



5035/01/EN/Final
WP 56

**Darbinis dokumentas dėl
tarptautinės ES duomenų apsaugos teisės dėl asmens duomenų tvarkymo internete,
naudojant ne ES esančias interneto svetaines, taikymo**

Priimta 2002 m. gegužės 30 d.

Darbo grupė buvo įkurta vadovaujantis Direktyvos 95/46/EB 29 straipsniu. Ji yra nepriklausomas ES patariamasis organas duomenų apsaugos ir privatumo klausimais. Jos uždaviniai yra išdėstyti Direktyvos 95/46/EB 30 straipsnyje ir Direktyvos 97/66/EB 14 straipsnyje. Sekretoriatą teikia:

The Europos Komisija, Internal Market DG, funkcionuojantis ir veikiamas vidaus rinkoje. Koordinavimas. Duomenų apsauga.
B-1049 Brussels - Belgium - Office: C100-6/136
Internetinis adresas: <http://europa.eu.int/comm/privacy>

DARBO GRUPĖ DĖL INDIVIDŲ APSAUGOS RYŠIUM SU ASMENS DUOMENŲ TVARKYMU

Įkurta pagal 1995 m. spalio 24 d. Europos Parlamento ir Tarybos Direktyvą 95/46/EB¹,

atsižvelgiant į šios Direktyvos 29 ir 30 straipsnių 1(a) ir 3 paragrafus,

atsižvelgiant į jos Procedūros taisykles ir ypač į jų 12 ir 14 straipsnius,

priėmė šį darbo dokumentą:

1. Įvadas

Šio dokumento tikslas yra diskutuoti dėl tarptautinio ES duomenų apsaugos teisės taikymo duomenų tvarkymui, ypač rinkimui, naudojantis interneto svetainėmis, registruotomis už ES ribų². Darbo dokumento tikslas – būti naudingu įrankiu ir pateikti nuorodas duomenų valdytojams ir jų patarėjams asmens duomenų tvarkymo, kai tai atliekama už ES ribų registruotose interneto svetainėse, klausimais. Kadangi ši sritis yra labai sudėtinga, o internetas – labai dinamiška aplinka, šis dokumentas nepasiūlys konkrečių sprendimų visais galimais susijusiais klausimais.

Šiame darbo dokumente “Privatumas internete”³ 29 Straipsnio Duomenų apsaugos darbo grupė nustatė aiškų poreikį nurodyti, kaip konkrečiai taikoma taisyklė dėl bendrosios duomenų apsaugos direktyvos taikytinų įstatymų (4 straipsnio 1 (c) paragrafas)⁴, ypač internetiniam asmens duomenų tvarkymui, kai jį atlieka valdytojas, registruotas už Bendrijos ribų. Nacionalinės duomenų apsaugos priežiūros institucijos privalo nuolat patarti verslui ir privatiems asmenims šiuo klausimu.

Poreikis nustatyti, ar nacionalinė teisė taikoma situacijoms, apimančioms kelias šalis, nėra specifinė duomenų apsaugai ar internetui, arba Europos Sąjungai. Tai bendrasis tarptautinės teisės klausimas, kylantis internetinėse ir ne internetinėse situacijose, kur vienas ar daugiau elementų yra susiję su daugiau nei viena šalimi. Būtinasis sprendimas, kaip nacionalinė teisė turi būti taikoma prieš priimant sprendimą, kurio turinys galėtų būti vystomas.

Šie sprendimai apima daugybės faktorių svarstymą. Pirmiausias ir svarbiausias yra konkrečios valstybės skiriamas dėmesys savo piliečių, gyventojų, verslo ir kitų subjektų teisių ir interesų, pripažintų nacionalinės teisės, gynimui. Daugelyje šalių baudžiamoji teisė (kuri yra priešinga teisei, nustatančiai teises ir laisves) reikalauja plačiausio taikymo, turinčio tarptautinį efektą. Žinomi Yahoo!⁵ arba CompuServe⁶ atvejai iliustruoja, kaip Teismai taiko

¹ Official Journal Nr. L 281 of 23/11/1995, p. 31, prieinamas adresu:
http://europa.eu.int/comm/internal_market/en/dataprot/index.htm

² Duomenų apsaugos direktyva 95/46/EB taip pat buvo įdiegta Europos Ekonominėje Zonoje (EEZ). Sąvoka “Europos Sąjunga” šiame dokumente turi būti suprantamai kaip apimanti ir EEZ.

³ “Privatumas internete – integruotas ES internetinės duomenų apsaugos taikymas”, WP 37, 21 Nov. 2000

⁴ Europos Parlamento ir Tarybos 1995 m. spalio 24 d. Direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo
O.J. n° L 281 of 23.11.1995, p. 31-50., prieinamas adresu:
http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html

⁵ TGI Paris, *ordonnance du référé* 2000 m. spalio 20 d.
http://legal.edhec.com/DTIC/Decisions/Dec_responsabilite_0.htm

⁶ AG München, 1998-05-28 sprendimas– 8340 Ds 465 Js 173158/95

nacionalinę baudžiamąją teisę, kad uždraustų priėjimą prie pornografinio ar rasistinio turinio užsienio interneto serverių. Nesenas Vokietijos Aukščiausiojo Teismo sprendimas baudžiamuoju klausimu nutiesė „Auschwitz Lüge“ leidėją (Auschwitz'o egzistavimo neigimas) Australijos interneto svetainėje, nors ir nebuvo įrodyta, kad ši svetainė buvo iš tiesų prieinama Vokietijoje⁷. Pagal Teismo sprendimą, šio konkretaus nusikaltimo kontekste, buvo pakankama, kad Interneto turinys „galėjo“ neigiamai paveikti visuomenės tvarką Vokietijoje, tačiau nebūtinai taip iš tikrųjų atsitiko.

Tokie tarptautiniai ginančiųjų taisyklių poveikiai išreiškia bendrą įstatymų leidėjo ar teisėjo rūpestį, kur būtina ginti piliečius, nepaisant teisėtvarkos sunkumų, kylančių dėl tarp valstybių susiklostančių situacijų, ir kaip taikyti jas praktikoje, siekiant užtikrinti, kad nustatytas tikslas būtų pasiektas.

ES teisėje keletas pavyzdžių iliustruoja tokį susitarimo siekimą.

Konkurencijos teisės srityje Europos Komisija gali priimti sprendimus, paveikiančius už ES ribų įsteigtas įmones, jei jos užsiima verslu ES teritorijoje. Geras pavyzdys yra nesenas Komisijos⁸ sprendimas blokuoti siūlomą susijungimą⁹ tarp General Electric ir Honeywell, dviejų JAV kompanijų. Šio sprendimo, priimto 2001 m. liepą, 1 straipsnyje buvo paskelbta, kad dviejų kompanijų susijungimas sukurs „neatitinkančią Bendrosios rinkos koncentraciją“. Komisija nustatė, kad susijungusios kompanijos Bendrijos ribose turės daugiau nei 250 milijonų eurų apyvartą, ir dėl to nusprendė, jog tai įvyktų „Bendrijos mastu“.

