

Valdybos nuomonė (70 str. 1 dalies b punktas)



Opinion of the Board (Art. 70.1.b)



Nuomonė 23/2018 dėl Komisijos pasiūlymų dėl Europos elektroninių įrodymų baudžiamosiose bylose pateikimo ir saugojimo orderių (70 straipsnio 1 dalies b punktas)

Priimta 2018 m. rugsėjo 26 d.

Turinys

Ivadas.....	3
1. Teisinis reglamento pasiūlymo pagrindas (SESV 82 straipsnis).....	4
2. Elektroninių įrodymų būtinybė, palyginti su savitarpio teisinės pagalbos susitarimais ir ETO	5
a) Elektroninių įrodymų būtinybė, palyginti su ETO ir savitarpio teisinės pagalbos susitarimuose numatytais apsaugos priemonėmis	5
b) Abipusio baudžiamumo principo atsisakymas	6
c) Tiesioginio kreipimosi į bendroves pasekmės	7
3. Naujas jurisdikcijos pagrindas ir vadinamasis vietos kriterijaus panaikinimas	8
4. Sąvoka „paslaugų teikėjai“ turėtų būti apribota arba papildyta papildomomis duomenų subjektų teisių apsaugos priemonėmis.....	9
5. Sąvokos „įmonė (buveinė)“ ir „teisinis atstovas“ šiuose pasiūlymuose turėtų būti aiškiai atskirtos nuo šių sąvokų Bendrajame duomenų apsaugos reglamente	10 10 ¹⁴
a) Įmonė (buveinė)	11
b) Teisinis atstovas.....	11
6. Naujos duomenų kategorijos	12
7. Europos įrodymų saugojimo ir pateikimo orderių procedūrų analizė	13
a) Turėtų būti padidintos orderių išdavimui taikomos ribos ir orderius turi išduoti arba tvirtinti teismai.....	14
b) Duomenų pateikimo terminai turėtų būti pagrįsti.....	15
c) Europos įrodymų pateikimo ir saugojimo orderiai neturi būti naudojami norint paprašyti kitos valstybės narės duomenų subjekto duomenų bent neinformavus tos valstybės narės kompetentingų institucijų, ypač kiek tai susiję su turinio duomenimis	16
d) Europos įrodymų saugojimo orderiai neturi būti naudojami paslaugų teikėjams siekiant išvengti duomenų saugojimo įsipareigojimų.....	16 16 ¹⁷
e) Konfidencialumas ir informacija apie naudotoją.....	17
f) Orderio vykdymo užtikrinimo procedūra, taikoma, kai paslaugų teikėjas atsisako jį vykdyti...	17
g) Orderių vykdymo užtikrinimas ir prieštaraujantys įsipareigojimai pagal trečiosios šalies teisės aktus (15–16 straipsniai)	18
h) Duomenų perdavimo saugumas vykdant orderį	20
Išvados.....	20

Europos duomenų apsaugos valdyba,

atsižvelgdama į 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB 70 straipsnio 1 dalies b punktą,

PRIĖMĖ ŠIA NUOMONĖ:

Įvadas

2018 m. balandžio mėn. Komisija pateikė pasiūlymą dėl Reglamento dėl Europos elektroninių įrodymų baudžiamosiose bylose pateikimo ir saugojimo orderių ir pasiūlymą dėl Direktyvos, kuria nustatomos teisinių atstovų skyrimo įrodymams baudžiamosiose bylose rinkti suderintos taisyklės. Šie du pasiūlymai COM(2018) 225 *final* ir COM(2018) 226 *final* yra vienas kitą papildantys. Bendras Komisijos siekiamas tikslas – pagerinti valstybių narių institucijų ir paslaugų teikėjų, įskaitant ES nepriklausančiose šalyse įsisteigusius paslaugų teikėjus, bendradarbiavimą ir pasiūlyti jurisdikcijos nustatymo ir užtikrinimo kibernetinėje erdvėje problemos sprendimo būdus.

Reglamento projekte numatomos taisyklės ir procedūros, taikomos išduodant, įteikiant ir vykdant įrodymų saugojimo orderius ir įrodymų pateikimo orderius elektroninių paslaugų teikėjų atžvilgiu, o Direktyvos projekte nustatomos ES neįsisteigusius paslaugų teikėjų teisinių atstovų skyrimo minimalios taisyklės.

2017 m. lapkričio mėn.¹, prieš Komisijai pateikiant pasiūlymo projektą, 29 straipsnio darbo grupė priminė, jog būtina užtikrinti, kad visi pasiūlymai dėl teisėkūros procedūra priimamų aktų visų pirma atitiktų galiojantį ES duomenų apsaugos *acquis* ir ES teisę bei teismų praktiką apskritai.

Visų pirma 29 straipsnio darbo grupė įspėjo dėl teisių į duomenų apsaugą ir privatumą apribojimų, kiek tai sietina su telekomunikacijų ir informacinės visuomenės paslaugų teikėjų tvarkomais duomenimis, ypač kai juos toliau tvarko teisėsaugos institucijos, priminė būtinybę užtikrinti visų ES priemonių suderinamumą su galiojančia Europos Tarybos Budapešto konvencija dėl kibernetinių nusikaltimų ir ES Direktyva dėl Europos tyrimo orderio (ETO) ir rekomendavo patikslinti atitinkamas procedūrinės taisyklės, kuriomis reglamentuojama prieiga prie elektroninių įrodymų nacionaliniu ir ES lygmenimis, siekiant užtikrinti, kad naujoji priemonė nesuteiktų institucijoms naujų įgaliojimų, kurie joms nepriklauso. Be šių bendrų pastabų, 29 straipsnio darbo grupė pateikė pastabų dėl tuo metu Komisijos svarstytų teisėkūros galimybių, susijusių su atitinkamų duomenų kategorijomis ir atitinkamomis priemonėmis prieigai prie jų apsaugoti, dėl galimybės pateikti įrodymų pateikimo orderius / prašymus siekiant priversti paslaugų teikėjus pateikti duomenis, esančius už ES ribų, taip pat dėl materialinių ir procedūrinių sąlygų, būtinų siekiant apsaugoti tiesioginę prieigą prie duomenų.

Atsižvelgdama į pateiktus konkrečius pasiūlymus dėl elektroninių įrodymų, Europos duomenų apsaugos valdyba siekia pateikti išsamesnę siūlomų teisinių priemonių analizę duomenų apsaugos aspektu.

¹ Žr. 29 straipsnio darbo grupės pareiškimą (http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48801).

1. Teisinis reglamento pasiūlymo pagrindas (SESV 82 straipsnis)

Siūlomas Elektroninių įrodymų reglamento projekto teisinis pagrindas yra SESV 82 straipsnio 1 dalis, susijusi su teisiniu bendradarbiavimu baudžiamosiose bylose, kurioje nustatyta, kad:

„1. Teisinis bendradarbiavimas baudžiamosiose bylose Sąjungoje grindžiamas nuosprendži ir teismo sprendim tarpusavio pripažinimo principu bei apima valstybi nari statym ir kit teis s akt suderinim 2 dalyje ir 83 straipsnyje nurodytose srityse.

Europos Parlamentas ir Taryba, spr sdami pagal prast teis k ros proced r , patvirtina priemones, kuriomis siekiama:

- a) nustatyti taisykles ir proced ras, kad visoje Sąjungoje b t užtikrintas vis nuosprendži ir teismo sprendim form pripažinimas;
- b) užkirsti keli jurisdikcij kolizijoms tarp valstybi nari ir jas spr sti;
- c) remti teis j ir teisini institucij darbuotoj mokym ;
- d) palengvinti su procesais baudžiamosiose bylose ir sprendim vykdymu susijus bendradarbiavim tarp valstybi nari teisini arba joms lygiaver i institucij .“

Kaip pabrėžė Komisija prie pasiūlymų pridėtame poveikio vertinime, „82 straipsnio 1 dalyje nurodyta, kad teisinis bendradarbiavimas baudžiamosiose bylose grindžiamas tarpusavio pripažinimo principu. Šis teisinis pagrindas būtų taikomas galimiems teisės aktams dėl tiesioginio bendradarbiavimo su paslaugų teikėjais, kai institucija išduodančiojoje valstybėje tiesiogiai kreiptųsi į subjektą (paslaugų teikėją) vykdančiojoje valstybėje ir net nustatytų jam įpareigojimus. Taip būtų įtrauktas naujas tarpusavio pripažinimo aspektas, apimantis ne tik tradicinį teisinį bendradarbiavimą Sąjungoje, kuris iki šiol grindžiamas procedūromis, kuriose dalyvauja dvi teisinės institucijos – viena išduodančiojoje valstybėje, o kita vykdančiojoje valstybėje.“ (pabraukta papildomai).

Kadangi šis teisinis pagrindas teikiant tiesioginius prašymus tarp valdžios institucijų ir privačių šalių pradėtas taikyti dar visai neseniai, Europos duomenų apsaugos valdyba apgailėstauja, kad Komisija nepateikė nei tolimesnės analizės, nei vertinimo.

Iš tikrųjų, kaip pabrėžė darbo grupė savo ankstesniame pareiškime, Europos duomenų apsaugos valdyba toliau akcentuoja, kad abejoja teisinio pagrindo tinkamumu, ir šioms abejonėms pritariama Europos Sąjungos Teisingumo Teismo analizėje ir jo generalinio advokato nuomonėje 1/15. Kalbant apie veiksmus, susijusius su 82 straipsnio kaip ES ir Kanados PNR susitarimo projekto teisinio pagrindo tinkamumu, Teismas pabrėžė, kad Kanados kompetentinga institucija „*nėra laikoma nei teismine institucija, nei jai lygiaverte institucija*“². Rengiant pasiūlymus dėl elektroninių įrodymų, vienas pagrindinių siekiamų tikslų, kaip teigia Komisija, yra išvengti „pernelyg sudėtingo“ teismo bendradarbiavimo. Todėl pasiūlymas yra pagrįstas principu, kuriuo vadovaujantis bendradarbiavimas turėtų vykti tarp institucijos ir paslaugų teikėjo, o ne tarp dviejų institucijų. Pagal numatytą procedūrą privatūs subjektai visų pirma yra gaunančioji šalis ir turi atsakyti į teismo institucijų pateikiamus prašymus.

Europos duomenų apsaugos valdyba pažymi, kad vykdant įrodymų pateikimo ir saugojimo orderius galėtų prireikti gaunančiosios institucijos dalyvavimo tokiais atvejais, kai gaunantysis paslaugų teikėjas nesilaiko savo įsipareigojimų, ir todėl gali tekti pareikalauti užtikrinti orderio *ex post* vykdymą. Tačiau kadangi pagrindinis nustatytos procedūros tikslas yra būtent tai, kad nedalyvautų gaunančioji

² Žr. Nuomonės 1/15 103 punktą ir Generalinio advokato išvados šioje byloje 108 punktą.

institucija, Europos duomenų apsaugos valdyba abejoja, kad šia papildoma procedūra galėtų būti pagrįstas 82 straipsnio, kaip vienintelio šios priemonės teisinio pagrindo, pasirinkimas.

