EUROPOS DUOMENŲ APSAUGOS PRIEŽIŪROS PAREIGŪNAS

Europos duomenų apsaugos priežiūros pareigūno nuomonės dėl Komisijos komunikato Europos Parlamentui ir Tarybai dėl pasitikėjimo ES ir JAV duomenų mainais atkūrimo ir Komisijos komunikato Europos Parlamentui ir Tarybai dėl „saugaus uosto“ nuostatų veikimo ES piliečių ir ES įsisteigusių bendrovių požiūriu santrauka

(Visą šios nuomonės tekstą anglų, prancūzų ir vokiečių kalbomis galima rasti EDAPP interneto svetainėje (www.edps.europa.eu))

(2014/C 116/04)

I. Įvadas

I.1. *Konsultacijos su EDAPP*

1. 2013 m. lapkričio 27 d. Komisija priėmė Komisijos komunikatą Europos Parlamentui ir Tarybai dėl pasitikėjimo ES ir JAV duomenų mainais atkūrimo ([1]) (toliau – komunikatas dėl pasitikėjimo atkūrimo). Prie šio komunikato pridedama ataskaita apie ES ir JAV *ad hoc* duomenų apsaugos darbo grupės ES pirmininkų išvadas (toliau – darbo grupė ir ataskaita).

2. Tą pačią dieną Komisija priėmė Komisijos komunikatą Europos Parlamentui ir Tarybai dėl „saugaus uosto“ nuostatų veikimo ES piliečių ir ES įsisteigusių bendrovių požiūriu ([2]) (toliau – komunikatas dėl „saugaus uosto“).

3. EDAPP teigiamai vertina tai, kad jam buvo suteikta galimybė pateikti Komisijai neoficialias pastabas prieš priimant minėtus dokumentus. Šiuos dokumentus Komisija priėmė po to, kai buvo paviešinta informacija apie JAV žvalgybos tarnybų vykdomas sekimo programas. Atsižvelgdamas į šių sekimo programų poveikį fizinių asmenų teisėms į privatumą ir jų asmens duomenų apsaugą ES, EDAPP šią nuomonę nusprendė priimti savo iniciatyva.

I.2. *Komisijos dokumentų tikslas ir taikymo sritis*

a) Komunikatas dėl pasitikėjimo atkūrimo ir ataskaita

4. Komunikate aptariami tolesni veiksmai, kurių reikia imtis paviešinus informaciją apie didelės apimties žvalgybos duomenų rinkimo programas (toliau – programos arba paviešintos programos) ir dėl šių programų poveikio ES ir JAV tarpusavio pasitikėjimui. Komunikate neminima paviešinta informacija, susijusi su panašia veikla ir (arba) bendradarbiavimu, kurį kartu su JAV vykdo ES valstybės narės arba kitos trečiosios valstybės.

5. Ataskaitoje, siekiant nustatyti su programomis susijusius faktus ir jų poveikį ES pagrindinėms teisėms ir ES piliečių asmens duomenims, sulyginamos ES ir JAV *ad hoc* duomenų apsaugos darbo grupės, kuri buvo sudaryta po 2013 m. liepos 18 d. COREPER posėdžio, ES pirmininkų išvados. Ataskaitoje analizuojama JAV teisinė sistema ([3]), duomenų rinkimo ir tolesnio tvarkymo procedūros ([4]) ir esami priežiūros ir teisių gynimo mechanizmai.

([1]) COM(2013) 846 final.

([2]) COM(2013) 847 final.

([3]) Visų pirma Konstitucija, kaip ją išaiškino Aukščiausiasis Teismas; 1978 m. Užsienio žvalgybos stebėjimo įstatymo (angl. *Foreign Intelligence Surveillance Act*, FISA) 702 straipsnis (iš dalies pakeistas 2008 m. FISA pakeitimų įstatymu (angl. FISA *Amendments Act*), 50 U.S.C., 1881a straipsnis) ir 2001 m. JAV Patriotų įstatymo (angl. USA PATRIOT *Act*) 215 straipsnis (kuriuo taip pat buvo pakeistas FISA, 50 U.S.C., 1861 straipsnis) ir vykdomoji nutartis Nr. 12333.