Už Bendrijos teritorijos veikiančios jos teisės mastas gali būti pastebimas ir vartotojų teisės srityje. Nuotolinio pardavimo Direktyvos¹⁰ 12 straipsnis skelbia, kad vartotojas nepraranda Direktyvoje jam garantuojamos apsaugos dėl tam tikrų sutarties punktų pasirinkimo, jei už ES ribų pasirinktos šalies teisė numato silpnesnę apsaugą, negu ES teisė. Tai atvejais, kada sutartis turi „glaudų ryšį“ su viena ar daugiau šalių, nepriklausančių ES¹¹. Posakis „glaudus ryšys“ paimtas iš 1980 m. Romos Konvencijos 7 straipsnio. Šis straipsnis skelbia, kad šalies „privalomos taisyklės“ turi būti taikomos situacijose, kurias reglamentuoja kitos šalies teisė, kai ši situacija turi „glaudų ryšį“ su šalimi.

Dar daugiau, yra buvę precedentinės teisės bylų, kuriose vadovautasi tais pačiais argumentais dėl Komercinių agentų Direktyvos¹². Europos Teisingumo Teismas nustatė¹³, kad kur komercinis agentas, atliekantis savo veiklą Bendrijos viduje, yra įdarbintas pagrindinio agento, įsteigto už Bendrijos ribų, pagrindinis agentas negali nesilaikyti Direktyvos sutartinės teisės reikalavimų, nustatančių, kad trečios šalies teisė taikoma santykiams. Teismas nustatė, kad Bendrijos teisė turi būti taikoma tais atvejais, kai „situacija“ yra glaudžiai susijusi su Bendrija.

⁷ BGH, 2000-12-12 sprendimas, Az: 1 StR 184/00.

⁸ 2001-07-03 nutarimas, bylos nr. COMP/M2220 pagal Susiliejinimo Procedūros Taisyklių (EEC) Nr. 4064/89 8(3) straipsnį.

⁹ Pagal šį susitarimą, Honeywell turėjo tapti visiškai priklausoma General Electric dukterine įmone.

¹⁰ Direktyva 97/7/EB

¹¹ Direktyvos 93/13 6(2) straipsnis dėl neteisingų terminų vartotojų kontraktuose ir Direktyvos 99/44 7(2) straipsnis dėl plataus vartojimo prekių pardavimo tam tikrų aspektų ir garantijos yra labai panašūs į 12(2) straipsnį. Juose abiejuose reikalaujama taikyti ES teisę ir abiejuose vartojamas terminas „glaudus ryšys“.

¹² Direktyva 86/653/EEC

¹³ Ingmar GB Ltd. ir Eaton Leonard Technologies byla C-381/98

Dar praktiškesnis pavyzdys gali būti rastas avialinijų pramonėje. Taryba išleido reglamentą, pavadintą KRS etikos kodeksu (Kompiuterinės Rezervavimo Sistemos)¹⁴. Šis reglamentas (kuriame reguliuojama, kaip KRS sistemos yra naudojamos) yra taikomas „bet kokiai kompiuterizuotai rezervavimo sistemai... kai ja siūloma naudotis ar ji yra naudojama Sąjungos teritorijoje, nepriklausomai nuo sistemos pardavėjo statuso ar tautybės, arba atitinkamo centrinio duomenų tvarkymo skyriaus buvimo vietos“. Todėl kai sistema galima naudotis ES, net jeigu pagrindinė sistemos įranga yra ne ES (o duomenys į sistemą teikiami per ES esančius terminalus arba kitaip), automatiškai yra taikoma ES teisė.

Todėl išnagrinėjus, kaip šiais eksteritorialiais atvejais yra taikoma ES teisė, galima daryti išvadą, kad paprastai yra taikomi panašūs kriterijai. Ar reikalaujama, kad santykiai turėtų „Bendrijos aspektą“ ar „glaudų ryšį“ su Bendrija, konkrečiose situacijose Europos teisingumo teismas, Europos Parlamentas ir Taryba, taip pat ir Europos Komisija mato esant tinkamu primesti ES taisykles ne ES subjektams.

Kitose šalyse, pavyzdžiui, Jungtinėse Amerikos Valstijose, teismai ir įstatymai taiko panašius argumentus, kad užsienio svetainės būtų reguliuojamos vietos taisyklių: JAV Vaikų Internetinio Privatumo Apsaugos Aktas 1998 (COPPA) taip pat yra taikomas užsienio svetainėms, renkančioms asmeninę informaciją iš vaikų JAV teritorijoje¹⁵. Pagal šį Federalinį įstatymą, svetainės operatorius, kuris orientuotas į 13 metų vaikus (ar tinklapio, skirto bendrai autorijai, tačiau operatorius tiksliai žino, kad tinklapyje iš vaikų renkama informacija) privalo laikytis COPPA nuostatų. Šis teisės aktas reguliuoja, kokią informaciją operatorius turi pateikti privatumo sutartyje, kada ir kaip operatorius privalo gauti patvirtinamą tėvų sutikimą, ir kaip operatorius yra atsakingas už vaikų privatumo ir saugumo internete apsaugą. Šiuo atveju yra įdomu tai, kad šis įstatymas yra taikomas ne konkrečiai JAV kompanijoms, bet „internete esančioms“ kompanijoms ir todėl Akto jurisdikcijos požiūriu yra visai nesvarbu, kur fiziškai yra svetainė, kol ji veikia JAV. Jeigu taip yra, svetainė bus reguliuojama tos srities JAV įstatymo.

Tiriant tarptautinę teisę, kyla mintis, kad Jungtinėse Valstijose vyrauja tendencija remtis keliais alternatyviais kriterijais, apibrėžiančiais plačią nacionalinės teisės taikymo sritį, kad galima būtų apimti kiek įmanoma daugiau atvejų, siekinat kiek įmanoma apsaugoti nacionalinius vartotojus ir pramonę. Dėl šios tendencijos neišvengiamai taikomi keli nacionaliniai įstatymai situacijose, įtraukiančiose tarpvalstybinių faktorių. Todėl tarptautiniuose teisės aktuose objektyviai ir nešališkai bandoma nustatyti svarbiausius kriterijus. Vis dėlto, paskutinės pastangos pasistūmėti į priekį su konvencijos dėl kontraktams taikytinų teisės aktų projektu, remiamu „Hagos Konferencijos“, žlugo, nes šalys negalėjo susitarti dėl lemiamo kriterijaus. Aptariant taikytinus teisės aktus, išryškėjo problemos esmė: tarp suinteresuotų šalių įvairių interesų reikia surasti teisingą pusiausvyrą.