Todėl Europos duomenų apsaugos valdyba mano, kad norint taikyti 82 straipsnį kaip teisinį pagrindą, pagrindiniai procedūriniai bendradarbiavimo veiksmai turi būti vykdomi tarp dviejų teisminių institucijų ir todėl tokiam bendradarbiavimui turėtų būti taikomas kitas teisinis pagrindas.

2. Elektroninių įrodymų būtinybė, palyginti su savitarpio teisinės pagalbos susitarimais ir ETO

Europos duomenų apsaugos valdyba pažymi, kad Komisija yra įsipareigojusi peržiūrėti kliūtis, trukdančias tirti nusikalstamas veikas, ypač susijusias su prieigos prie elektroninių įrodymų suteikimu. Savo aiškinamajame memorandume Komisija nurodo pasiūlymo aplinkybes ir pabrėžia elektroninių įrodymų nepastovumą, jų tarptautinį aspektą, taip pat būtinybę pritaikyti bendradarbiavimo mechanizmą prie skaitmeninio amžiaus. Pasiūlymais dėl reglamento ir direktyvos dėl elektroninių įrodymų perdavimo ir prieigos prie jų nesiekama pakeisti ankstesnes bendradarbiavimo baudžiamosiose bylose priemones, kaip antai Budapešto konvenciją, Savitarpio teisinės pagalbos susitarimą ir Europos tyrimo orderį (ETO direktyva). Komisijos nuomone, pasiūlymais dėl elektroninių įrodymų siekiama pagerinti institucijų ir paslaugų teikėjų teisinį bendradarbiavimą baudžiamosiose bylose Europos Sąjungoje ir su trečiosiomis šalimis, visų pirma su Jungtinėmis Amerikos Valstijomis.

Kadangi šios naujos papildomos priemonės bus konkrečiai skirtos prieigai prie elektroninių įrodymų ir jų perdavimui, Europos duomenų apsaugos valdyba įvertins priemonių, susijusių su ETO direktyva ir Savitarpio teisinės pagalbos susitarimu, pridėtinę vertę.

a) Elektroninių įrodymų būtinybė, palyginti su ETO ir savitarpio teisinės pagalbos susitarimuose numatytais apsaugos priemonėmis

Pagrindinis Komisijos pateiktas argumentas, kuriuo pritariama pasiūlymams dėl elektroninių įrodymų, yra tai, kad jais būtų paspartintas procesas, kuriuo siekiama apsaugoti elektroninius įrodymus, kuriuos saugo ir (arba) turi kitoje jurisdikcijoje įsisteigę paslaugų teikėjai, ir juos gauti.

Vis dėlto Europos duomenų apsaugos valdyba apgailestauja, kad poveikio vertinime nebuvo nurodyta būtinybė parengti naują priemonę, kuria būtų suteikiama prieiga prie elektroninių įrodymų. Iš tiesų iš pasiūlymų nematyti, kad nebuvo galima panaudoti jokių kitų mažiau intervencinių priemonių pasiūlymo dėl elektroninių įrodymų tikslui pasiekti, ir galėjo būti apsvarstyti alternatyvūs sprendimai. Pavyzdžiui, buvo galima išnagrinėti galimybę iš dalies pakeisti ir patobulinti ETO direktyvą; be to, taip būtų įgyvendintas ETO direktyvoje nustatytas reikalavimas iki 2019 m. gegužės 21 d. įvertinti poreikį iš dalies pakeisti jos tekstą³. Kita galimybė galėjo būti numatyti įrodymų saugojimo orderio naudojimą siekiant įšaldyti duomenis, kol bus pateiktas savitarpio teisinės pagalbos susitarimu pagrįstas oficialus prašymas. Šie sprendimai būtų suteikę galimybę išlaikyti šiose priemonėse numatytas apsaugos priemones, kartu užtikrinant, kad asmens duomenys, kurių prašoma, nebūtų ištrinti.

Europos duomenų apsaugos valdyba pažymi, kad ETO direktyvoje nustatyti ilgesni terminai, nei pasiūlyme dėl elektroninių įrodymų. Iš tiesų vykdančioji institucija turi per 30 dienų priimti sprendimą

³ Žr. ETO direktyvos 37 straipsnį.

dėl prašymo pripažinimo⁴, o tada per 90 dienų įvykdyti orderį⁵. Europos duomenų apsaugos valdyba mano, kad ETO vykdančiosioms institucijoms suteikiamas 30 dienų svarstymo laikotarpis yra labai svarbi apsaugos priemonė, suteikianti joms galimybę įvertinti, ar vykdymo prašymas yra tinkamai pagrįstas ir atitinka ETO išdavimo ir perdavimo sąlygas⁶.

Europos duomenų apsaugos valdyba nuogaštauja, kad pasiūlymuose dėl elektroninių įrodymų nurodytas 10 dienų terminas, per kurį turi būti išduotas Europos įrodymų pateikimo orderio sertifikatas, neskiriant laiko apsvaistymui, užkerta kelią tinkamai įvertinti, ar Europos įrodymų pateikimo orderio sertifikatas atitinka visus kriterijus ir yra teisingai užpildytas.

Todėl Europos duomenų apsaugos valdyba rekomenduoja, kad Europos įrodymų pateikimo orderio sertifikato gavėjui būtų skirta daugiau laiko nustatyti, ar orderis turėtų būti vykdomas, ar ne.

Europos duomenų apsaugos valdyba pažymi, jog Europos įrodymų saugojimo orderio atveju nėra garantijų, kad bus saugomi tik tie duomenys, kurie turi būti pateikti. Iš tiesų duomenys gali būti saugomi ilgiau nei 60 dienų, nes nėra nustatyto termino, per kurį išduodančioji institucija turi informuoti adresatą, kad jis neišduotų įrodymų pateikimo orderio ar jį panaikintų. Todėl Europos duomenų apsaugos valdyba rekomenduoja bent nustatyti terminą, per kurį išduodančioji institucija galėtų atsisakyti išduoti arba panaikinti įrodymų pateikimo orderį, kad būtų laikomasi Bendrajame duomenų apsaugos reglamente⁷ nustatyto duomenų kiekio mažinimo principo.

Galiausiai Europos duomenų apsaugos valdyba pažymi, kad ETO direktyvoje nustatytas įrodymų grąžinimas iš išduodančiosios valstybės vykdančiajai institucijai⁸. Tačiau Elektroninių įrodymų reglamento pasiūlyme apie tokią galimybę neužsimenama. Nėra aišku, kas nutinka elektroniniams įrodymams po to, kai jie perduodami išduodančiajai institucijai.

Todėl Europos duomenų apsaugos valdyba rekomenduoja, kad reglamento pasiūlyme būtų pateikta daugiau informacijos apie šių elektroninių įrodymų naudojimą po to, kai jie perduodami išduodančiajai institucijai, kad būtų laikomasi Bendrojo duomenų apsaugos reglamento nuostatų ir skaidrumo principo⁹, taip pat savitarpio teisinės pagalbos susitarimuose nustatyto specifiškumo principo.

b) Abipusio baudžiamumo principo atsisakymas

Europos duomenų apsaugos valdyba pripažįsta, kad tarpusavio pripažinimas priklauso nuo abipusio baudžiamumo taikymo ir taip valstybės narės gali išlaikyti savo suverenumą. Tačiau abipusis baudžiamumas vis dažniau laikomas sklandaus teismo bendradarbiavimo kliūtimi. ES valstybės narės vis labiau nori bendradarbiauti, net jeigu tyrimo priemonės yra susijusios su veiksmis, kurie nelaikomi pažeidimais jų nacionalinėje teisėje. Vis dėlto Europos duomenų apsaugos valdyba primena, kad abipusio baudžiamumo principu siekiama suteikti papildomą apsaugos priemonę, kuria būtų užtikrinama, kad valstybė negalėtų tikėtis kitos valstybės pagalbos taikant baudžiamąją sankciją, kuri netaikoma kitos valstybės teisėje. Pavyzdžiui, taip valstybei būtų užkertamas kelias reikalauti, kad kita valstybė padėtų įkalinti asmenį už jo politinius įsitikinimus, jeigu tie įsitikinimai nėra kriminalizuoti valstybėje, į kurią kreipiamasi, ar patraukti baudžiamojon atsakomybėn asmenį už jam atliktą abortą, jeigu tas asmuo gyvena kitoje valstybėje, kurioje abortas nėra neteisėtas. Abipusio baudžiamumo principas taip pat dažnai taikomas kartu su papildomais apribojimais ar apsaugos priemonėmis,

⁴ ETO direktyvos 12 straipsnio 3 dalis.

⁵ ETO direktyvos 12 straipsnio 4 dalis.

⁶ ETO direktyvos 6 straipsnis.

⁷ Bendrojo duomenų apsaugos reglamento 5 straipsnio 1 dalies c punktas.

⁸ ETO direktyvos 13 straipsnio 3 ir 4 dalys.

⁹ Bendrojo duomenų apsaugos reglamento 5 straipsnio 1 dalies a punktas.

susijusiais su sankcijomis, jeigu jos pernelyg skiriasi prašymą pateikusioje valstybėje ir vykdančiojoje valstybėje. Pagrindinis pavyzdys – tam tikruose savitarpio teisinės pagalbos susitarimuose nustatytas įsipareigojimas netaikyti mirties bausmės, kai ji netaikoma pagal vienos iš dviejų šalių teisę.

Europos duomenų apsaugos valdyba pažymi, kad abipusio baudžiamumo principas neįtrauktas į Elektroninių įrodymų reglamento pasiūlymą. Tačiau dėl to panaikinami ne tik įprasti su tarpusavio pripažinimu susiję formalumai, bet ir apsaugos priemonės, susijusios su pačiu abipusio baudžiamumo principu.

Iš tiesų Europos duomenų apsaugos valdyba atkreipia dėmesį į tai, kad nėra nuorodų į šalis, kurioje įsisteigęs prašymą gavęs paslaugų teikėjas, teisę ir kad orderis dėl bet kokių duomenų saugojimo, įskaitant duomenis apie abonentus ir prieigos duomenis, gali būti išduotas dėl bet kurios nusikalstamos veikos¹⁰, nepaisant to, ar kitose valstybėse narėse yra nustatytos panašios nusikalstamos veikos, ar ne.

Įrodymų pateikimo orderiai gali būti išduodami ir vykdomi tik tuomet, jeigu dėl tos pačios nusikalstamos veikos panašioje vidaus situacijoje išduodančiojoje valstybėje gali būti taikoma panaši priemonė¹¹. Be to, kaip paaiškino Komisija reglamento pasiūlymo aiškinamajame memorandume, nustatomas sandorių arba turinio duomenų specifiškumas, nes jie yra laikomi labiau neskelbtiniais. Iš tiesų orderiai, susiję su sandorio arba turinio duomenimis, yra pagrįsti didžiausios laisvės atėmimo bausmės, kuri yra ne trumpesnė kaip treji metai, riba siekiant užtikrinti, kad būtų laikomasi proporcingumo principo ir gerbiamos susijusių asmenų teisės¹². Tačiau Europos duomenų apsaugos valdyba pabrėžia, kad ES dar nėra atliktas suderinimas dėl nusikalstamų veikų, už kurias baudžiama laisvės atėmimo bausme, kurios ilgiausias terminas – ne mažiau kaip 3 metai.