([4]) Remiantis JAV darbo grupei pateikta informacija ir išslaptintais dokumentais, įskaitant Užsienio žvalgybos stebėjimo teismo (toliau – FISC) nuomones ir viešus dokumentus, pvz., vidaus FTB operacijų advokato bendrąsias gaires.

6. Ataskaitoje minima „antroji kryptis“, kuri taip pat buvo numatyta per 2013 m. liepos 18 d. COREPER posėdį. Ataskaitoje nurodyta, kad pagal šią „antrąją kryptį“ ES institucijos gali užduoti JAV valdžios institucijoms klausimus, susijusius su tariamu ES institucijų ir diplomatinių misijų sekimu, o valstybės narės gali rengti dvišales diskusijas su JAV valdžios institucijomis dėl su jų nacionaliniu saugumu susijusių klausimų.

7. Ataskaitoje taip pat nurodoma, kad dėl šios „antrosios krypties“ išskyrimo darbo grupės diskusijos buvo suvaržytos ir jai buvo pateikiama ne visa informacija. EDAPP šiuo atžvilgiu nepateikta jokios informacijos dėl „antrosios krypties“ arba paralelinės darbo grupės sukūrimo. Todėl Komisijos prašoma informuoti EDAPP apie išvadas dėl „antrosios krypties“, visų pirma atsižvelgiant į tariamą ES institucijų ir diplomatinių misijų sekimą.

b) Komunikatas dėl „saugaus uosto“

8. Komunikate dėl „saugaus uosto“ analizuojamos „saugaus uosto“ funkcijos, nustatomi trūkumai ir pateikiami pasiūlymai dėl galimų patobulinimų. Jame pripažįstama, kad duomenų, perduodamų tarp ES ir JAV, kiekis didėja ir kad vis daugiau įmonių įsipareigoja laikytis „saugaus uosto“ principų. Priminusi „saugaus uosto“ struktūrą ir veikimo principus, Komisija pabrėžia poreikį geriau užtikrinti, kad įsipareigojusios įmonės ir jų subrangovai laikytųsi principų. Kaip nurodoma komunikate, šiuo atveju būtų reikalaujama, kad įsipareigojusios įmonės veiksmingiau perkeltų „saugaus uosto“ principus į savo privatumo politiką ir leistų su ja susipažinti visuomenei. Federalinė prekybos komisija turėtų aktyviais veiksmais užtikrinti, kad šių principų būtų laikomasi. Be to, duomenų apsaugos institucijos turėtų dalyvauti didinant informuotumą apie „saugų uostą“ ES ir tai jos turi daryti visų pirma imdamosi veiksmų ES duomenų apsaugos kolegijoje. Komisija taip pat siūlo sprendimus, kuriais siekiama patobulinti alternatyvaus ginčo sprendimo mechanizmus.

9. Atsižvelgdama į prieigą prie duomenų, perduotų pagal „saugaus uosto“ schemą, ir tolesnį jų tvarkymą JAV valdžios institucijose, Komisija pabrėžia, kad tokia prieiga ir tvarkymas turėtų apsiriboti tik tuo, kas yra būtina ir proporcinga. Ji taip pat reikalauja, atidžiai stebėti taikomus privatumo politikos apribojimus, kuriais siekiama tenkinti nacionalinio saugumo, viešojo intereso arba teisėsaugos reikalavimus, kad jais nebūtų pažeidžiama užtikrinama apsauga. Komisija taip pat ragina įsipareigojusias įmones laikytis skaidrumo principų dėl šių apribojimų ir jų poveikio ryšio konfidencialumui ir taip didinti piliečių informuotumą.

I.3. *Šios nuomonės taikymo sritis ir tikslas*

10. Šioje nuomonėje daugiausia dėmesio skiriama komunikatui dėl pasitikėjimo atkūrimo ir komunikatui dėl „saugaus uosto“, kiek jis susijęs su pirmuoju komunikatu. Todėl jame tiesiogiai nekomentuojama su ES valstybėmis narėmis susijusi paviešinta informacija, nepaisant to, ar ji susijusi su bendradarbiavimu su JAV, ar pačiomis valstybėmis narėmis arba sekimo veikla, kurią atlieka trečiosios valstybės, išskyrus JAV.