Tokiame fone reikia pažymėti, kad ES duomenų apsaugos direktyvoje yra aiški nuostata dėl taikytinų teisės aktų kriterijaus. Nepaisant to, ar ši nuostata yra lengvai suprantama ir pritaikoma, vis dėlto tai yra privalumas asmenų ir verslo naudai, kad duomenų apsaugos direktyvoje atkreipiamas dėmesys į šį esminį klausimą.

2. Direktyvos 95/46/EB 4 straipsnis dėl taikytinų teisės aktų

Direktyvos 4 straipsnis skamba taip: Taikytini nacionalinės teisės aktai

1. Kiekviena valstybė narė taiko nacionalines nuostatas, kurias ji priima pagal šią direktyvą, kai tvarkomi asmens duomenys, jeigu:

¹⁴ KRS etikos kodeksas (suderinta Tarybos Reglamento versija Nr. 2299/89, pataisytas 3089/93, pataisytas 323/99)

¹⁵ 15 U.S.C. § 6502 (1)(A)(I), mintėtas Joel R. Reidenberg, žr. 5 išnašą.

(a) tvarkoma, duomenų valdytojo padaliniui veikiant valstybės narės teritorijoje; jeigu tas pats duomenų valdytojas steigiamas kelių valstybių narių teritorijoje, jis privalo imtis reikalingų priemonių, kad kiekvienas jo padalinys vykdytų taikytinų nacionalinių įstatymų nustatytas prievolės;

(b) duomenų valdytojas įsikūręs ne valstybės narės teritorijoje, bet tokioje vietoje, kur jos nacionaliniai įstatymai galioja, remiantis tarptautine viešąja teise;

(c) duomenų valdytojas įsisteigęs ne Bendrijos teritorijoje ir tvarkydamas asmens duomenis naudojami automatinė ar kitokia įranga, esančia minėtos valstybės narės teritorijoje, nebent tokia įranga būtų naudojama tiksliai duomenis tranzitu persiunčiant per bendrijos teritoriją.

2. Susiklosčius 1 dalies c punkte nurodytoms aplinkybėms, duomenų valdytojas privalo paskirti atstovą, įsteigtą minėtos valstybės narės teritorijoje, nepažeisdamas nuostatų dėl teisinių veiksmų, kurių gali būti imtasi prieš patį duomenų valdytoją.

Šiame straipsnyje aptariami atvejai, keliant klausimą dėl asmens duomenų tvarkymo operacijoms taikytino įstatymo: tai tokie atvejai, kai mažiausiai vienas asmens duomenų tvarkymo aspektas liečia ne vieną valstybę narę. Pavyzdžiui, tiesioginės rinkodaros kompanija sudaro kelių valstybių narių vartotojų adresų sąrašus ir juos naudoja valstybėje, nepriklausančioje Sąjungai, kad galėtų siųsti reklamą šiems vartotojams. Arba JAV svetainė ES gyvenančių asmenų kompiuteriuose palieka savo elektroninį pėdsaką (*cookie* failą), kad galima būtų susieti personalinį kompiuterį su tinklapiu, norint susieti informaciją su kitais.

Direktyva apibendrintai atskiria situacijas, kada tarpvalstybiniai elementai izoliuojami nuo ES valstybių narių ar teritorijų, esančių už geografinių Europos Sąjungos sienų, tačiau kur valstybės narės teisės aktai yra taikomi, remiantis tarptautine viešąja teise („diplomatini atvejais”)¹⁶ ir situacijas, kada tvarkymas įtraukia Europos Sąjungos ribas viršijančius elementus¹⁷.

Dėl Bendrijos viduje susidarančių situacijų, direktyvos tikslas yra dvejopas: siekiama išvengti spragų (netaikomas duomenų apsaugos įstatymas) ir išvengti nacionalinių įstatymų daugkartinio taikymo. Kai direktyvoje kalbama apie taikytinus įstatymus ir nustatomas kriterijus, lemiantis, kurio įstatymo pagrindu galima išspręsti bylą, pati direktyva atlieka vadinamąjį „konflikto taisyklės“ vaidmenį ir neberekia kreiptis į kitus egzistuojančius tarptautinės privatinės teisės kriterijus.

Kad būtų rastas atsakymas, direktyva naudoja „valdytojo įsisteigimo vietas“ kriterijų arba «jungiamąjį faktorių», kitaip tariant, kilmės šalies principą, paprastai taikomą Vidaus rinkoje. Konkrečiai tai reiškia:

Kai duomenys tvarkomi duomenų valdytojo padaliniui veikiant valstybės narės teritorijoje, tvarkymui yra taikomas tos valstybės narės duomenų apsaugos įstatymas.

Kai tas pats valdytojas yra įsisteigęs kelių valstybių narių teritorijoje, kiekvienas įkurtas padalinys, savo veikloje tvarkydamas duomenis, turi laikytis kiekvienos valstybės narės atitinkamame įstatyme nustatytų prievolių. Tai nėra kilmės šalies principo išimtis. Tai yra tik griežtas jo taikymas: jei valdytojas nusprendžia turėti ne vieną, o kelis padalinius, jis nieko nelaimi iš to, kad jam veikiant visoje vidaus rinkoje pakanka laikytis vieno įstatymo.

¹⁶ Šis atvejis nebus nagrinėjamas šiame dokumente. Taip pat reikia įsidėmėti, kad direktyva ir todėl 4 straipsnis taikomi privačiam ir viešajam asmens duomenų tvarkymo, reguliuojamo Bendrijos teisės, sektoriams. Šiame darbo dokumente nenagrinėjami 4 straipsnio taikymo viešajam sektoriui atvejai.

¹⁷ Toks skyrimas daugiausia taikomas valdytojui. Bet kokių atveju reikia išaiškinti, kad direktyvos taikymo neveikia faktas, kad valdytojas, esantis ES, už ES ribų turi veikiantį procesorių. Tokiu atveju direktyva vis tiek taikoma visoms tvarkymo operacijoms.

Toks valdytojas tada susiduria su paraleliu atitinkamų nacionalinių įstatymų taikymu atitinkamame jo padalinyje. Darbo grupė galėtų nagrinėti šį klausimą ateityje.