Europos duomenų apsaugos valdyba prieštarauja tam, kad būtų atsisakyta abipusio baudžiamumo principo, kuriuo siekiama užtikrinti, kad valstybė negalėtų remtis kitų valstybių pagalba siekdama, kad jos baudžiamąją teisę už jos ribų taikytų valstybė, kuri nesilaiko to paties požiūrio, ypač atsižvelgiant į tai, jog baudžiamosios teisės srityje atsisakoma kitų svarbių tradicinių apsaugos priemonių (žr. tolesnį 3 punktą dėl vietos kriterijaus ir 7 punkto g papunktį dėl galimo prieštaravimo trečiųjų šalių teisei).

c) Tiesioginio kreipimosi į bendroves pasekmės

Europos duomenų apsaugos valdyba pripažįsta, kad elektroniniai įrodymai vis lengviau prieinami privačioje infrastruktūroje ir jie gali būti už tyrimą atliekančios šalies ribų ir priklausyti paslaugų teikėjams.

Europos duomenų apsaugos valdyba atkreipia dėmesį į tai, jog po Belgijoje priimtų sprendimų dėl „Yahoo!“¹³ ir „Skype“¹⁴, taip pat atsižvelgiant į teroristinius išpuolius, reikia sklandesnio ir spartesnio viešųjų ir privačiųjų subjektų bendradarbiavimo. Poveikio vertinime Komisija nurodo trijų tipų procedūrinės priemonės, susijusios tiek su valdžios institucijomis, tiek su paslaugų teikėjais. Tai yra teisminis bendradarbiavimas, tiesioginis bendradarbiavimas ir tiesioginė prieiga. Taikant pirmą priemonę atsakomybė už ETO vykdymą tenka ne paslaugų teikėjui, o vykdančiajai institucijai¹⁵; antra priemonė, kai bendradarbiaujama tiesiogiai, pagrįsta paslaugų teikėjo bendradarbiavimu. Labiausiai

¹⁰ Siūlomo Elektroninių įrodymų reglamento 5 straipsnio 3 dalis ir 6 straipsnio 2 dalis.

¹¹ Siūlomo Elektroninių įrodymų reglamento 5 straipsnio 2 dalis.

¹² Siūlomo Elektroninių įrodymų reglamento 5 straipsnio 4 dalies a punktas.

¹³ *Hof van Cassatie*, Belgija, „Yahoo!“ Inc., Nr. P.13.2082.N, 2015 m. gruodžio 1 d.

¹⁴ *Correctionele Rechtbank van Antwerpen, afdeling Mechelen*, Belgija, Nr. ME20.F1.105151-12, 2016 m. spalio 27 d. „Skype“ apskundė sprendimą.

¹⁵ 10–16 straipsniai.

ribojanti priemonė paslaugų teikėjo atžvilgiu yra tiesiogine prieiga, nes valdžios institucijos gali gauti duomenis be tarpininkų pagalbos.

Todėl Europos duomenų apsaugos valdyba nuoga stauja, kad kai į paslaugų teikėjus bus kreipiamasi tiesiogiai, jie neužtikrins asmens duomenų apsaugos taip veiksmingai, kaip tai gali ir yra įpareigotos padaryti valdžios institucijos, ir pabrėžia, kad dėl to asmenims ir pačioms bendrovėms nebus taikomos tam tikros procedūrinės garantijos¹⁶, numatytos vykdant teisminį bendradarbiavimą. Pavyzdžiui, paslaugų teikėjas, kuriam pateiktas prašymas, turėtų kreiptis į kitos valstybės (narės) teismą, kad užginčytų orderį, o vykdant teisminį bendradarbiavimą jam tektų susidurti su savo šalies institucijomis. Europos duomenų apsaugos valdyba rekomenduoja į pasiūlymą dėl reglamento įtraukti papildomą pagrindą, kuriuo būtų užtikrinta, kad paslaugų teikėjai gins asmens pagrindines teises, pavyzdžiui, teisę į duomenų apsaugą ir teisę į privatų ir šeimos gyvenimą, taip pat rekomenduoja informuoti kompetentingą duomenų apsaugos instituciją siekiant užtikrinti, kad būtų galima vykdyti kontrolę.

3. Naujas jurisdikcijos pagrindas ir vadinamojo vietos kriterijaus panaikinimas

Europos duomenų apsaugos valdyba atkreipia dėmesį į tai, kad Komisija pabrėžia, jog vienas iš svarbiausių šiais pasiūlymais numatytų pakeitimų yra vietos kriterijaus panaikinimas ir galimybė kompetentingoms institucijoms reikalauti saugoti ir pateikti duomenis, neatsižvelgiant į tai, kur tie duomenys faktiškai saugomi.

Kalbant apie duomenų apsaugą, tai, kad ES duomenų apsaugos teisės aktai taikomi, nepaisant to, kur susijusių asmenų duomenys yra saugomi, nėra naujiena. Bendrojo duomenų apsaugos reglamento taikymas priklauso arba nuo to, kad duomenų valdytojas ar tvarkytojas įsisteigęs ES, arba nuo to, ar ES duomenų subjektų duomenys yra tvarkomi, net kai valdytojas ar tvarkytojas nėra įsisteigęs ES teritorijoje¹⁷; tokiu atveju jie taip pat turi paskirti teisinį atstovą ES¹⁸. Dėl duomenų apsaugos svarbu pažymėti, kad išplėsta teritorine taikymo sritimi siekiama ES duomenų subjektams užtikrinti visapusiškesnę apsaugą, nepaisant to, kur įsisteigusi jų duomenis tvarkanti bendrovė.

Todėl, nors vietos kriterijaus panaikinimas gali būti naujovė baudžiamosios teisės srityje, tai nėra esminis pakeitimas duomenų apsaugos atžvilgiu. Be to, Europos duomenų apsaugos valdyba taip pat pažymi, kad vis tiek išlaikyta sąsaja su ES teritorija, nes tik Sąjungoje paslaugas siūlantys teikėjai patenka į šių pasiūlymų taikymo sritį, o tai, jog prašymai gali būti pateikiami tik vykdant baudžiamosios veikos tyrimus, reiškia, kad yra sąsaja su ES (arba todėl, kad nusikaltimas buvo įvykdytas valstybės narės teritorijoje, arba todėl, kad nusikaltimo auka arba nusikaltėlis buvo valstybės narės pilietis).

Jeigu vietos kriterijaus panaikinimas bus taikomas baudžiamojoje teisėje, svarbiausias Europos duomenų apsaugos valdybai kylantis klausimas – kaip užtikrinti, kad toks pokytis nekenktų duomenų apsaugai ir duomenų subjektų bei paslaugų teikėjui, kuriems pateiktas prašymas, procesinėms teisėms baudžiamosiose bylose. Šiuo atžvilgiu Europos duomenų apsaugos valdyba pripažįsta, kad ES procedūrinės garantijos bent iš dalies suderintos ir turi būti nustatomos laikantis Europos žmogaus teisių konvencijos. Taigi galima teigti, kad vietos kriterijaus panaikinimas tikriausiai turėtų mažiau

¹⁶ Taip pat žr. tarptautinės duomenų apsaugos aspektu Tarptautinės duomenų apsaugos ir telekomunikacijų darbo grupės darbinį dokumentą „*Working paper on Standards for data protection and personal privacy in cross-border data requests for criminal law enforcement purposes*“, 2018 m. balandžio 9–10 d., 63-iasis posėdis, Budapeštas (Vengrija).

¹⁷ Žr. 3 straipsnį, ypač 2 dalį.

¹⁸ Žr. 27 straipsnį.

pasekmių tais atvejais, kai įrodymų prašoma ES viduje, palyginti su priešinga situacija, kai trečiųjų šalių institucijos prašo duomenų iš ES įsisteigusių bendrovių tokiomis pačiomis sąlygomis kaip nustatytosios Elektroninių įrodymų reglamento projekte. Europos duomenų apsaugos valdyba nuogąstauja, kad dėl to gali susidaryti daugiau sudėtingų situacijų. Šiomis aplinkybėmis trečiosios šalies, kurioje taikomos kitokios procedūrinės garantijos ir galbūt mažiau tokių garantijų baudžiamosios teisės srityje, institucijos galėtų turėti prieigą prie duomenų, kurie ES būtų apsaugoti papildomomis apsaugos priemonėmis. Šiuo atžvilgiu Europos duomenų apsaugos valdyba primena savo susirūpinimą dėl dvigubų standartų ir silpnėjančios pagrindinių teisių apsaugos, kai paslaugų teikėjai ir duomenų subjektai negali pasinaudoti ES teisėje numatytais procedūrinėmis garantijomis, jeigu prašymą pateikia trečiosios šalies institucija.

Be to, kadangi šis naujas jurisdikcijos pagrindas „neatsižvelgiant į duomenų vietą“ taikomas kartu su procedūra, grindžiama daugiausia kompetentingų institucijų teikiamais tiesioginiais prašymais paslaugų teikėjams, Europos duomenų apsaugos valdyba nuogąstauja, kad duomenų apsaugos priemonių gali netaikyti prašymus gaunančios privačios bendrovės, kurios nėra saistomos teisinių priemonių, kaip antai savitarpio teisinės pagalbos susitarimo, kuriuo tradiciškai reglamentuojami duomenų mainai tarp teisminių institucijų ir numatomos apsaugos priemonės. Visų pirma įgyvendinant savitarpio teisinės pagalbos susitarimus taikomos minimalios apsaugos priemonės yra, pavyzdžiui, konfidencialumo įsipareigojimai ir specifiškumo principas, kuris reiškia, kad duomenys nebus tvarkomi kitais tikslais.

Todėl Europos duomenų apsaugos valdyba primena, kad turėtų būti taikomos Direktyvoje 2016/680 nustatytos apsaugos priemonės, įskaitant priemones, susijusias su duomenų perdavimu, ir ypač nustatytosios 39 straipsnyje, jeigu paslaugų teikėjas įsisteigęs trečiojoje šalyje ir nėra priimtas sprendimas dėl tinkamumo šioje srityje. Europos duomenų apsaugos valdyba pabrėžia, kad ši nuostata visų pirma reiškia, jog turi būti informuojama orderį (-ius) ir perdavimo dokumentus išdavusios institucijos valstybės narės kompetentinga duomenų apsaugos institucija, taip pat kiek tai susiję su paaiškinimu dėl neveiksmingo ar netinkamo perdavimo trečiosios šalies kompetentingai institucijai.