11. Nuomonėje pirmiausia pateikiamos pastabos dėl bendro komunikate įtvirtinto požiūrio į pasitikėjimo atkūrimą. II dalyje trumpai analizuojami susijusios teisinės sistemos taikymo ir jos sukeliamų pasekmių klausimai, įskaitant pastabas dėl komunikato dėl „saugaus uosto“. Šiuo metu 29 straipsnio duomenų apsaugos darbo grupė ([1]) nagrinėja taikytiną ES ir tarptautinę teisinę sistemą, todėl šioje nuomonėje šis klausimas nėra pernelyg išsamiai aptariamas. III dalyje pateikiamos Komisijos rekomendacijos dėl tolesnių veiksmų, kurių reikia imtis.

I.4. *Pastabos dėl komunikate dėl pasitikėjimo atkūrimo įtvirtinto požiūrio*

12. Komunikate daugiausia dėmesio skiriama faktui, kad pasitikėjimas tarp ES ir JAV, kaip strateginių partnerių, stipriai nukentėjo dėl paviešintos informacijos apie programas ir jis turi būti atkurtas. EDAPP teigiamai vertina tai, kad šis faktas nėra ginčijamas.

([1]) Pagal Direktyvą 95/46/EB įsteigta 29 straipsnio duomenų apsaugos darbo grupė yra nepriklausomas patariamasis organas. Ją sudaro ES nacionalinių duomenų apsaugos institucijų atstovai, EDAPP ir Komisija.

13. Vis dėlto programos, kurių įgyvendinimas tam tikrais atvejais aiškiai patvirtinamas ataskaitoje ([1]), daro poveikį ne tik pasitikėjimui, bet ir ES bei Europos Tarybos pirminėje ir antrinėje teisėje nustatytoms teisėms, visų pirma teisėms į privatumą ir duomenų apsaugą. Taip pat matyti, kad tai yra didelės apimties žvalgybos duomenų rinkimo programos, kurios faktiškai įgyvendinamos pagal JAV teisinę sistemą ([2]), kaip išaiškino JAV Aukščiausiasis Teismas ([3]). Ataskaitoje taip pat patvirtinama, kad trūksta apsaugos ir saugumo priemonių, nustatytų teisių, priežiūros ir teisių gynimo priemonių, kuriomis pagal JAV teisinę sistemą galėtų pasinaudoti ES piliečiai ([4]).

14. Kaip ne kartą pabrėžė Komisija, piliečių ir įmonių pasitikėjimas interneto ryšiu priklauso nuo galimybės pasinaudoti veiksmingomis techninėmis privatumo, tiksliau tariant, ryšio konfidencialumo apsaugos priemonėmis. Šį poreikį taip pat pripažino JAV žvalgybos ir ryšio technologijų peržiūros grupė ([5]), kuri pateikė keletą rekomendacijų, padėsiančių atkurti pasitikėjimą šifravimo priemonėmis, komercine programine įranga ir mechanizmų, padedančių greitai pašalinti programinės įrangos trūkumus, veikimu. Manoma, kad sumažėjęs pasitikėjimas šiomis sistemomis yra vienas žalingiausių padarinių, kurį neseniai vykusiose diskusijose dėl ryšio žvalgybos operacijų nurodė kompetentingiausi saugumo ekspertai ([6]). Atsižvelgiant į veiksmingo kibernetinio saugumo Europoje svarbą, šį techninį ir politinį uždavinį, remiantis Komisijos iniciatyva, reikėtų spręsti ES lygmeniu.

15. Komunikato 3 dalyje Komisija aptaria būsimus veiksmus, kurių reikia imtis siekiant atkurti pasitikėjimą duomenų perdavimu tarp ES ir JAV. EDAPP teigiamai vertina šią dalį, kurioje daugiausia dėmesio skiriama esamos teisinės sistemos patobulinimams ir siūlomos naujos priemonės. Tačiau Komisija nenagrinėja, kokią įtaką programos turėjo taikytinoms nacionalinėms, ES ir Europos Tarybos priemonėms. EDAPP mano, kad komunikate reikėjo daugiau dėmesio skirti poveikiui esamoms teisinėms priemonėms.