Kilmės šalies principo taikymas yra pateisinamas vidaus rinkoje, kurioje nacionaliniai duomenų apsaugos įstatymai teikia lygiavertę apsaugą, nes yra suderinta asmenų teisė į duomenų apsaugą, pramonės subjektų prievolės bei kitų valdytojų asmens duomenų tvarkymas. Todėl kilmės šalies principas, kuris tam tikru būdu riboja valstybių narių duomenų apsaugos įstatymų taikymo sritį, neveikia neigiamai jos gyventojų ar pramonės subjektų teisių ir interesų. Tiesą sakant, net jei valstybių narių įstatymai nėra taikytini kiekvienam tvarkymui, įtraukiančiam nacionalinį duomenų subjektą arba atliekamam nacionalinėje teritorijoje, tai, kad kitos valstybės narės įstatymas yra taikytinas, turi labai ribotą įtaką, atsižvelgiant į tai, kad abu įstatymai yra suderinti pagal direktyvą ir todėl abu yra lygiaverčiai. Be to, nacionalinių duomenų apsaugos institucijų bendradarbiavimas užtikrina pasitikėjimą, konfidencialumą ir efektyvų įstatymo, kad ir koks būtų taikytinas, vykdymą¹⁸.

Visai kitokia situacija susiklosto, kai tvarkymo operacijose dalyvauja trečiosios šalies valdytojas. Šių trečiųjų šalių nacionaliniai įstatymai nėra suderinti, direktyva nėra taktinė šiose šalyse ir asmenų apsaugos, ryšium su jų asmens duomenų tvarkymu, gali nebūti arba ji gali būti silpna. Kilmės šalies principas, kuris siejamas su valdytojo padaliniu, negali padėti nustatyti taikytiną įstatymą. Būtina pereiti prie kito jungiamojo faktoriaus. Europos Parlamentas ir Taryba nusprendė grįžti prie vieno iš klasikinių tarptautinės teisės jungiamųjų faktorių, kuris fiziškai susieja veiksma su teisine sistema. ES įstatymų leidėjas pasirinko šalį, kurios teritorijoje išdėstyta naudojama įranga¹⁹. Taigi, direktyva taikoma, kai valdytojas įsikūręs ne Bendrijos teritorijoje, tačiau yra nusprendęs tvarkyti asmens duomenis konkrečiais tikslais ir naudotis įranga, automatinė ar kitokia, esančia valstybės narės teritorijoje.

Direktyvos 95/46/EB 4 straipsnio 1 c) paragrafe esančios šios nuostatos tikslas yra, kad asmuo neliktų neapsaugtas ryšium su jo šalyje atliekamu tvarkymu tik todėl, kad valdytojas nėra įsisteigęs Bendrijos teritorijoje. Tai būtų paprasta, nes valdytojas iš esmės niekaip nėra susijęs su Bendrija. Bet taip pat galima įsivaizduoti, kad valdytojais įkuria savo padalinius už ES ribų, kad išvengtų ES įstatymo taikymo.

Nieko nevertas pasakymas, kad asmeniui nereikia būti ES piliečiu, fiziškai būti arba gyventi ES. Direktyvoje nėra skirstymo tautybės ar vietos pagrindu, nes su jos pagalba derinami valstybių narių įstatymai dėl pagrindinių teisių, priklausančių visiems žmonėms, nepaisant jų tautybės. Vadinasi, tokiais atvejais, kurie bus aptarti toliau, asmuo galėtų būti JAV ar kiniečių tautybės. Kalbant apie ES duomenų apsaugos įstatymo taikymą, šis asmuo bus saugomas, kaip ir bet koks ES pilietis. Svarbiausia yra, kur naudojama tvarkymo įranga yra išdėstyta

Bendrijos įstatymų leidėjo sprendimas, kad tvarkymas, kuriam naudojama ES esanti įranga, turi paklusti jos duomenų apsaugos įstatymui atspindi tikrąjį rūpinimąsi, kad asmenys savo teritorijoje būtų apsaugoti. Tarptautiniu lygiu pripažįstama, kad valstybės gali suteikti tokią apsaugą. GATS'o XIV straipsnyje nustatomi atleidimai nuo laisvo verslo taisyklių, kad būtų apsaugoti asmenys, atsižvelgiant į jų teisę į privatumą ir duomenų apsaugą, ir kad šis įstatymas būtų vykdomas.

Kitame skyriuje aiškinami svarbiausieji terminai, kad būtų galima apibrėžti taikytiną įstatymą:

2.1 Įsisteigimas

¹⁸ Žr. Direktyvos 95/46/EB 28 straipsnio 6 paragrafo pirmąjį sakinį: „Kad ir kokie nacionaliniai įstatymai būtų taikomi tvarkant aptariamus duomenis, kiekviena priežiūros institucija yra kompetentinga savo valstybės narės teritorijoje naudotis pagal 3 šio straipsnio dalį jai suteiktais įgaliojimais“ ir paskutinį to paties paragrafo sakinį dėl įsipareigojimo bendradarbiauti.

¹⁹ Tai ne tas atvejis, kai įranga naudojama tik tranzito per Bendrijos teritoriją tikslais.

Įsisteigimo sąvoka yra svarbi direktyvos 4 (1) straipsnyje ta prasme, kai valdytojas nėra įsisteigęs Bendrijos teritorijoje. Vieta, kurioje yra įsisteigęs valdytojas, reiškia efektyvų ir tikrąjį veiklos vykdymą stabilių susitarimų dėka ir turi būti apibrėžiama pagal Europos Bendrijų Teisingumo teismo precedentų teisę. Anot Teismo, į įsisteigimo įtsąvoką įeina faktinė veikla neapibrėžtam laikotarpiui įsteigtame padalinyje²⁰. Šį reikalavimą atitinka kompanija, įsisteigusi nustatytam laiko tarpui.

Kompanijos, teikiančios paslaugas interneto tinklapiuose įsisteigimo vieta nėra ta, kurioje yra jos tinklapį aptarnaujanti technika arba vieta, kurioje tinklapis yra prieinamas, bet vieta, iš kurios kompanija siekia vykdyti savo veiklą²¹. Pavyzdžiai: tiesioginės rinkodaros kompanija yra registruota Londone ir čia vysto savo europines kampanijas. Tai, kad ji naudojami tinklo serveriais Berlyne ir Paryžiuje, nekeičia fakto, kad ji įsteigta Londone.

2.2. Valdytojas

Valdytojas yra iš direktyvos paimta bendroji sąvoka, apibūdinanti fizinį ar juridinį asmenį, kuris vienas ar kartu su kitais nustato asmens duomenų tvarkymo tikslus ir priemones (Direktyvos 95/46/EB 2 (d) straipsnis). Apibrėžimas yra neutralus valdytojo įsisteigimo atžvilgiu. Jis yra platus, nes kiekvienas tvarkymas turi būti priskirtinas vienam ar keliems valdytojams. Pagal direktyvos 4 (1) straipsnį, tai reiškia, kad kažkur turi būti valdytojas. Atrodo būtina, kad būtų tvarkoma užsiimant veikla, patenkančia į Bendrijos teisės ir direktyvos taikymo sritį. Į direktyvo taikymo sritį nepapuola fizinio asmens asmeninėje ar ūkinėje veikloje atliekamas tvarkymas.