4. Sąvoka „paslaugų teikėjai“ turėtų būti apribota arba papildyta papildomomis duomenų subjektų teisių apsaugos priemonėmis

Kalbant apie paslaugų teikėjus, Europos duomenų apsaugos valdyba pritaria plačiai apibrėžčiai, kuri suteikia galimybę įtraukti tiek ryšių paslaugas, tiek virštinklines (angl. *over-the-top*, OTT) paslaugas, nes visos šios paslaugos yra funkciškai lygiavertės ir todėl numatytos priemonės gali turėti panašų poveikį teisei į privatų gyvenimą ir teisei į ryšių konfidencialumą, kaip pabrėžiama 29 straipsnio darbo grupės pareiškime ir ankstesnėje Nuomonėje 01/2017 dėl siūlomo E. privatumo reglamento. Iš tiesų Elektroninių įrodymų reglamento pasiūlymas apima paslaugų teikėjus, teikiančius elektroninių ryšių paslaugas, apibrėžtas Direktyvos, kuria nustatomas Europos elektroninių ryšių kodeksas, 2 straipsnio 4 dalyje, informacinės visuomenės paslaugas, apibrėžtas Direktyvos (ES) 2015/1535 1 straipsnio 1 dalies b punkte, „kurias teikiant duomenų saugojimas yra pagrindinė naudotojui teikiamos paslaugos savybė, įskaitant socialinius tinklus, elektronines prekyvietes, palengvinančias jų naudotojų ir kitų prieglobos paslaugų teikėjų tarpusavio sandorių sudarymą“, arba interneto domeno vardo ir IP numeravimo

paslaugas, „pvz., IP adresų teikėjų, domeno vardų registruotojų ir susijusias privatumo ir tarpininkavimo paslaugas“¹⁹.

Tačiau kadangi pagal reglamento projektą paslaugų teikėjas yra „fizinis ar juridinis asmuo, kuris teikia vieną ar daugiau iš toliau nurodytų kategorijų paslaugų“, Europos duomenų apsaugos valdybai susirūpinimą kelia tai, kad ši priemonė galėtų būti taikoma tiek valdytojams, tiek tvarkytojams pagal Bendrąjį duomenų apsaugos reglamentą. Kadangi „paslaugų teikimas“, kaip apibrėžta reglamento projekto 2 straipsnio 4 dalyje, apima sąlygų sudarymą vienoje ar keliuose valstybėse narėse esantiems juridiniams ar fiziniams asmenims naudotis nurodytomis paslaugomis, palaikant esminį ryšį su atitinkama (-omis) valstybe (-ėmis) nare (-ėmis), ši veikla apima veiklą, kurią vykdo tvarkytojas valdytojo vardu, pavyzdžiui, duomenų saugojimą.

Taigi Europos duomenų apsaugos valdyba nuogaustauja, kad nesant apribojimų paslaugų teikėjams, veikiantiems kaip valdytojai, kaip apibrėžta Bendrajame duomenų apsaugos reglamente, ir nenumačius konkrečios prievolės tvarkytojui informuoti duomenų valdytoją, išdavus įrodymų pateikimo ar saugojimo orderį gali būti pažeistos duomenų subjektų teisės. Tai ypač aktualu, nes tais atvejais, kai įsipareigojimai gali vienas kitam prieštarauti ir neleisti adresatui įteikti gautų orderių, pačiame reglamento projekte teisminės institucijos taip pat raginamos kreiptis į tinkamiausią subjektą nepaisant taikomų duomenų apsaugos taisyklių, ypač atsižvelgiant į tai, kad gali būti prašoma pateikti bet kokius duomenis, o ne tik asmens duomenis, kuriems taikomas Bendrasis duomenų apsaugos reglamentas²⁰.

Pagal Bendrąjį duomenų apsaugos reglamentą tvarkytojas tik vykdo valdytojo duotus nurodymus. Todėl valdytojas privalo užtikrinti, kad būtų gerbiamos duomenų subjektų teisės, ir pateikti jiems atitinkamą informaciją, įskaitant informaciją, susijusią su jų duomenų gavėjais, pavyzdžiui, įgyvendinant jų teisę susipažinti su duomenimis. Tvarkytojas negaus šių prašymų iš duomenų subjektų ir negalės jiems atsakyti, jeigu to aiškiai nepaprašys valdytojas.

Todėl Europos duomenų apsaugos valdyba pabrėžia, kad duomenų subjektai, kuriems naudingas Bendrojo duomenų apsaugos reglamento taikymas, gali neturėti galimybės veiksmingai pasinaudoti savo teisėmis, jeigu valdytojas negalės pateikti išsamios informacijos, išskyrus atvejus, kai jų teisės apribotos taikant Bendrąjį duomenų apsaugos reglamentą. Europos duomenų apsaugos valdyba taip pat pažymi, kad nenustačius konkrečių tvarkytojui taikomų įpareigojimų informuoti valdytoją, kai prašomi duomenys susiję su duomenų subjektais, kurie nesinaudoja Bendrojo duomenų apsaugos reglamento teikiama apsauga, tikimybė, kad informacija nebus pateikta, yra dar didesnė. Tokiu atveju duomenų prašančios teisminės institucijos nebūtinai bus įpareigos informuoti duomenų subjektus apie tolesnį jų duomenų tvarkymą. Todėl Europos duomenų apsaugos valdyba ragina į taikymo sritį įtraukti tik valdytojus, kaip apibrėžta Bendrajame duomenų apsaugos reglamente, arba įtraukti nuostatą, kuria būtų patikslinta, kad tokiu atveju, kai paslaugų teikėjas, į kurį kreipiamasi, nėra duomenų valdytojas, jis privalo informuoti valdytoją.

5. Sąvokos „įmonė (buveinė)“ ir „teisinis atstovas“ šiuose pasiūlymuose turėtų būti aiškiai atskirtos nuo šių sąvokų Bendrajame duomenų apsaugos reglamente

¹⁹ Siūlomo Elektroninių įrodymų reglamento 2 straipsnio 3 dalies c punktas.

²⁰ Žr. 7 straipsnio 3 ir 4 dalis.

Kadangi vietos kriterijus duomenų atžvilgiu netaikomas, įrodymų pateikimo ir saugojimo orderių adresatai pagal siūlomo reglamento taikymo sritį gali būti tik Sąjungoje paslaugas siūlantys paslaugų teikėjai, įsisteigę ES arba už jos ribų, kurie įpareigoti paskirti teisinį atstovą pagal direktyvos projekte siūlomas taisykles. Todėl šios sąvokos „įmonė (buveinė)“ ir „teisinis atstovas“ yra apibrėžtos priemonių projektuose.

Europos duomenų apsaugos valdyba atkreipia dėmesį į tai, jog šios sąvokos taip pat vartojamos kitose ES priemonėse, visų pirma Bendrajame duomenų apsaugos reglamente. Taigi pasiūlymų projektuose ir Bendrajame duomenų apsaugos reglamente vartojamos sąvokos turėtų būti tiksliau apibrėžtos ir atskirtos.

a) Įmonė (buveinė)

Europos duomenų apsaugos valdyba taip pat primena, kad reglamento projekte vartojama sąvoka „įmonė“ neturi būti painiojama su Bendrajame duomenų apsaugos reglamente vartojama sąvoka „buveinė“. Reglamento projekte įmonės sąvoka, apibrėžta 2 straipsnio 5 dalyje, yra platesnė nei Bendrajame duomenų apsaugos reglamente vartojama sąvoka „buveinė“, nes į ją įtrauktas „faktinis ekonominės veiklos vykdymas neribotą laikotarpį naudojant stabilią infrastruktūrą, iš kurios vykdoma paslaugų teikimo verslo veikla, arba stabilią infrastruktūrą, iš kurios valdoma įmonė“, neatsižvelgiant į tai, ar asmens duomenys tvarkomi šiai įmonei (buveinei) vykdant veiklą, ar ne. Taigi, Bendrajame duomenų apsaugos reglamente vartojama sąvoka „buveinė“ neabejotinai įtraukta į reglamento projekte apibrėžtą įmonės sąvoką, tačiau reglamento projekte apibrėžta sąvoka gali būti neįtraukta į Bendrajame duomenų apsaugos reglamente vartojamą sąvoką.

Todėl Europos duomenų apsaugos valdyba įspėja, kad paslaugų teikėjų įmonės (buveinės) pagal reglamento projektą nebūtinai gali reikšti, kad tenkinamos Bendrojo duomenų apsaugos reglamento taikymo pagal 3 straipsnio 1 dalį sąlygos. Atsižvelgiant į tai, valdytojai ir tvarkytojai raginami patikrinti, ar Bendrasis duomenų apsaugos reglamentas nėra taikomas pagal 3 straipsnio 2 dalį, nes tai reikštų, kad turi būti paskirtas teisinis atstovas ES ir nėra vieno langelio principu veikiančio mechanizmo.

b) Teisinis atstovas

29 straipsnio darbo grupė savo pareiškime pabrėžė, kad reikėtų vengti bet kokios painiavos tarp įsipareigojimo paskirti teisinį atstovą pagal Bendrojo duomenų apsaugos reglamento 27 straipsnį ir teisinio atstovo skyrimo, numatyto pagal Elektroninių įrodymų reglamento projektą.

Atsižvelgdama į pateiktą pasiūlymo projektą, Europos duomenų apsaugos valdyba norėtų priminti šias rekomendacijas ir ypač pabrėžti, kad, jos nuomone, rengiant elektroninių įrodymų pasiūlymus bet kuriuo atveju turi būti paskirtas teisinis atstovas pagal Direktyvos dėl teisinių atstovų skyrimo projektą; jam turi būti paskirtos konkrečios funkcijos, neatsižvelgiant į paslaugų teikėjo suteiktus įgaliojimus, taip pat suteikti įgaliojimai atsakyti į prašymus ir veikti paslaugų teikėjo vardu ir suteikta didesnė atsakomybė nei pagal Bendrąjį duomenų apsaugos reglamentą paskirtam teisiniam atstovui.

Be to, Europos duomenų apsaugos valdyba pabrėžia, kad įpareigojimas pagal pasiūlymų dėl elektroninių įrodymų projektus bet kuriuo atveju paskirti teisinį atstovą, neatsižvelgiant į tai, ar paslaugų teikėjas įsisteigęs ES, ar ne, galimybė paskirti kelis to paties paslaugų teikėjo teisinius atstovus pagal Direktyvos dėl elektroninių įrodymų projektą ir įpareigojimas apie teisinio atstovo paskyrimą informuoti valstybių narių institucijas skiriasi nuo Bendrojo duomenų apsaugos reglamento nuostatų, kuriose nenumatytas toks įpareigojimas pranešti apie paskirtą teisinį atstovą, paskyrimui taikomos išimties ir ribota teisinių atstovų atsakomybė.

Todėl atsižvelgdama į svarbius skirtumus, vienu atveju susijusius su paslaugų teikėju, o kitu – su valdytoju arba tvarkytoju vaidmeniu, atsakomybe ir santykiais su kitomis įmonėmis (buveinėmis), Europos duomenų apsaugos valdyba rekomenduoja, kad tais atvejais, kai paslaugų teikėjas nėra įsisteigęs ES, tačiau jam taikomas tiek Bendrasis duomenų apsaugos reglamentas pagal 3 straipsnio 2 dalį, tiek Elektroninių įrodymų reglamentas, turėtų būti paskirti du atskiri teisiniai atstovai, atliekantys aiškiai atskirtas funkcijas, nustatytas pagal priemonę, kuria remiantis jie buvo paskirti.

6. Naujos duomenų kategorijos

Siūlomo reglamento 2 straipsnyje apibrėžiamos skirtingos duomenų kategorijos: duomenys apie abonentą, prieigos duomenys, sandorių duomenys ir turinio duomenys. Komisijos pasiūlymo 20 konstatuojamojoje dalyje taip pat nurodoma, kad „*duomenų kategorijos, kurioms taikomas šis reglamentas, apima duomenis apie abonentą, prieigos duomenis, sandorio duomenis (šios trys kategorijos vadinamos su turiniu nesusijusiais duomenimis) ir turinio duomenis. Šis skirtumas, išskyrus prieigos duomenis, galioja daugumos valstybių narių įstatymuose ir dabartinėje JAV teisinėje sistemoje, pagal kurią paslaugų teikėjams leidžiama su turiniu nesusijusiais duomenimis savanoriškai dalytis su užsienio teisėsaugos institucijomis*“.