IV. Išvados

79. EDAPP teigiamai vertina Komisijos numatytas priemones, tačiau atkreipia dėmesį į tai, kad atskleista JAV žvalgybos agentūrų sekimo veikla poveikį turi ne tik ES ir JAV duomenų srautams. Ji taip pat turi poveikį esamoms ir įgyvendinamoms ES piliečių teisėms į privatumo užtikrinimą ir jų asmens duomenų apsaugą. Šios teisės yra numatytos ES ir Europos Tarybos pirminėje ir antrinėje teisėje. Todėl EDAPP apgailestauja, kad komunikate dėl pasitikėjimo atkūrimo nėra skirta daugiau dėmesio poveikiui esamoms teisinėms priemonėms.

80. EDAPP norėtų atkreipti dėmesį į keletą aspektų, kuriuos Komisija turėtų labiau išplėtoti apibrėždama tolesnius veiksmus, kurių reikia imtis, ir nurodo, kad:

— teisingas dabartinės Europos duomenų apsaugos teisinės sistemos taikymas ir užtikrinimas yra būtinas ne tik pagal teisės aktus, tai taip pat iš esmės padėtų atkurti pasitikėjimą. Ši nuostata taip pat taikoma priemonėms, reglamentuojančioms tarptautinį duomenų perdavimą tarp ES ir JAV, įskaitant esamus „saugaus uosto“ principus,

— Komisija turėtų priminti, kad nacionalinio saugumo tikslais nustatytos pagrindinių teisių išimtys arba apribojimai yra pateisinami ir leistini tik tuo atveju, jeigu jie yra būtini, proporcingi ir atitinka EŽTT ir Teisingumo Teismo jurisprudenciją,

([1]) Žr. ataskaitos p. 5, 10 ir 26, kuriuose, remiantis išslaptintomis Užsienio žvalgybos stebėjimo teismo nuomonėmis, patvirtinama, kad „JAV žvalgybos agentūros gali naudoti 702 straipsnyje nurodytus plataus masto metodus, pvz., PRISM duomenų rinkimą iš interneto paslaugų teikėjų arba „išsiuntimo srauto“ duomenų, kurie perduodami per JAV, rinkimą“.

([2]) JAV patvirtino, kad žvalgybos duomenys, kai reikia gauti duomenis apie ne JAV asmenis, gali būti renkami remiantis kitais teisiniais pagrindais, tačiau nepateikė išsamios informacijos apie teisėsaugos institucijas ir taikytinas procedūras. Darbo grupei nurodyti ne visi susiję teisiniai pagrindai (žr. ataskaitos p. 13).

([3]) Žr. ataskaitos p. 4–12.

([4]) Žr. ataskaitos p. 26–27.

([5]) „Liberty and Security in a Changing World“, Prezidento sudarytos žvalgybos ir ryšių technologijų peržiūros grupės ataskaita ir rekomendacijos, visų pirma 25, 29 ir 30 rekomendacijos. Galima rasti adresu http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

([6]) B. Schneier, C. Soghoian, 2013 m. rugsėjo 6 d. ataskaita, galima rasti adresu http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security; B. Preneel, ISSE 2013, baigiamoji pastaba, „The Cryptographic Year in Review“, galima rasti adresu http://homes.esat.kuleuven.be/~preneel/preneel_isse13.pdf.

