirmiausia faktais, gaunamais tiesiogiai internete, pavyzdžiui, autoriaus teisės saugomų dokumentų teikimu stebėjimo tinkluose. Tokiu būdu buvo gaunami tokie duomenys: galimo pažeidimo data ir laikas, saugomo dokumento pobūdis bei netiesioginiai identifikatoriai, tarkim, galimo pažeidimo autoriaus pseudonimai. Kyla didelė pagunda užbaigti asmeninės informacijos rinkinį papildomomis detalėmis, nesunkiai randamomis pasitelkus interneto

⁹ Žr. Rekomendacijas 2/2001 dėl tam tikrų minimalių reikalavimų renkant asmens duomenis tiesioginiu ryšiu (on-line) Europos Sąjungoje, 5020/01/EN/galutinė, WP 43, priimtos gegužės 17.

paslaugų teikėjus ar kitose duomenų bazėse, pavyzdžiui, „Whois“ duomenų bazėje, kurioje kaupiama informacija apie domenų savininkus.

Darbo grupė primygtinai reikalauja laikytis teisinių apribojimų, taikomų pakartotiniam asmeninės informacijos naudojimui. Duomenų bazių turinys, nepriklausomai nuo to, ar jos viešos, ar ne, gali būti tvarkomos ir toliau naudojamos tik tam tikslui, kokiam buvo pirmą kartą duomenys renkami. Aptariant „Whois“ duomenų bazę, Darbo grupė jos 2003 m. birželio 13 d.¹⁰ nuomonėje jau yra pabrėžusi, jog „duomenų apsaugos požiūriu svarbu tiksliai apibrėžti, koks yra „Whois“ tikslas ir koks jos tikslas (-ai) gali būti laikomas teisėtu ir suderinamu su pirminiu tikslu.[...] Šis reikalas yra labai subtilus, nes „Whois“ katalogai negali būti naudojami kitiems tikslams jau vien todėl, kad tai nėra pageidaujama tokių katalogų potencialių vartotojų. Kai kurie tikslai, kurie galėtų kelti duomenų apsaugos (suderinamumo) klausimus, yra, pavyzdžiui, duomenų naudojimas privataus sektoriaus atstovų, užsiimančių tvarkos palaikymu savo pajėgomis, susijusiu su įtariamais jų teisių pažeidimais, pvz., skaitmeninio teisių valdymo srityje.“

Remiantis suderinamumo principu bei konfidencialumo principu, įtrauktu į 2002/58 ir 95/46 direktyvas, duomenys, gaunami interneto paslaugų teikėjų ir tvarkomi konkrečiais tikslais, įskaitant daugiausia telekomunikacijų paslaugų teikimą, negali būti perduoti trečiosioms šalims, tokioms kaip teisės valdytojai, išskyrus įstatymo nustatytais apibrėžtomis aplinkybėmis perdavimą viešosioms teisėsaugos institucijoms.

➤ Interneto paslaugų teikėjų vaidmuo

Darbo grupė primena, jog remiantis 2000/31 Direktyvos dėl elektroninės prekybos 15 straipsniu, interneto paslaugų teikėjams negalima priskirti sisteminės priežiūros, sekimo ir bendradarbiavimo prievolės.

Be to, interneto paslaugų teikėjai negali įsipareigoti, išskyrus atskirus atvejus, kai yra teisėsaugos institucijų įsakymas, bendrai „a priori“ saugoti visus su autoriaus teise susijusius duomenis. Darbo grupė ne kartą¹¹ yra teigusi, jog „kai srauto duomenys turi būti išsaugoti konkrečiais atvejais, tam turi būti aiškus poreikis, saugojimo periodas privalo būti kuo trumpesnis ir veikla turi būti aiškiai reglamentuota įstatymu, tokiu būdu sudarant pakankamas apsaugos priemones nuo neteisėtos prieigos bei nuo bet kokio kitokio piktnaudžiavimo.“

➤ Teismo duomenų tvarkymas

Kaip išdėstyta Duomenų apsaugos direktyvos 8 straipsnyje, tvarkymas duomenų, susijusių su pažeidimais, kriminaliniais teistumais ar apsaugos priemonėmis, gali būti vykdomas tik griežtai pagal valstybių narių nustatytas sąlygas. Kadangi bet kuris asmuo akivaizdžiai turi teisę tvarkyti teisminius duomenis vykstant jo(jos) bylai, pats principas neleidžia nuodugnaus tyrimo, rinkimo ir centralizavimo asmens duomenų, vykdomo trečiųjų šalių, įskaitant sisteminį tyrimą bendru mastu, kaip, tarkim, interneto skenavimas ar prašymas perduoti asmens duomenis, surinktus kitų dalyvių - interneto paslaugų teikėjų ar „Whois“ katalogų valdytojų. Tokie tyrimai priklauso teismo institucijų kompetencijai.

Šiuo atžvilgiu, Darbo grupė pastebi, jog naujoji 2004 m. balandžio 28 d. priimta Direktyva dėl intelektinės nuosavybės teisių vykdymo numato sąlygas, pagal kurias asmens duomenų galės reikalauti teismo institucijos. Šios institucijos gali reikalauti, pagal teisėtą ir suderintą prašymą,

¹⁰ Nuomonė 2/2003 apie duomenų apsaugos taikymo principus „Whois“ katalogams, 10972/03/EN galutinė, WP 76.

¹¹ Žr. Nuomonę 5/2002, priimtą 2002 m. spalio 11 d., dėl Europos duomenų apsaugos įgaliotinių pareiškimo, priimto Tarptautinėje konferencijoje Kordife (2002 m. rugsėjo 9-11 d.) dėl privalomo sisteminio telekomunikacijos srauto duomenų išsaugojimo, 11818/02/EN galutinė, WP 64.

perduoti informaciją apie šaltinį ir prekių bei paslaugų paskirstymo tinklus, kurie pažeidžia intelektinės nuosavybės teisę, kai pažeidimas yra komercinis, ir, nepažeidžiant su informacinių šaltinių konfidencialumu ar asmens duomenų tvarkymu susijusių principų. Turi būti nustatyta pusiausvyra tarp teisėtų autoriaus teisės valdytojų ir atskirų asmenų interesų. Šiuo atžvilgiu komercinės naudos kriterijus, susijęs su pažeidimu, gali būti lemiamas.

4. Išvados

Darbo grupė reiškia susirūpinimą dėl to fakto, kad teisėtas technologijų naudojimas kūriniių apsaugai gali būti žalingas asmens duomenų apsaugai. Apsvarsčiusi duomenų apsaugos principų taikymą skaitmeniniam teisių valdymui, ji išvelgia didėjantį atotrūkį tarp asmenų apsaugos neryšinėje (off-line) ir tiesioginio ryšio (on-line) aplinkoje, ypač atsižvelgiant į asmenų sekimą ir profiliavimą. Darbo grupė ragina plėtoti ir diegti tokias technines priemones, kurių savybės atitinka privatumo, skaidraus ir riboto unikalių identifikatorių naudojimo reikalavimus bei suteikia vartotojui pasirinkimo galimybę.

Dėl tyrimo įgaliojimų, Darbo grupė mano, kad reikia priminti, jog privačių asmenų, pavyzdžiui, autoriaus teisių turėtojų, vykdomi tyrimai turi būti atliekami pagal aukščiau apibūdintus teisės rėmus, ypač jei tai susiję su informacija, kuri gali būti renkama teisėtai, ir šiems asmenims priskirtų teisių įgyvendinimo galias.