Šiomis aplinkybėmis Europos duomenų apsaugos valdyba pirmiausia pabrėžia, kad pagal ES duomenų apsaugos teisės aktus visų keturių pirmiau išvardytų kategorijų duomenys turi būti laikomi asmens duomenimis, nes jie apima informaciją, susijusią su fiziniu asmeniu, kurio tapatybė yra nustatyta arba gali būti nustatyta, nepaisant to, ar siūlomame reglamente duomenų subjektas nurodomas kaip „abonentas“ ar kaip „naudotojas“. Taip pat reikia pažymėti, kad „elektroniniai duomenys“, apibrėžti Komisijos pasiūlymo 2 straipsnio 6 dalyje, apima visas keturias duomenų kategorijas ir todėl yra susiję su asmens duomenimis. Todėl siūlomame reglamente nustatomos ne prieigos prie įrodymų taisyklės, apibrėžtos ir numatytos pagal nacionalinę teisę ir teismo procesus, o naujos materialinės ir procedūrinės sąlygos, susijusios su prieiga prie asmens duomenų.

Nors siūlomame reglamente nustatomos naujos asmens duomenų pakategorės, kurioms taikomos skirtingos procedūrinės sąlygos, Europos duomenų apsaugos valdyba primena, kad remiantis atitinkama Europos Sąjungos Teisingumo Teismo praktika, nustatant, ar esama pagrindinės teisės į privatų gyvenimą apribojimo, nėra svarbu, ar informacija apie atitinkamų asmenų privatų gyvenimą yra neskelbtina arba ar suinteresuoti asmenys patyrė kokių nors nepatogumų.

Be to, Europos duomenų apsaugos valdyba primena, kad dėl su turiniu nesusijusių duomenų, kurie, kaip numatyta Komisijos pasiūlyme, apima duomenis apie abonentą, prieigos duomenis ir sandorio duomenis, Europos Sąjungos Teisingumo Teismas savo sprendime sujungtose bylose C-203/15 ir C-698/15 *Tele2 Sverige AB* konstatavo, kad metaduomenys, pavyzdžiui, srauto duomenys ir buvimo vietos duomenys, suteikia galimybę atitinkamų asmenų profiliui nustatyti – ne mažiau neskelbtinai informacijai, kiek tai susiję su teise į privataus gyvenimo užtikrinimą, nei konkretus pranešimų turinys²¹.

Atsižvelgdama į tai, kas jau išdėstyta 2017 m. lapkričio 29 d. 29 straipsnio darbo grupės pareiškime dėl tarpvalstybinės prieigos prie elektroninių įrodymų duomenų apsaugos ir privatumo aspektų, Europos duomenų apsaugos valdyba dar kartą išreiškia abejones ir susirūpinimą dėl to, kaip šiuo metu apibrėžiami „su turiniu nesusiję“ ir „turinio“ duomenys, taip pat dėl keturių asmens duomenų kategorijų, nurodytų siūlomame reglamente. Iš tiesų neatrodo, kad keturios siūlomos kategorijos yra

²¹ 2016 m. gruodžio 21 d. ESTT sprendimo 99 punktas.

aiškiai apibrėžtos, o „prieigos duomenų“ apibrėžtis vis dar yra neaiški, palyginti su kitomis kategorijomis. Todėl Europos duomenų apsaugos valdyba apgailestauja, kad Komisijos poveikio vertinime ir pasiūlyme nėra pagrįsta šių naujų asmens duomenų pakategorių nustatymo logika, ir išreiškia susirūpinimą dėl skirtingo lygio garantijų, susijusių su prieigos prie šių asmens duomenų kategorijų materialinėmis ir procedūrinėmis sąlygomis, ypač atsižvelgiant į tai, jog kai kuriais atvejais sunku praktiškai įvertinti, kuriai duomenų kategorijai bus priskirti prašomi duomenys. Pavyzdžiui, IP adresai galėtų būti priskiriami tiek sandorių, tiek abonentų duomenims.

Atsižvelgdama į tai, Europos duomenų apsaugos valdyba taip pat primena, kad savo pasiūlymo dėl Reglamento dėl teisės į privatų gyvenimą ir asmens duomenų apsaugos elektroninių ryšių sektoriuje (e. privatumas) 14 konstatuojamojoje dalyje Komisija teigia, jog „elektroninių ryšių duomenys turėtų būti apibrėžti pakankamai plačiai ir technologškai neutraliai, kad apimtų bet kokią informaciją apie perduodamą turinį arba turinį, kuriuo keičiamasi (elektroninių ryšių turinį), ir informaciją apie galutinį elektroninių ryšių paslaugų gavėją, kuri tvarkoma perduodant, platinant elektroninių ryšių turinį arba sudarant sąlygas juo keistis, įskaitant duomenis, naudojamus ryšių operacijos šaltiniui ir paskirties vietai, geografinėi vietai, datai, laikui, trukmei ir rūšiai atsekti ir nustatyti.“ Kadangi esama ir būsima e. privatumo sistema, taip pat susiję teisės į privatų gyvenimą apribojimai bus taikomi teisėsaugos institucijų prieigos prie elektroninių įrodymų taisyklėms, Europos duomenų apsaugos valdyba rekomenduoja, kad į siūlomą reglamentą būtų įtraukta platesnė elektroninių ryšių duomenų apibrėžtis, siekiant užtikrinti, kad atitinkamos prieigos apsaugos priemonės ir sąlygos, kurios turi būti nustatytos, nuosekliai aprėptų tiek turinio, tiek su turiniu nesusijusius duomenis.

7. Europos įrodymų saugojimo ir pateikimo orderių procedūrų analizė

Apskritai kalbant, įrodymų pateikimo ar saugojimo orderių pateikimo procedūra yra tokia:

- Kompetentinga teisminė institucija, t. y. išduodančioji institucija, priklausomai nuo prašomų duomenų ir orderio tipo, išduoda orderį pagal (neišsamias) sąlygas, išvardytas 5 ir 6 straipsniuose, ir naudodama suderintą sertifikatą išsiunčia jį paslaugų teikėjo teisiniui atstovui ar bet kuriai iš jo įmonių (buveinių) ES, t. y. adresatui.
- Gavę sertifikatą, adresatai vykdo orderį, t. y. per 10 dienų arba skubos atveju per 6 valandas perduoda duomenis arba saugo juos iki 60 dienų, išskyrus atvejus, kai neįmanoma to padaryti dėl to, kad sertifikatas yra neišsamus, dėl *force majeure* ar faktinio adresato negalėjimo arba dėl to, kad adresatas atsisako jį vykdyti dėl prieštaraujančių įsipareigojimų, susijusių arba su trečiosios šalies pagrindinėmis teisėmis, arba su jos pagrindiniais interesais, arba dėl kitų priežasčių.
- Jeigu adresatas nevykdo gauto orderio nepateikdamas priežasčių, kurias patvirtintų išduodančioji institucija, numatomos vykdymo procedūros, kurių imasi kompetentinga vykdymo užtikrinimo institucija valstybėje narėje, kurioje yra atstovaujamas arba įsisteigęs paslaugų teikėjas, išskyrus atvejus, kai taikomos riboto atsisakymo pagrindų sąrašo priežastys ir vykdymo užtikrinimo institucija prieštarauja orderio pripažinimui ir vykdymui.
- Jeigu adresatas pateikia motyvuotą prieštaravimą dėl orderio, pagrįstą prieštaraujančiais įsipareigojimais, išduodančioji institucija perduoda bylą kompetentingam savo valstybės narės teismui, kuris tada turi įvertinti galimą prieštaravimą, jeigu prieštaravimo nėra, patenkinti orderį. Esant prieštaravimui, kai nustatomi prieštaraujantys įsipareigojimai, susiję su trečiosios šalies pagrindinėmis teisėmis ar pagrindiniais interesais, kompetentingas teismas per savo

nacionalines centrinės valdžios institucijas kreipiasi į trečiosios šalies centrinės valdžios institucijas ir skiria 15 dienų terminą atsakymui pateikti, kuris, pateikus pagrįstą prašymą, gali būti pratęstas dar 30 dienų, arba, kai adresatas nurodo kitas atsisakymo priežastis, pats nusprendžia patenkinti arba atmesti orderį.

- Nepažeidžiant Bendrajame duomenų apsaugos reglamente ir Teisėsaugos direktyvoje numatytų priemonių, asmenys, kurių duomenys buvo gauti išduodant įrodymų pateikimo orderį, taip pat turi teisę pasinaudoti veiksmingomis teisių gynimo nuo šio orderio priemonėmis.

Europos duomenų apsaugos valdyba įvertino reglamento projekte numatytas procedūras ir nustatytas apsaugos priemones, taikomas įvairiuose etapuose, ir kiekvienu toliau nurodytu aspektu rekomenduoja taikyti toliau išvardytas apsaugos priemones ir pakeitimus.

a) Turėtų būti padidintos orderių išdavimui taikomos ribos ir orderius turi išduoti arba tvirtinti teismai

Kiek tai susiję su orderių išdavimo sąlygomis, Europos duomenų apsaugos valdyba palankiai vertina griežtesnių priemonių prieš sandorių ir turinio duomenų apsaugos priemonių taikymo principą. Tačiau valdyba pažymi, kad, atsižvelgiant į tai, jog valstybėse narėse baudžiamosios sankcijos nėra visapusiškai suderintos, nuoroda į nusikalstamas veikas, už kurias išduodančiojoje valstybėje baudžiama laisvės atėmimo bausme, kurios ilgiausias terminas – ne mažiau kaip 3 metai²², reiškia, kad ES taikomos skirtingos ribos ir yra neatitinkimų duomenų subjektų duomenų apsaugos srityje.

Be to, Europos duomenų apsaugos valdyba pabrėžia, kad ypač atsižvelgiant į plačią duomenų apie abonentą apibrėžtį, nustatyta riba, taikoma įrodymų saugojimo ir įrodymų pateikimo orderiams, susijusiems su duomenimis apie abonentą ar priemonių duomenimis, atrodo gana žema, kadangi nusikalstamos veikos iš esmės gali pagrįsti tokių orderių išdavimą. Institucijų, turinčių teisę išduoti tokius orderius, veiksmai taip pat yra labiau ribojami joms išduodant įrodymų pateikimo orderius, susijusius su sandorių ir turinio duomenimis, nei išduodant įrodymų saugojimo arba pateikimo orderius, susijusius su duomenimis apie abonentą ar priemonių duomenimis, nes prokurorai gali išduoti ar tvirtinti tik pastaruosius orderius, o bet koks teisėjas, teismas ar ikiteisminio tyrimo teisėjas gali išduoti ar tvirtinti bet kokius orderius.