— EDAPP visiškai sutinka, kad siekiant konsoliduoti ir tobulinti ES duomenų apsaugos sistemą, reikia skubiai priimti tinkamus esminius duomenų apsaugos reformos pasiūlymus, kad būtų užtikrinta veiksmingesnė ir nuoseklesnė asmens duomenų ir privatumo apsauga visose ES teisės aktų taikymo srityse. Pasiūlymuose taip pat turėtų būti numatyta tinkama duomenų apsauga tuo atveju, kai šie duomenys toliau naudojami teisėsaugos tikslais, ir sprendžiant tarptautinės jurisdikcijos kolizijos klausimus,

— „saugaus uosto“ principai turėtų būti peržiūrimi ir sugriežtinami atsižvelgiant į Komisijos rekomendacijas. EDAPP rekomenduoja nustatyti griežtesnius terminus, per kuriuos turi būti imamasi šių veiksmų, įskaitant tinkamą tolesnę jų stebėseną tuo atveju, jei būtų pastebėti kokie nors trūkumai,

— ES ir JAV teisėsaugos institucijų bendradarbiavimui taikomos duomenų apsaugos priemonės turi būti sugriežtintos. Per dabartines derybas dėl bendro susitarimo neturėtų būti įteisinamas masinis duomenų perdavimas, bet paisoma esamos duomenų apsaugos sistemos ir dabartinės jos peržiūros rezultatų. Visų pirma reikėtų užtikrinti galimybę visiems duomenų subjektams, nepaisant jų pilietybės, pasinaudoti veiksmingais teisių gynimo mechanizmais. Vėliau šis principas turėtų būti taip pat taikomas esamiems tarptautiniams susitarimams, prireikus nustatant tinkamas pereinamąsias nuostatas,

— Komisija turėtų remti JAV administracijos ir JAV Kongreso pastangas priimti bendro pobūdžio įstatymą dėl privatumo, kuriame būtų numatytos griežtos apsaugos priemonės ir tinkama priežiūra, visų pirma tose srityse, kuriose šiuo metu iš esmės neužtikrinama privatumo apsauga,

— šiuo metu vykstančios derybos, kuriose siekiama priimti TTIP, neturėtų daryti neigiamo poveikio piliečių asmens duomenų apsaugai. Tuo pat metu Komisija turėtų apsvarstyti galimybę nustatyti bendrą tikslą, t. y. laipsniškai didinti privatumo ir duomenų apsaugos teisinių sistemų sąveiką, prie kurio įgyvendinimo galėtų prisidėti JAV, kaip nurodyta pirmiau,

— tarptautiniu lygmeniu remiant privatumo standartus reikėtų:

  i. visapusiškai didinti naujų tarptautinių priemonių atitiktį Europos duomenų apsaugos sistemai;

  ii. skatinti, kad trečiosios valstybės, visų pirma JAV, laikytųsi Europos Tarybos Konvencijos Nr. 108;

  iii. skatinti nustatyti tarptautinę priemonę, kurioje būtų reikalaujama laikytis duomenų apsaugos standartų vykdant žvalgybos veiklą. Ši priemonė galėtų būti nustatyta JT lygmeniu remiantis Tarptautinio pilietinių ir politinių teisių pakto (angl. ICCPR) 17 straipsniu,

— vykdant sekimo veiklą visada reikėtų laikytis pareigos gerbti teisinės valstybės ir būtinumo ir proporcingumo demokratinėje visuomenėje principus. Todėl reikėtų pateikti paaiškinimus apie visų susijusių lygmenų teisines sistemas ir prireikus jas papildyti. Šiose sistemose reikėtų numatyti tinkamus ir pakankamai griežtus priežiūros mechanizmus,

— ES institucijos ir visi valstybių narių susiję subjektai, kaip duomenų valdytojai, taip pat tiesiogiai atsako už veiksmingą IT saugumo užtikrinimą. Tai apima duomenų saugumui kylančios rizikos vertinimo atlikimą tinkamu lygmeniu. Šiuo įpareigojimu taip pat reikalaujama skatinti atlikti iššifravimo mechanizmų mokslinius tyrimus ir duomenų valdytojų ir piliečių informuotumo apie parduodamų arba naudojamų produktų keliamą riziką privatumui ir reikalaujama, kad produktų kūrėjai naudotų konkrečius dizaino kūrimo metodus, kad tokios rizikos būtų išvengta arba ji būtų bent jau sumažinta. ES turėtų inicijuoti švietimo iniciatyvas, susijusias su internete tvarkomų duomenų saugumu.

Priimta Briuselyje 2014 m. vasario 20 d.

Peter HUSTINX

Europos duomenų apsaugos priežiūros pareigūnas