Kad direktyvos 4 (1) c straipsnis pradėtų veikti, valdytojas turi „asmens duomenų tvarkymo tikslais *naudotis* įranga” (ir ne tik duomenų tranzitui), kuri yra valstybės narės teritorijoje²². Tai reikštų, kad valdytojas yra aktyvus ir turi konkretų tikslą. Jo sprendimas dėl tvarkymo tikslų ir priemonių apima šį aspektą.

2.3. Įranga

Direktyvoje nėra šio termino apibrėžimo. Pagal Kolinzo Anglų kalbos žodyną, „įranga“ apibrėžiama kaip įrankių ar prietaisų rinkinys, sudarytas konkrečiam tikslui.

Įrangos pavyzdžiai yra personaliniai kompiuteriai, terminalai ir serveriai, kurie gali būti naudojami beveik visoms tvarkymo operacijoms atlikti.

Direktyvoje paaiškinta, kad *įranga* gali būti automatinė arba kitokia, jei ji yra naudojama ne tik informacijos perdavimui per Bendrijos teritoriją.

Tipinis atvejis, kai įranga naudojama tik perdavimui, yra telekomunikacijų tinklai (back bones, kabeliai ir t.t.), kurie yra interneto dalis ir kuriais interneto komunikacijos keliauja iš pradinio taško į paskirties tašką.

2.4. Naudojimasis įranga

²⁰ Byla C-221/89 Factortame [1991] ECR I-3905 §20.

²¹ Direktyva 2000/31/EB, konstatuojamoji dalis 19.

²² Reikia įsidėmėti, kad egzistuoja skirtumas tarp angliškoje 4 (1) c straipsnio versijoje vartojamo žodžio „equipment“ (įranga) ir vartojamo kitose 4 (1) c straipsnio versijose, kuriose jis artimesnis angliškam žodžiui „means“ (būdai). Kitose 4 (1) c straipsnio versijose vartojama terminija atitinka 2 (d) straipsnio formuluotę, apibrėžiančią valdytoją: asmuo, kuris nustato tvarkymo tikslus ir „būdus“. Reikėtų pripažinti, kad angliškame tekste ankstesnių direktyvos versijų (pavyzdžiui, pataisytame 1992 m. pasiūlyme) Taip pat vartojamas terminas „means“ (būdai) ir jis buvo pakeistas vykstant deryboms, vėlyvoje stadijoje, terminu „equipment“ (įranga), ką galime matyti 1995 m. kovo mėn. išdėstyame tekste.

Nustatymas, kada „duomenų valdytojas, tvarkydamas asmens duomenis, naudojami įranga“, direktyvos 4 (1) (c) straipsnyje yra lemiamas duomenų apsaugos įstatymo taikymo ES veiksnys.

Darbo grupė skatintų, kad ši duomenų apsaugos direktyvos taisyklė būtų apdairiai taikoma konkrečiais atvejais. Jos tikslas yra užtikrinti, kad asmenys būtų patenkinti nacionalinių duomenų apsaugos įstatymų teikiama apsauga ir nacionalinių duomenų apsaugos institucijų vykdoma duomenų tvarkymo priežiūra būtinaisiais atvejais, kai tai yra prasminga ir kai įmanoma vykdyti įstatymą, atsižvelgiant į tai, kad susiduriama su vienos valstybės sienas peržengiančia situacija.

Turėdama tai omenyje, Darbo grupė mano, kad tarp ES interneto vartotojo ir ne ES įsteigtos svetainės susiklostantiems santykiams nebūtinai yra taikytinas ES duomenų apsaugos įstatymas. Darbo grupė iškelė nuomonę, kad, tvarkydamas asmens duomenis, valdytojas turėtų naudotis jo žinioje esančia įranga.

Tuo pačiu metu nėra būtina, kad duomenų valdytojas visiškai kontroliuotų įrangą. Duomenų valdytojo disponavimo įranga apimtis gali skirtis. Būtinasis valdymo laipsnis duodamas, jei valdytojas, nustatydamas, koks įrangos darbo principas, daro atitinkamus sprendimus dėl duomenų turinio ir jų tvarkymo procedūros. Kitaip tariant, duomenų valdytojas nustato, kurie duomenys renkami, kaupiami, perduodami, keičiami ir t.t., koku būdu ir koku tikslu.

Darbo grupė mano, kad „naudojimosi“ sąvoka suponuoja du veiksnius: tam tikrą duomenų valdytojo vykdomą veiklą ir valdytojo ketinimą tvarkyti asmens duomenis. Tai reiškia, kad ne kiekvienam „įrangos“ „naudojimui“ Europos Sąjungos viduje yra taikoma direktyva.

Duomenų valdytojo teisės disponuoti nereikėtų painioti su įrangos nuosavybe ar priklausymu nei duomenų valdytojui, nei asmeniui. Iš tikrųjų, direktyvoje netaikoma svarba jokios įrangos nuosavybei.

Darbo grupės pateikta interpretacija atitinka direktyvos 4 (1) straipsnio nuostatos motyvaciją, pateiktą ES įstatymo leidėjo. 20 konstatuojamoje dalyje aiškinama, kad „*tai, kad duomenis tvarko trečioje šalyje įsteigtas asmuo, neturėtų kliudyti šioje direktyvoje numatytai asmenų apsaugai; kadangi tokiais atvejais tvarkymą turėtų reglamentuoti tos valstybės narės, kurioje įrengtos duomenų tvarkymui naudojamos priemonės, priimti teisės aktai, ir turėtų būti garantijos, kurios užtikrintų, kad šioje direktyvoje numatytos teisės ir prievolės yra tikrai gerbiamos*“. Tokia yra išvada, reikalinga, kad būtų pasiektas svarbus direktyvos tikslas, kuris yra „*užtikrinti, kad asmenims suteikiama visa apsauga, kurią jiems numato ši direktyva*“.

3. Praktiniai pavyzdžiai

Šiame skyriuje siekiama 4 straipsnyje numatytus orientyrus pavaizduoti konkrečiais tipiškų atvejų sprendimais. Žemiau aptariamų atvejų bendras bruožas yra tas, kad interneto vartotojas nebūtinai visada žino, ar tinklapis, kurį jis aplankys ir kuriam suteiks savo duomenis (to nežinodamas arba sąmoningai), yra ES ar kur nors kitur. Sričių pavadinimų be geografinių nuorodų negalima fiziškai surasti, nepateikus papildomos informacijos, ir netgi dėl jas turinčių negalima garantuoti, kad tinklapį valdantis serveris yra nurodytoje šalyje.