Europos duomenų apsaugos valdyba ypač apgailestauja, kad žemiausia riba, pagal kurią teisėsaugos institucijos turi galimybę dėl bet kokios nusikalstamos veikos reikalauti priemonių prieš abonento ir priemonių duomenų, pagrįsta Europos Sąjungos Teisingumo Teismo praktikos (kurioje daugiausia dėmesio skiriama kitiems duomenims) *a contrario* aiškinimu, siekiant atskirti taikytinas apsaugos priemones. Europos Sąjungos Teisingumo Teismas konkrečiai pabrėžė, kad kompetentingos institucijos gali gauti priegią prie srauto ir buvimo vietos duomenų tik kovos su sunkiais nusikaltimais tikslais²³. Europos duomenų apsaugos valdyba galėtų suprasti, jei pasiūlyme būtų numatyta galimybė prašyti priemonių tik prieš pagrindinės informacijos, kuri tik suteiktą galimybę nustatyti asmens tapatybę neatskleidžiant jokių ryšių duomenų be išankstinio teismo leidimo. Tačiau ji apgailestauja dėl plataus Komisijos šio sprendimo aiškinimo *a contrario* ir ragina nustatyti griežtesnes apsaugos priemones, kad būtų apriboti priemonių prieš kitų duomenų apie abonentą ir priemonių duomenų suteikimo pagrindai.

²² Žr. 5 straipsnio 3 dalies a punktą.

²³ Žr. bylos 203/15 125 punktą.

Europos duomenų apsaugos valdyba siūlo suteikti prieigą prie šių duomenų tik reglamento projekte išvardytų nusikaltimų atvejais arba sunkių nusikalstamų veikų atvejais, ypač atsižvelgiant į žemesnę išankstinių leidimų ribą, numatytą šiems duomenims.

Be to, Europos duomenų apsaugos valdyba pabrėžia, kad dėl šio *a contrario* aiškinimo pasiūlymu prokurorams suteikiama galimybė išduoti arba patvirtinti orderius. Europos duomenų apsaugos valdyba laikosi nuomonės, kad išskyrus atvejus, kai prašoma suteikti tik pagrindinę informaciją, kuri tiesiog suteiktų galimybę nustatyti asmens tapatybę neatskleidžiant ryšio duomenų, tai būtų žingsnis atgal, palyginti su Europos Sąjungos Teisingumo Teismo praktika, susijusia su prieiga prie ryšių duomenų. Iš tiesų Europos Sąjungos Teisingumo Teismas savo praktikoje, susijusioje su prieiga prie ryšių duomenų teisėsaugos tikslais, be kitų kriterijų ir „išskyrus tinkamai pagrįstus skubos atvejus“²⁴, nustatė galimybę suteikti tokią prieigą tik „teismui ar nepriklausomai administracinei institucijai atlikus išankstinę kontrolę“, „gavus motyvuotą kompetentingų nacionalinių institucijų prašymą, kurį jos pateiktų vykdydamos prevencijos, atskleidimo arba baudžiamojo persekiojimo procedūras“.²⁵

Europos duomenų apsaugos valdyba primena, kad sąvoka „teismas“ yra savarankiška ES teisės sąvoka ir kad Europos Sąjungos Teisingumo Teismas nuolat pabrėžia ir primena kriterijus, kuriuos turi atitikti teismas, kad būtų laikomas teismu, įskaitant nepriklausomumo kriterijų²⁶, kuris nėra taikomas prokurorams, kaip savo praktikoje nurodė ir EŽTT²⁷.

Todėl taikant 4 straipsnio 1 dalies a ir b punktus ir 3 straipsnio a ir b punktus atliekamos procedūros, kurioms bus taikoma gerokai mažiau duomenų apie abonentą ir prieigos duomenų apsaugos priemonių, nes pats prokuroras galės prašyti duomenų netaikant papildomos kontrolės, kurią vykdytų valstybės, kurioje yra prašomi duomenys, institucija ar institucija, kurioje yra bendrovės, į kurią kreipiamasi, teisinis atstovas, taip pat netaikant jokios nepriklausomos administracinės institucijos vykdomos kontrolės.

Be to, Europos duomenų apsaugos valdyba pažymi, kad vadinamoji papildoma apsaugos priemonė, numatyta 5 straipsnio 2 dalyje, apriboja galimybę išduoti įrodymų pateikimo orderį, jeigu dėl tos pačios nusikalstamos veikos panašioje vidaus situacijoje galėjo būti taikoma panaši priemonė. Tačiau ji įspėja dėl tokios nuostatos neigiamo poveikio: užuot suteikusi papildomų apsaugos priemonių, ji skatina valstybes nars išplėsti savo galimybes prašyti pateikti duomenis apie abonentą ar prieigos duomenis, kad užtikrintų galimybę išduoti įrodymų pateikimo orderius pagal šį reglamentą.

b) Duomenų pateikimo terminai turėtų būti pagrįsti

Europos duomenų apsaugos valdyba pažymi, kad Europos įrodymų pateikimo orderiai vykdomi ne vėliau kaip per 10 dienų nuo sertifikato gavimo, išskyrus atvejus, kai išduodančioji institucija nurodo priežastis, dėl kurių informacija turi būti atskleista anksčiau, o skubos atvejais – ne vėliau kaip per 6 valandas, kaip nustatyta 9 straipsnio 1 ir 2 dalyse.

Tačiau Europos duomenų apsaugos valdyba pasigedo kriterijų, pagal kuriuos būtų nustatomas įpareigojimas institucijoms įrodyti duomenų pateikimo skubumą, net ir *ex post*, siekiant suteikti galimybę patikrinti, kaip taikoma ši labai greita procedūra, o šešių valandų terminas gali reikšti, kad paslaugų teikėjo atliekamas patikrinimas prieš pateikiant duomenis gali būti labai paviršutiniškas arba jo gali išvis nebūti. Iš tiesų poveikio vertinime pabrėžiama, jog būtina, kad kompetentingos institucijos laiku gautų prieigą prie duomenų. Vis dėlto visi poveikio vertinime pateikti pavyzdžiai susiję su

²⁴ Žr. bylos 203/15 120 punktą.

²⁵ Žr. sujungtas bylas C 293/12 ir C 594/12, 62 punktą.

²⁶ Žr., pvz., bylą C 203/14.

²⁷ Žr., pvz., 2010 lapkričio 23 d. sprendimą *Moulin / Prancūzija*.

įrodymais, kurių reikia tais atvejais, kai daromi sunkūs nusikaltimai (teroristinių nusikaltimų atvejai, kai žmonės paaimami įkaitais, vykdoma seksualinė prievarta prieš vaikus), tačiau įrodymų nepastovumas nėra tinkamas pagrindas, kai be jo nėra kitų konkrečių skubos priežasčių. Be to, proporcingumo aspektu duomenų nepastovumas nesuteikia jokio papildomo pagrindo šiose situacijose gauti prieigą prie duomenų taikant mažiau apsaugos priemonių, kai, be duomenų nepastovumo, nėra kitų skubos priežasčių.

Europos duomenų apsaugos valdyba taip pat abejoja dėl būtinybės numatyti šešių valandų terminą, kartu numatant, kad šis terminas nebūtų taikomas, kol išduodančioji institucija „per penkias dienas“ pateiktų papildomų paaiškinimų, jeigu paslaugų teikėjas negalėtų vykdyti savo įsipareigojimo.

Todėl Europos duomenų apsaugos valdyba ragina į poveikio vertinimą įtraukti papildomų elementų siekiant pagrįsti šių terminų būtinybę tais atvejais, kai daromas nusikaltimas ar nusikaltimas, už kurį traukiama baudžiamoji atsakomybė, nėra sunkus, jeigu tokie išsamūs elementai nėra nustatyti, taip pat ragina įtraukti išsamius kriterijus, kuriais remiantis būtų pateisinama skuba Europos įrodymų pateikimo orderio sertifikatų išdavimo atveju. Pavyzdžiui, galėtų būti numatytas toks pat modelis, kaip ir ETO direktyvoje. ETO direktyvoje numatomas trumpesnis terminas, kai tai pateisinama „dėl procesinių terminų, nusikalstamos veikos sunkumo arba kitų ypatingos skubos aplinkybių“ (žr. 12 straipsnio 2 dalį), arba 24 valandų terminas, skirtas sprendimui dėl laikinųjų priemonių priimti (žr. 32 straipsnio 2 dalį.) Reglamento projekto poveikio vertinime nenumatyti konkretūs elementai, kuriais būtų pagrįsta, kodėl šie terminai nėra veiksmingi, o vieninteliai elementai, kurie pabrėžiami, yra tai, jog siunčiamais prašymais pernelyg apkraunamos gaunančiosios teisminės institucijos, kurios negali laikytis terminų.

c) Europos įrodymų pateikimo ir saugojimo orderiai neturi būti naudojami norint paprašyti kitos valstybės narės duomenų subjekto duomenų bent neinformavus tos valstybės narės kompetentingų institucijų, ypač kiek tai susiję su turinio duomenimis

Europos duomenų apsaugos valdyba primena, kad esamose priemonėse numatytas teisminis bendradarbiavimas ir papildomos apsaugos priemonės, visų pirma siekiant patikrinti prašymų būtinumą ir proporcingumą, ir pabrėžia, kad visos šios apsaugos priemonės yra juo labiau pateisinamos, kai prašomi duomenys yra turinio duomenys, kurie susiję su daugiau duomenų subjektų teisių į jų asmens duomenų ir privatumo apsaugą apribojimų. Šiuo atžvilgiu Europos duomenų apsaugos valdyba primena, kad ETO direktyvoje taip pat numatyta galimybė perimti telekomunikacijų tinklais perduodamą informaciją naudojantis kitos valstybės narės teikiama technine pagalba (žr. 30 straipsnį), taip pat nustatytas įpareigojimas pranešti kitos valstybės narės kompetentingai institucijai apie bet kokį duomenų perėmimą, kai pagalba nėra reikalinga ir kai susijęs duomenų subjektas yra arba bus tos valstybės narės teritorijoje (žr. 31 straipsnį).

Europos duomenų apsaugos valdyba nepateisina procedūros, numatytos Elektroninių įrodymų reglamento projekte, kuri suteikia galimybę pateikti turinio duomenis visiškai nedalyvaujant bent valstybės narės, kurioje yra duomenų subjektas, kompetentingoms institucijoms.

d) Europos įrodymų saugojimo orderiai neturi būti naudojami paslaugų teikėjams siekiant išvengti duomenų saugojimo įsipareigojimų

Europos duomenų apsaugos valdyba atkreipia dėmesį į tai, kad Europos įrodymų saugojimo orderių pagrindinis tikslas – užkirsti kelią duomenų ištrynimui.

Europos duomenų apsaugos valdyba pripažįsta, kad kai kuriais atvejais tai gali būti reikalinga ir proporcinga, tačiau apgailestauja, kad nėra pakankamai apsaugos priemonių, taikomų išduodant tokius orderius. Visų pirma, Europos duomenų apsaugos valdyba rekomenduoja, kad kai įrodymų saugojimo orderiai išduodami tik dėl konkrečių duomenų (projekte, regis, suteikiama galimybė teikti plataus pobūdžio prašymus) ir kai tokie orderiai išduodami dėl duomenų, kuriuos numatyta ištrinti laikantis duomenų saugojimo principo, orderis niekada nebūtų naudojamas kaip pagrindas paslaugų teikėjui tvarkyti duomenis po pradinės ištrynimo datos. Kitaip tariant, duomenys turėtų būti „išaldyti“.

Be to, sąsaja tarp įrodymų saugojimo orderio ir vėlesnio prašymo pateikti duomenis, ar tai būtų daroma pasitelkiant Europos įrodymų pateikimo orderį, ETO prašymą ar savitarpio teisinės pagalbos prašymą, turėtų būti stiprinama siekiant užtikrinti, kad Europos įrodymų saugojimo orderiai būtų išduodami tik tada, kai patenkinamas kitas prašymas (jie neturėtų būti tik svarstomi kaip galimybė), o kai kitas prašymas atmetamas, įrodymų saugojimo orderio galiojimas taip pat pasibaigtų, nelaukiant 60 dienų²⁸, jeigu vėliau pateiktas prašymas atmetamas anksčiau.

e) Konfidencialumas ir informacija apie naudotoją

Europos duomenų apsaugos valdyba pažymi, kad į reglamento projektą įtrauktas specialus straipsnis²⁹, susijęs su pateiktų orderių konfidencialumu. Tam, kad būtų išvengta painiavos ir nesusipratimų dėl teisės į duomenų apsaugą, Europos duomenų apsaugos valdyba primena, kad nors Bendrajame duomenų apsaugos reglamente nustatyta, kad duomenų subjektų teisių apribojimai siekiant užtikrinti nusikalstamų veikų prevenciją, tyrimą, atskleidimą ar baudžiamąjį persekiojimą turėtų būti numatyti įstatymuose ir viešai skelbiami³⁰ ir kad į šias teisėkūros priemones turi būti įtrauktos konkrečios nuostatos dėl duomenų subjektų teisės būti informuotam apie apribojimą, išskyrus atvejus, kai tai gali pakenkti apribojimo tikslui³¹, jame nėra nustatytas įpareigojimas atskirai informuoti duomenų subjektus apie kiekvieną teisės saugos institucijų pateiktą priegigos prašymą.

Tačiau Europos duomenų apsaugos valdyba taip pat primena, kad Duomenų apsaugos direktyvoje numatyta ši duomenų subjektų teisė gauti informaciją iš pačių kompetentingų institucijų, jeigu ši teisė nėra apribota; ši teisė suteikiama visiems duomenų subjektams, o ne tik duomenų subjektams, gyvenantiems ES teritorijoje.

f) Orderio vykdymo užtikrinimo procedūra, taikoma, kai paslaugų teikėjas atsisako jį vykdyti

Europos duomenų apsaugos valdyba atkreipia dėmesį į tai, kad reglamento projekto 14 straipsnyje numatyta procedūra, kuria užtikrinamas orderio vykdymas, kai adresatas nesilaiko jame nustatytų reikalavimų, vykdoma bendradarbiaujant išduodančiajai institucijai ir vykdančiosios valstybės kompetentingai institucijai.

Vis dėlto ši procedūra nesuteikia vykdymo užtikrinimo institucijai galimybės atsisakyti užtikrinti perduoto orderio vykdymą dėl kitų nei vien procedūrinių priežasčių (taip pat, kaip ir adresatas daugiausia dėl nepakankamos pateiktos informacijos ar faktinio negalėjimo pateikti duomenis), nes atitinkami duomenys saugomi pagal nacionalinę teisę teikiamų privilegijų ir imunitetų arba dėl to, kad

²⁸ Žr. 10 straipsnio 1 dalį.

²⁹ Žr. 11 straipsnį.

³⁰ Žr. 23 straipsnio 1 dalies d punktą.

³¹ Žr. 23 straipsnio 2 dalies h punktą.

jų atskleidimas gali pakenkti jos pagrindiniams interesams, pavyzdžiui, nacionaliniam saugumui ir gynybai³².

Todėl Europos duomenų apsaugos valdyba dar kartą išreiškia susirūpinimą dėl perduoto orderio bet kokio pakartotinio patikrinimo, kurį vykdo gaunančioji kompetentinga institucija, panaikinimo, palyginti su kitomis priemonėmis. Netgi pagrindas atsisakyti užtikrinti orderio vykdymą dėl to, kad juo būtų pažeista Chartija, regis, yra viršesnis už įprastą ribą, susijusią su atitinkamo asmens pagrindinių teisių pažeidimu. Todėl remiantis Europos arešto orderio, kuriame numatytas privalomas ir pasirenkamas atsisakymo pagrindas, pavyzdžiu ar bent jau ETO direktyva, kurioje bendrai numatyta, kad „laisvės, saugumo ir teisingumo erdvės kūrimas Sąjungoje grindžiamas tarpusavio pasitikėjimu ir prezumpcija, kad kitos valstybės narės laikosi Sąjungos teisės ir visų pirma paiso pagrindinių teisių“, tačiau ta prezumpcija yra nuginčijama³³, reglamento projekte turėtų būti bent jau numatyta įprastinė nukrypti leidžianti nuostata, pagal kurią tais atvejais, kai esama pagrįstų priežasčių manyti, kad dėl orderio vykdymo būtų pažeista atitinkamo asmens pagrindinė teisė ir kad vykdančioji valstybė nesilaikytų savo įsipareigojimų, susijusių su Chartijoje įtvirtintų pagrindinių teisių apsauga, turėtų būti atsisakoma užtikrinti orderio vykdymą.

g) Orderių vykdymo užtikrinimas ir prieštaraujantys įsipareigojimai pagal trečiosios šalies teisės aktus (15–16 straipsniai)

Europos duomenų apsaugos valdyba palankiai vertina reglamento projekte numatytą galimybę adresatams atsisakyti vykdyti orderį dėl to, kad juo būtų pažeidžiamos pagrindinės teisės, nes ja siekiama suteikti apsaugos priemonės tais atvejais, kai teisiniai įsipareigojimai vienas kitam prieštarauja. Taip pat labai svarbu, kad pasiūlyme būtų numatytos konsultacijos su trečiųjų šalių institucijomis, bent jau kilus prieštaravimams, taip pat įsipareigojimas atšaukti orderį, kai trečiosios šalies institucija pareiškia prieštaravimą.

Todėl numatyta procedūra, pagal kurią atsisakoma vykdyti orderį dėl prieštaraujančių įsipareigojimų pagal trečiosios šalies teisės aktus, turėtų būti gerokai patobulinta.

Pirma, Europos duomenų apsaugos valdyba pažymi, kad reglamento projektu privačiai bendrovei, kaip įrodymų pateikimo orderio adresatui, pavedama įvertinti, ar tas orderis prieštarautų taikomiems trečiosios šalies teisės aktams, kuriais draudžiama atskleisti prašomus duomenis, ar ne. Bendrovė turi pateikti motyvuotą prieštaravimą, kuriame būtų nurodyta visa svarbi informacija apie trečiosios šalies teisę, jos taikymą nagrinėjamoje byloje ir prieštaraujančių įsipareigojimų pobūdį.

Svarbiausia, kad Europos duomenų apsaugos valdyba yra susirūpinusi dėl to, kad kai kyla toks prieštaravimas, išduodančiosios institucijos valstybės narės kompetentingas teismas pats įvertina, ar esama prieštaravimo, ar ne, nes tik nustatęs prieštaravimą teismas susisieikia su trečiosios šalies institucijomis. Todėl šiuo atžvilgiu ES kompetentingam teismui suteikiama kompetencija pateikti galutinį trečiosios šalies teisės išaiškinimą, neturint itin daug patirties šioje srityje. Todėl Europos duomenų apsaugos valdyba mano, kad įpareigojimas konsultuotis su trečiosios šalies kompetentingomis institucijomis šiame pasiūlyme yra pernelyg ribotas. Kalbant apie duomenų apsaugą, Europos duomenų apsaugos valdyba atkreipia teisės aktų leidėjo dėmesį į tai, kad jeigu kompetentingas trečiosios šalies teismas aiškintų Bendrąjį duomenų apsaugos reglamentą siekdamas įvertinti, ar jis prieštarauja jame nustatytiems reikalavimams, ES duomenų apsaugos institucijos ir kompetentingi teismai išlaikytų kompetenciją vertinti perdavimo teisėtumą remiantis trečiosios šalies

³² Žr. 14 straipsnio 2 dalį.

³³ Žr. ETO direktyvos 19 konstatuojamąją dalį.

Formatted: Lithuanian

Formatted: Lithuanian

teismo ar administracinės institucijos sprendimu, pagal kurį reikalaujama perduoti ar atskleisti asmens duomenis, kuriems taikomas Bendrasis duomenų apsaugos reglamentas³⁴.

Be to, Europos duomenų apsaugos valdyba pabrėžia, kad prašančiosios ES valstybės kompetentingo teismo atliekamas trečiosios šalies teisės aktų vertinimas turi būti pagrįstas objektyviais elementais, ir yra susirūpinusi dėl kriterijų, į kuriuos turi atsižvelgti kompetentingas teismas vertindamas trečiosios šalies teisę pagal reglamento projekto 15 straipsnio 4 dalį ir 16 straipsnio 5 dalies a punktą. Iš tiesų teismas turėtų įvertinti tai, „ar pagal trečiosios šalies teisę, užuot siekus apsaugoti pagrindines teises arba trečiosios šalies pagrindinius interesus, susijusius su nacionaliniu saugumu arba gynyba, akivaizdžiai siekiama apsaugoti kitus interesus arba ja siekiama apsaugoti neteisėtą veiklą nuo teisės saugos prašymų atliekant baudžiamuosius tyrimus“ ar „atitinkamos trečiosios šalies teisės saugomą interesą, įskaitant trečiosios šalies interesą užkertant kelią duomenų atskleidimui“. Pavyzdžiui, nors iš esmės turėtų būti atliekamas įrodymais pagrįstas vertinimas atsižvelgiant į visą turimą informaciją, bent jau turint omenyje galimą tokio sprendimo poveikį, formuluotė („ja siekiama“) yra neaiški ir turėtų būti pakeista („jos tikslas / uždavinys“).

Europos duomenų apsaugos valdyba apgailestauja dėl to, kad su trečiosios šalies institucijomis būtų konsultuojamasi ir jos galėtų prieštarauti duomenų pateikimo orderio vykdymui tik tuo atveju, jeigu ES kompetentingas teismas manytų, jog esama reikšmingo prieštaravimo, perduotų visą informaciją atitinkamos trečiosios šalies centrinės valdžios institucijoms, o tos trečiosios šalies centrinė valdžios institucija pareikštų prieštaravimą per labai trumpą ir ne ilgesnį kaip 50 dienų terminą (15 dienų terminas, kuris gali būti pratęstas dar 30 dienų, o po paskutinio galimo priminimo gali būti skiriamos papildomos 5 dienos). Visais kitais atvejais kompetentingas teismas galėtų patenkinti įrodymų pateikimo orderį ir skirti piniginę baudą orderį atsisakiusiam vykdyti paslaugų teikėjui. Taigi Europos duomenų apsaugos valdyba yra susirūpinusi, kad ES kompetentingi teismai nebus platesniu mastu įpareigoti konsultuotis su atitinkamų šalių kompetentingomis institucijomis siekiant užtikrinti, kad vykdant šią procedūrą būtų sistemingai atsižvelgiama į abiejų šalių argumentus ir parodoma dar daugiau pagarbos trečiųjų šalių teisei.