Atvejis A: Slapukas

Duomenų valdytojas nusprendžia rinkti asmens duomenis tekstinio failo (*cookie*) pagalba, kuris yra vartotojo personalinio kompiuterio kietajame diske, o jo kopijos gali būti saugomos svetainėje ar trečioje šalyje²³. Jei ir toliau perduodama informacija, slapuke

²³ *Slapukas* yra duomenų vienetas, kurį sukuria tinklo serveris ir kuris gali būti saugomas teksto failuose, esančiuose interneto vartotojo kietajame diske, o kopija gali būti laikoma svetainėje. Jie standartinė HTTP

saugoma informacija (todėl ir vartotojo PK) yra prieinama tinklapiui, kad duomenų valdytojas galėtų identifikuoti PK. Todėl valdytojas turi galimybę sujungti visą informaciją, kurią jis yra surinkęs anksčiau, su informacija, kurią jis renka vėliau. Tokiu būdu yra įmanoma sukurti pakankamai detalius vartotojo apibūdinimus.

Slapukai yra standartinė HTTP srauto dalis ir todėl gali būti lengvai pernešami IP-srauto. Slapuke gali būti bet kokia informacija, kokią svetainė pageidauja įtraukti į jį: žiūrėti puslapiai, skelbimai, vartotojo identifikavimo numeris ir taip toliau²⁴.

SET-COOKIE yra įdėta į HTTP antraštę²⁵, būtent nematomose nuorodose. Jeigu trukmė yra fiksuota²⁶, slapukas bus išsaugotas interneto vartotojo kietajame diske ir persiųstas atgal į jį sukūrusį tinklapį tam laikotarpiui.

Kaip paaiškinta aukščiau, į vartotojo PK galima žiūrėti kaip į įrangą pagal direktyvos 95/46/EB 4 (1) c straipsnį. Jis yra įrengtas valstybės narės teritorijoje. Duomenų valdytojas nusprendžia naudotis šia įranga asmens duomenų tvarkymo tikslais ir, kaip yra paaiškinta ankstesniuose paragrafuose, kelios techninės operacijos atliekamos nekontroliuojant duomenų subjektui. Duomenų valdytojas valdo vartotojo įrangą ir ši įranga naudojama ne tik informacijos tranzito per Bendrijos teritoriją tikslais.

Todėl Darbo grupė mano, kad nacionalinis valstybės narės, kurioje yra šis vartotojo personalinis kompiuteris, įstatymas taikomas klausimui, kokiomis sąlygomis jo asmens duomenys gali būti tvarkomi jo kietajame diske patalpinant slapukus.

Kaip buvo pabrėžiama ankstesnėse Darbo grupės rekomendacijose²⁷, vartotojas turi būti informuotas, kada jis gaus slapuką, saugomą ar siunčiamą interneto programinės įrangos. Vartotojui skirtoje žinutėje reikėtų tiksliai apibūdinti, kokią informaciją norima sagoti slapuke ir kokių tikslų, taip pat ir koks šio failo galiojimo terminas. Tada vartotojui turėtų būti suteiktas pasirinkimas sutikti ar ne, kad slapukas būtų siunčiamas ar saugomas, galimybė nustatyti, kokia informacijos dalis galėtų būti saugoma ar perkelta iš slapuko, atsižvelgiant, pavyzdžiui, į šio failo galiojimo laikotarpį arba į tai, kokie yra siunčiantys ir gaunantys tinklapiai²⁸.

srauto dalis, ir todėl gali būti lengvai pernešami IP-srauto. Slapuke gali būti unikalūs skaičiai (GUI, Global Unique Identifier), su kurio pagalba lengviau nustatomas asmuo, negu dinamiškų IP-adresų pagalba. Taip svetainė gali sekti, kokie yra vartotojo būdas ir ką jis mėgsta.

Slapukuose yra eilė URL adresų, kuriuose jie veikia. Kai naršyklė encounters URL adresus, konkretūs slapukai siunčiami į tinklo serverį.

Slapukai gali būti skirtingų rūšių: jie gali būti ilgai išliekantys, tačiau gali būti ir ribotos trukmės, vadinamieji sesijos slapukai.

²⁴ Žr. J. HAGEL III ir M. SINGER knygą *Net Worth: the emerging role of the intermediary in the race for customer information*, Harvard Business School Press, 1999, p. 275.

²⁵ Technškai kalbant, tap pat įmanoma įdiegti slapukus JavaScript'e arba <META-HTTP EQUIV> laukuose, esančiuose HTML kode.

²⁶ Nefiksuotos trukmės slapukai yra vadinami "session cookies" ir dingsta, kai naršyklė išsikrauna arba kai socket užsidaro.

²⁷ Rekomendacija 1/99 DG 17 „Nematomas ir automatinis asmens duomenų tvarkymas, atliekamas programinės ir techninės įrangos pagalba, internete“.

²⁸ Daugiau informacijos apie slapukų pobūdį ir kaip su jais elgtis pateikiama „Privatumas internete – Integruotas ES požiūris į duomenų apsaugą internete“ Darbo dokumentas, WP 37 5063/00. 16 puslapyje yra bendras aprašymas „Slapukai yra duomenų vienetai, kuriuos galima saugoti tekstiniuose failuose, kuriuos galima patalpinti interneto vartotojo kietajame diske, o kopija gali būti saugoma svetainėje“.

Atvejis B: JavaScript, reklaminės užsklandos ir kiti panašūs **applications**

JavaScript'ai yra programinės įrangos **applications** atsiųsti iš tinklapio į vartotojo kompiuterį ir leidžiantys tolimiems serveriams vartotojo PK **run applications**. Priklausomai nuo programinės įrangos turinio, JavaScript'ai gali būti naudojami informacijos pateikimui tinklapyje, bet ir virusų įvedimui į kompiuterį (vadinamieji piktavališkieji Java) ir/arba rinkti ir tvarkyti kompiuteryje esančius asmens duomenis. Kai duomenų valdytojas nusprendžia naudotis šiais prietaisais rinkdamas ir tvarkydamas asmens duomenis, jis naudojasi įranga padal direktyvą ir privalės laikytis ES teisės nuostatų.

Reklamos agentūra, susitarusi su svetainės savininkais (pvz., **search engine sites**), užsako naršyklę (plačiau, kompiuterį), kad duomenų subjektas prisijungtų ne tik prie **search engine**, kuriuos jis/ji nori aplankyti, bet ir prie reklamos agentūros serverio. Tokiu būdu reklamos agentūra gali ne tik siųsti reklamines užsklandas²⁹ į duomenų subjekto ekraną, bet ir naudotis vartotojo naršykle renkantis ir **content data that individual sends to the search engine**. Reklaminės užsklandos į reikalingą svetainę patalpintos per nematomą nuorodą į reklamos agentūrą³⁰. Todėl iš savo buvimo vietos duomenų valdytojas turi kontroliuoti naršyklės funkcionavimą, kad ji susisietų ir perduotų informaciją trečiajam šaliai.