Kaip jau pabrėžta pirmiau minėtame 29 straipsnio darbo grupės pareiškime, Europos duomenų apsaugos valdyba ragina ypatingą dėmesį skirti trečiosiose šalyse priimamoms panašioms priemonėms, galinčioms daryti poveikį duomenų subjektų teisėms ir jų teisei į privatumą ES, ypač panašių priemonių, kurios tiesiogiai prieštarautų ES duomenų apsaugos teisės aktams, keliamai rizikai.

Be to, Europos duomenų apsaugos valdyba pabrėžia, kad išduodančiosios institucijos valstybės narės kompetentingas teismas gali nebūti kompetentingas užtikrinti orderio vykdymą, kaip numatyta reglamento projekto 14 straipsnyje, o dėl to teisės kolizijos atveju dar labiau padidėtų prieštaraujančių procedūrų tikimybė ir nebūtų atliekami kryžminiai patikrinimai. Tai susiję su tuo, kad kai kuriais atvejais gali dalyvauti trys valstybės: orderį išdavusios institucijos valstybė, paslaugų teikėjo trečioji šalis ir valstybė narė, kurioje yra paslaugų teikėjo teisinis atstovas ES ir kurioje orderis turėtų būti vykdomas. Taigi, laikydamasis šiuo metu numatytos procedūros, prašančiosios institucijos valstybės narės (A) teismas galėtų savaip aiškinti trečiosios šalies (B), kurioje yra paslaugų teikėjas, teisę neklausdamas tos trečiosios šalies institucijų nuomonės (o jos būtų prieštaravusios orderiui) ir paprašyti kitos ES valstybės narės (C) vykdyti jo sprendimą be galimybės prieštarauti.

Be to, Europos duomenų apsaugos valdyba taip pat palankiai vertina tai, kad, be Bendrajame duomenų apsaugos reglamente ir Teisės saugos direktyvoje numatytų teisių gynimo priemonių, yra numatytos konkrečios teisių gynimo priemonės, taikomos įrodymų pateikimo orderių atvejais. 29 straipsnio darbo grupė savo ankstesniame pareiškime jau ragino priimti tokias apsaugos priemones. Vis dėlto Europos

³⁴ Žr. Bendorjo duomenų apsaugos reglamento 48 straipsnį.

duomenų apsaugos valdyba apgailestauja, kad tokios teisių gynimo priemonės nėra numatytos įrodymų saugojimo orderių atvejais, kadangi šiais orderiais gali būti ribojamos asmenų, kurių duomenys yra saugomi, pagrindinės teisės. Dėl įrodymų saugojimo orderių duomenys gali būti saugomi ilgiau, nei jie būtų saugomi pagal duomenų apsaugos taisykles. Todėl įrodymų saugojimo orderis pats savaime lemia atitinkamo duomenų subjekto pagrindinių teisių apribojimą; jo pagrindimas turi būti peržiūrimas ir jam turi būti taikomos teisių gynimo priemonės, ypač tais atvejais, kai įrodymų saugojimo orderis išduodamas kartu su įrodymų pateikimo orderiu siekiant gauti duomenis. Kaip savo pareiškime rekomendavo 29 straipsnio darbo grupė, turėtų būti numatytos teisių gynimo priemonės, kurios būtų bent lygiavertės vidaus atvejais taikomoms priemonėms.

h) Duomenų perdavimo saugumas vykdant orderį

Europos duomenų apsaugos valdyba pažymi, kad reglamento projekte numatytas tik orderių perdavimas gavėjams, esantiems Europos Sąjungoje, tačiau nenumatytas joks specialus duomenų perdavimo kanalas tarp adresatų ir paslaugų teikėjų, esančių už Europos Sąjungos ribų.

Europos duomenų apsaugos valdyba palankiai vertina tai, jog nėra daugiau nuostatų, leidžiančių nukrypti nuo bendros ES duomenų apsaugos sistemos, tačiau primena, kad bet koks adresatui nusiųstas orderis, kurį vykdant duomenys turėtų būti perduodami už ES ribų, turėtų būti išduodamas laikantis Bendrajame duomenų apsaugos reglamente nustatytos teisinės sistemos. Apeidami teisinio bendradarbiavimo teisinę sistemą, kurioje numatyta, kad turi būti laikomasi duomenų apsaugos priemonių, įrodymų pateikimo ir saugojimo adresatai neturėtų taip pat apeiti duomenų perdavimo reikalavimų, kad vykdytų tokius orderius.

Be to, Europos duomenų apsaugos valdyba palankiai vertina tai, jog nėra nuostatų, įpareigojančios iššifruoti šifruotus duomenis³⁵, tačiau ji susirūpinusi dėl to, kad pasiūlymo projekte nenumatyti konkretūs reikalavimai adresatams įvertinti pateiktų duomenų autentiškumą, ir pabrėžia, kad šis vertinimas taip pat suteikia pridėtinę vertę įprastinėms teisiniu bendradarbiavimu grindžiamoms priemonėms, taip pat įspėja apie didesnę riziką, kylančią atitinkamiems duomenų subjektams, kai toks vertinimas nėra atliekamas.

Išvados

Atsižvelgdama į šį vertinimą, Europos duomenų apsaugos valdyba nori teisėkūros institucijoms pateikti šias rekomendacijas:

- 1) Reglamento teisinis pagrindas neturėtų būti SESV 82 straipsnio 1 dalis.
- 2) Naujos priemonės būtinybė, palyginti su galiojančia ETO direktyva ar savitarpio teisinės pagalbos susitarimu, turėtų būti geriau pagrįsta, taip atliekant išsamią pagrindines teises mažiau ribojančių priemonių, analizę; pavyzdžiui, turėtų būti išnagrinėtos galimybės iš dalies pakeisti šias galiojančias priemones arba į šios priemonės taikymo sritį įtraukti tik įrodymų saugojimo orderius kartu taikant kitas galiojančias prašymo suteikti prieigą prie duomenų procedūras.
- 3) Reglamente turėtų būti numatytas ilgesnis terminas, per kurį vykduojantis paslaugų teikėjas galėtų užtikrinti apsaugos priemones, taikomas siekiant apsaugoti pagrindines teises.
- 4) Turėtų būti išlaikytas abipusio baudžiamumo principas, ypač jeigu atsisakoma buvimo vietos duomenų kriterijaus siekiant išlaikyti įpareigojimą atsižvelgti į apsaugos priemones, numatytas

³⁵ Žr. 19 konstatuojamąją dalį ir poveikio vertinimo 240 p.

- abiejose susijusiose valstybėse (prašančiosios institucijos valstybėje ir valstybėje, kurioje yra paslaugų teikėjas).
- 5) Į reglamento taikymo sritį turėtų būti įtraukti tik valdytojai, kaip apibrėžta Bendrajame duomenų apsaugos reglamente, arba turėtų būti įtraukta nuostata, pagal kurią tokiu atveju, kai paslaugų teikėjas, į kurį kreipiamasi, yra ne duomenų valdytojas, o tvarkytojas, jis privalo informuoti valdytoją.
 - 6) Į reglamentą turėtų būti įtrauktos apsaugos priemonės, taikomos perduodant duomenis, jeigu paslaugų teikėjas būtų įsisteigęs trečiojoje šalyje ir nebūtų priimtas sprendimas dėl tinkamumo šioje srityje, arba nuoroda į Direktyvą 2016/680 dėl šių apsaugos priemonių taikymo.
 - 7) Kadangi privalomas teisinio atstovo skyrimas skiriasi nuo Bendrajame duomenų apsaugos reglamente numatyto įpareigojimo, šiame reglamente turėtų būti tiksliai nurodyta, kad pagal Elektroninių įrodymų reglamentą paskirtas teisinis atstovas turėtų būti kitas nei teisinis atstovas, skiriamas pagal Bendrojo duomenų apsaugos reglamento 3 straipsnio 2 dalį.
 - 8) Į reglamentą turėtų būti įtraukta platesnė elektroninių ryšių duomenų apibrėžtis siekiant užtikrinti, kad atitinkamos priegos apsaugos priemonės ir sąlygos, kurios turi būti nustatytos, nuosekliai aprėptų tiek turinio, tiek su turiniu nesusijusius duomenis.
 - 9) Reglamentu turėtų būti padidintos orderių išdavimui taikomos ribos ir orderius turi išduoti arba tvirtinti teismai, išskyrus atvejus, susijusius su pateikiamais abonentų duomenimis, jeigu šios duomenų kategorijos apibrėžtis bus labai susiaurinta įtraukiant tik pagrindinę informaciją, suteikiančią galimybę nustatyti asmens tapatybę nesinaudojant prieiga prie jokių ryšių duomenų.
 - 10) Reglamentu turėtų būti suteikiama prieiga prie duomenų apie abonentą ir prieigos duomenų tik griežtai apibrėžtame sąraše išvardytų nusikaltimų atvejais arba sunkių nusikalstamų veikų atvejais.
 - 11) Terminas, per kurį turi būti pateikti duomenys, ypač skubos atvejais, reglamente turėtų būti geriau pagrįstas, o galimybė taikyti greitą 6 valandų procedūrą turėtų apimti įpareigojimą prašančiosioms institucijoms pagrįsti, dėl kokios ekstremaliosios situacijos turi būti taikoma ši procedūra, net ir *a posteriori*, siekiant suteikti galimybę patikrinti, kaip naudojamos šiais išskirtiniais įgaliojimais.
 - 12) Turėtų būti panaikinta procedūra, kuri suteikia galimybę pateikti duomenis nedalyvaujant valstybės narės, kurioje yra duomenų subjektas, kompetentingoms institucijoms.
 - 13) Reglamente numatytos apsaugos priemonės, taikomos išduodant Europos įrodymų saugojimo orderius, turėtų būti tobulinamos.
 - 14) Į reglamentą bent jau turėtų būti įtraukta numatyta įprastinė nukrypti leidžianti nuostata, pagal kurią tais atvejais, kai esama pagrįstų priežasčių manyti, kad dėl orderio vykdymo būtų pažeista atitinkamo asmens pagrindinė teisė ir vykdančioji valstybė nesilaikytų savo įsipareigojimų, susijusių su Chartijoje įtvirtintų pagrindinių teisių apsauga, turėtų būti atsisakoma užtikrinti orderio vykdymą.
 - 15) Reglamente turėtų būti numatytas platesnio masto įpareigojimas konsultuotis su trečiosios šalies, kurioje yra paslaugų teikėjas, kurio prašoma pateikti duomenis, kompetentingomis institucijomis teisės kolizijos atveju siekiant išvengti subjektyvių vieno teismo aiškinimų.
 - 16) Įrodymų saugojimo orderių galiojimo trukmė turėtų būti labiau susieta su įrodymų pateikimo orderiais, išduodamais kartu su jais.
 - 17) Turėtų būti geriau užtikrinamas duomenų perdavimo saugumas.
 - 18) Turėtų būti numatytas duomenų autentiškumo patikrinimas, ypač tais atvejais, kai gali būti pateikiami šifruoti duomenys.

Europos duomenų apsaugos valdybos vardu

Pirmininkė

(Andrea Jelinek)