Be to, kad galėtų klientui pateikti pačią „tinkamiausią“ reklaminių skelbimų tinklo reklamuotojai sukuria **profiles** nustatydami slapukus nematomose nuorodose. Priklausomai nuo naršyklės konfigūracijos, vartotojas gali žinoti, kad ruošiamasi patalpinti slapuką ir gali duoti arba ne sutikimą. Kliento **profile** yra susijęs su skelbimų agentūros slapuko identifikacijos numeriu ir jis gali būti padidintas kiekvieną kartą, kai klientas, sudaręs sutartį su skelbėju, lankosi svetainėje. Tokiu būdu iš vartotojo kompiuterio pagalba bus papildomai renkami asmens duomenys ir **without his intervention every time the Internet user visits the web site that contains the banner**.

Direktyva taip pat taikoma slapta įranga, kuri yra į asmens kompiuterį slapta instaliuotos programinės įrangos dalis, surinktai informacijai, pavyzdžiui, kada persiunčiama didesnės apimties programinė įranga (pvz., muzikos grotuvų programinė įranga), kad atgal būtų atsiunčiama su duomenų subjektu susijusi informacija (pvz., muzikiniai pavadinimai, kurių asmenys nori paklausti). Tokios rūšies programinė įranga populiariai yra vadinama **E.T. applications** „nes, jeigu jos prisijungia prie vartotojo kompiuterio ir sužino, ką nori sužinoti, jos daro tai, ką padarė Steven Spielberg'o ateivis: skambina namo“³¹.

Šios naujos stebėjimo programinės įrangos **applications** dažnai naudojasi JavaScript ir panašia technologija ir aiškiai naudojasi duomenų subjekto įranga (kompiuteriu, naršykle, kietuoju disku ir t.t.) duomenų rinkimui ir jų persiuntimui į kitą vietą. Kadangi šios technologijos pagal apibrėžimą naudojamos neinformavus vartotojo (pavadinimas tuo atžvilgiu yra aiškus), jos yra nematoma ir neteisėta tvarkymo forma.

79 puslapyje **details 'Cookie Killers' dealing with both the response by industry to deal with the privacy problems of cookies-the cookie opposition mechanism, and that of privacy activists- independent programmes such as cookie washer, cookie cutter and cookie master.**

²⁹ Reklaminiai segmentai yra mažos grafinės dėžutės, pasirodančios viršuje arba esančios svetainės turinyje.

³⁰ Žr. daugiau informacijos 8 skyriuje, Cybermarketing, DG 37, Privatumas internete.

³¹ Žr. Adamo Koheno straipsnį Time žurnale 2000 m. liepos 31 d.: *Kaip saugoti savo privatumą: kas jus stebi? Jie vadinami E.T. programomis. Jie jus seka ir praneša "skambindami į namus". Milijonai žmonių nesąmoningai juos perkelia.*

29 straipsnio Darbo grupė suvokia tai, kad be šių dviejų ankstesniame skyriuje paminėtų pavyzdžių, praktikoje pasitaiko kitokių su internetu susijusių atvejų, kuriuos aiškinti gali būti sunkoka, iš dalies dėl techninio kai kurių naudojamų sistemų sudėtingumo.

Darbo grupė ir toliau svarstys šį klausimą ateityje ir galėtų kreiptis į kitus praktikos atvejus, atsižvelgdama į nacionalinę patirtį ir technikos pasiekimus, kurie ateityje gali būti labai reikšmingi.

Ji nori pabrėžti, kad netgi tais atvejais, kai direktyvos taikymas nėra visiškai aiškus, Darbo grupė išipareigojusi tęsti dialogą su trečiųjų šalių kompanijomis ir organizacijomis, kurios renka asmens duomenis Europos Sąjungoje, kad būtų keliami duomenų apsaugos standartai duomenų subjektams.

4. Ką tai reiškia praktiškai?

a) Asmens duomenų rinkimą lemiančių principų taikymas

Visais atvejais ES duomenų apsaugos įstatymo taikymas be viso kito reiškia :

- Siekdamas teisingai ir teisėtai rinkti asmens duomenis, duomenų valdytojas turi aiškiai apibrėžti tvarkymo tikslus.
- Duomenų valdytojas taip pat turi užtikrinti, kad duomenys yra pakankami, tinkami ir nepertekliniai ryšium su jų rinkimo tikslu.
- Rinkimas turi remtis teisiniu pagrindu (nedviprasmišku sutikimu, sutarties vykdymu, teisinės prievolės laikymusi, siekiant duomenų valdytojo teisėtų interesų ir t.t.) ir asmuo turi teisę gauti, ištaisyti ar ištrinti savo duomenis.
- Asmuo turi būti bent jau informuotas, kas yra duomenų valdytojas ir jo atstovas, jei toks yra, koks duomenų rinkimo tikslas, gavėjas ir kokios jo teisės³².
- Kitas svarbus aspektas yra duomenų tvarkymo saugumas, kuris gali reikalauti, kad valdytojas, iš karto pradėdamas tvarkymą, taikytų konkrečias technines ir organizacines priemones, apsaugančias duomenis nuo atsitiktinio ar neteisėto sunaikinimo ar atsitiktinio praradimo, pakeitimo, neteisėto atskleidimo ar galimybės gauti duomenis, ypač kai duomenys yra perduodami per tinklą. Tokios priemonės garantuos apsaugos lygį, atitinkantį esančią riziką ir duomenų rūšį.
- Jautriųjų duomenų rinkimą reguliuoja konkrečios, ypatingai saugumo reikalavimus nagrinėjančios, nuostatos³³.

Kaip duomenų apsaugos direktyva taikoma duomenų tvarkymui interneto svetainėse, detaliau paaiškinta Darbo grupės rekomendacijoje 2/2001 dėl tam tikrų minimalių reikalavimų asmens duomenų rinkimui internete Europos Sąjungoje³⁴.

³² Direktyvos 10 straipsnis teigia, kad, kai yra būtina užtikrinti duomenų subjekto atžvilgiu teisingą duomenų tvarkymą, turi būti pateikta papildoma informacija.

Elektroninių pėdsakų atveju, asmuo privalo turėti galimybę sutikti ar atsisakyti, kad būtų paliktas elektroninis pėdsakas, taip pat ir galimybę apibrėžti, kokius duomenis jis nori tvarkyti elektroninio pėdsako pagalba ir kokių ne.

³³ Kai kurios valstybės narės gali reikalauti išankstinės patikros, prieš pradėdant jautriųjų duomenų tvarkymą.

b) Procedūriniai aspektai

Pagal direktyvos 95/46/EB 4 (2) straipsnį, duomenų valdytojas privalo paskirti atstovą, įsteigtą tos valstybės narės teritorijoje, kurioje yra įranga.

Informaciją dėl duomenų valdytojo ir atstovo tapatybės galima nesunkiai įtraukti į tinklapio privatumo sutartį arba į bendrą informaciją apie atsakingojo už tinklapį tapatybę, kad už svetainę atsakingą duomenų valdytoją galima būtų lengva nustatyti ir su juo susisiekti.

Galima pasiūlyti palčiai naudotis galimybe, kad vienas atstovas galėtų veikti kelių valdytojų vardu arba numatyti kitus pragmatiškus sprendimus.

Direktyva numato kelis variantus dėl pranešimo nacionalinei duomenų apsaugos institucijai apie ketinamą tvarkymo operaciją (būtent rinkimą). Pagal 18 (1) straipsnio pirmąjį sakinį, duomenų valdytojas ar jo atstovas privalo pranešti priežiūros institucijai prieš atlikdamas bet kurią tvarkymo operaciją arba operacijų grupę. 19 (1) (a) straipsnis nurodo, kad pranešime, šalia kitų dalių, turi būti duomenų valdytojo ir jo atstovo vardas ir adresas.

Pagal 18 (2) straipsnio antrąją pastraipą, valstybės narės gali supaprastinti reikalavimą pranešti arba atleisti nuo jo dviem atvejais: esant tvarkymo operacijų kategorijoms, kurios neturėtų neigiamai paveikti duomenų subjektų teisių ir laisvių arba kai duomenų valdytojas paskiria pareigūną asmens duomenų apsaugai, kuris, nepriklausomai veikdamas, užtikrina, jog duomenų valdytojas laikytųsi duomenų apsaugos įstatymų³⁵.

Darbo grupė supranta, kad šių nuostatų taikymas gali sukelti praktinių problemų ir galbūt vėliau skirs šiems klausimams dėmesio.

c) Įgyvendinimas

Yra akivaizdu, jog užtikrinti taisyklių laikymąsi tarptautiniame kontekste nėra taip paprasta, kaip vienoje valstybėje. Piliečiai turi tai suvokti. Vis dėlto, egzistuoja kelios galimybės ir jos gali būti plėtojamos, siekiant deramo įstatymų įgyvendinimo.

Geras teisės aktų laikymasis visų pirma pareikalauja, kad Europos ir tarptautinės organizacijos žinotų, kokie yra direktyvos reikalavimai dėl duomenų rinkimo Europos Sąjungoje. Platesnis šios rekomendacijos paskleidimas gali būti tik pirmas žingsnis. Čia įtraukiami ir technologiniai sprendimai, teikiantys iš aksto numatytą asmens duomenų rinkimo struktūrą, kuri sujungs apibūdintus reikalavimus į programinės įrangos prietaisus, naudojamus asmens duomenų rinkimui. Darbo grupė jau yra minėjusi apie galimybę sugalvoti produkto leidimo procedūras, kurios apimtų patikrą, kaip laikomasi asmens duomenų apsaugos teisinių reikalavimų. Europos ženklų/tinklo patvirtinimų sistema, atvira ir ne ES svetainėms, turėtų būti tokios veiklos kertiniu akmeniu.

Be to, konkrečiu atveju asmuo Europos Sąjungoje, kuris turi problemų dėl ne ES įkurtos svetainės, galėtų pateikti svarstyti savo bylą kompetentingai nacionalinei duomenų apsaugos priežiūros institucijai. Ši institucija nustatytų, ar direktyva, atitinkamai ir nacionalinis duomenų apsaugos įstatymas, gali būti taikomas. Jei taip, institucija dėl problemos sprendimo galėtų užmegzti ryšius su užsienio svetaine. Jeigu byla pateikiama valstybės narės, kurioje gyvena asmuo, teismui, teismas nuspręs, ar jis gali imti bylą į savo jurisdikciją (ką pagal tarptautinę procesinę teisę galima daryti, nes labiausiai suinteresuota šalis yra asmuo, gyvenantis toje pačioje teritorijoje, kur yra teismas). Kai teismas turi

³⁴ Žr. šiuo klausimu DG 43 rekomendaciją 2/2001 dėl tam tikrų minimalių reikalavimų smens duomenų tvarkymui internete Europos Sąjungoje. Reikia diskutuoti, ar visi DG 43 paminėti veiksniai taikomi ir duomenų rinkimui internete ES, kurį atlieka už ES ribų įsikūrę duomenų valdytojai.

³⁵ Dėl konkrečių nacionalinio įstatymo nuostatų, įgyvendinančių šį direktyvos straipsnį, žr.: http://europa.eu.int/comm/internal_market/en/dataprot/law/impl.htm

jurisdikciją, jis taiko direktyvos 95/46/EB 4 straipsnį, atitinkamai ir nacionalinį įstatymą, perkeldamas jį ir teismas gali nustatyti, kad užsienio tinklapis to asmens duomenis tvarkė neteisėtai ir neteisingai. Daugelyje trečiųjų šalių jau leidžiama sutikti su teismo sprendimu ir jį vykdyti, bet net jeigu jos to nedaro, yra pavyzdžių, kai užsienio svetainės visgi gali vadovautis teismo sprendimu ir pritaikyti duomenų tvarkymą, siekdamos vystyti verslą ir išlaikyti gerą komercinį įvaizdį.

Trečiojoje šalyse, kur egzistuoja duomenų apsaugos taisyklės ir institucijos, tai įgyvendinti yra akivaizdžiai mažiau problematiška.

5. Išvados

- 29 straipsnio duomenų apsaugos darbo grupė yra tos nuomonės, kad nacionalinių įstatymų interpretavimas, koks jis pateikiamas šiame darbo dokumente, būtų labai naudingas, siekiant teisinės už Europos Sąjungos ribų įsisteigusių svetainių apsaugos. Darbo grupė yra įsitikinusi, kad aukštą asmenų apsaugos lygį galima užtikrinti tik tada, jei už Europos Sąjungos ribų įsisteigusios, tačiau įrangą naudojančios ES, svetainės, kaip paaiškinta šiame darbo dokumente, gerbs asmens duomenų tvarkymo, ypač rinkimo, garantijas ir asmenų teises, pripažįstamas Europoje ir bet kuriuo atveju taikytinas visiems Europos Sąjungoje įsteigtiems tinklapiams.
- 29 straipsnio Duomenų apsaugos darbo grupė mano, kad Europos duomenų apsaugos taisyklių pragmatinio propagavimo programos tobulinimas padės trečiųjų šalių duomenų valdytojams geriau suprasti, vykdyti ir parodyti privatumo laikymąsi. Europos ženklų/tinklo patvirtinimų sistema, atvira ir ne ES svetainėms, turėtų būti tokios veiklos kertiniu akmeniu.
- 29 straipsnio duomenų apsaugos darbo grupė skatina Komisiją atsižvelgti į šį darbo dokumentą savo tolesniame darbe.

Sudarytas Briuselyje, 2002 m. gegužės 30 d.

Darbo grupei

Pirmininkaujantis

Stefano RODOTA

Į lietuvių kalbą išvertė Valstybinės duomenų apsaugos inspekcijos vyr. referentė
Inga Rimkevičienė