

Justina DEŠRIŪTĖ
Lietuvos teisės institutas

ESMINIAI ASMENS DUOMENŲ APSAUGOS BAUDŽIAMAJAME PROCESSE REFORMOS EUROPOS SĄJUNGOJE ASPEKTAI IR JŲ ĮTAKA NACIONALINIAM TEISINIAM REGULIAVIMUI

Straipsnyje apžvelgiami esminiai Europos Sąjungos teisėkūroje vykstančios asmens duomenų apsaugos baudžiamajame procese reformos aspektai. Aptariamas kintantis asmens duomenų subjekto vaidmuo, pagrindinių teisių, susijusių su asmens duomenų apsauga, katalogas bei jų gynėbės būdai. Nurodžius esmines naujosios direktyvos dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, nustatymo ar traukimo baudžiamajame atsakomybės už jas arba baudžiamųjų sankcijų vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo nuostatas, įvertinami būtini nacionalinio reguliavimo pokyčiai šių nuostatų kontekste.

Asmens duomenų apsauga – sritis, kurios aktualumas auga kartu su technologijų plėtoje. Vis daugiau veiksmų atliekama elektroninėje erdvėje, gerokai didėja joje sukauptos ir pasiekiamos informacijos apie asmenis kiekis. Dalis šios informacijos yra konfidencialaus pobūdžio, jai būtina griežta apsauga. Užtikrinti savo asmens duomenų saugumą, kaip ir tai, kiek jų pasirenkama atskleisti kitiems subjektams, visų pirma yra kiekvieno žmogaus teisė ir pareiga, tačiau esama atvejų, kai šiais duomenimis disponuoja kiti subjektai. Šis disponavimas gali vykti tiek asmeniui apie tai žinant, tiek ne. Su pastarąja situacija dažnai susiduriama baudžiamajame procese, kai teisėsaugos institucijos renka, kaupia, naudoja konfidencialaus pobūdžio informaciją apie juos dominančius asmenis. Asmens duomenų apsaugos klausimas tampa taip pat svarbus tarptautinio pobūdžio baudžiamuosiuose procesuose. Vykstant tarptautiniam bendradarbiavimui, kyla po-

reikis nurodyto pobūdžio informaciją ne tik teisėtai rinkti, vertinti ir panaudoti, tačiau ir ja keistis skirtingų valstybių teisėsaugos institucijoms. Tam, kad šie procesai vyktų sklandžiai ir kartu visapusiškai apsaugant asmens, kurio duomenimis disponuojama, teises, yra būtinos aiškios, tikslios, lanksčios ir efektyvios taisyklės.

Šis poreikis aiškiai matyti Europos Sąjungos teisėkūroje. Asmens duomenų apsaugos srityje šiuo metu vyksta intensyvi reforma. 2016 m. balandžio 16 d. Europos Parlamentas balsavo už asmens duomenų apsaugos reformą, pradėtą 2012 metais, ir priėmė naujus teisės aktus, kuriuose reglamentuojami asmens duomenų apsaugos klausimai. Galutiniai suderintų teisės aktų tekstai 2016 m. gegužės 4 d. paskelbti ES Oficialiajame leidinyje¹, valstybės narės iki 2018 m. gegužės 6 d. privalės perkelti naujus teisės aktus į nacionalinę teisę. Pagrindinės reformos priežastys – aktualumą praradęs ir nesistemingas srities reguliavimas. Teisės aktai šioje srityje yra priimti prieš ilgą laiką. Pagrindinis teisės aktas, kuriuo vadovautasi teisinėje praktikoje – 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva Nr. 95/46/EB² dėl asmens apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo. Asmens duomenų panaudojimo mastai nuo šio laiko patyrė didelius pokyčius. Technologijų raida lėmė tai, kad duomenų panaudojimo būdai, prieinamumas ir sklaida tapo kur kas didesni. Kita priežastis – nesistemingas teisės aktų priėmimas. 1995 m. direktyva numatė tik esminius principus, kaip turi būti tvarkomi asmens duomenys, tačiau specifinėse srityse būtinos papildomos taisyklės priimtos atskirais teisės aktais, dažnai įtraukiant taisykles į platesnio reguliavimo teisės aktus. Asmens duomenų apsauga baudžiamajame procese yra būtent viena šių specifinių sričių. 2008 m. lapkričio 27 d. Europos Parlamento ir Tarybos pamatiniame sprendime 2008/977/TVR³ dėl asmens duomenų, tvarkomų vykdant policijos ir teisminį bendradarbiavimą baudžiamosiose bylose, apsaugos nustatyta, kokia asmens duomenų apsauga galioja baudžiamajame procese, vykdant tarptautinį bendradarbiavimą tarp ES valstybių narių. Tačiau pamatinio sprendimo apimtis gana siaura ir neužtikrina visų asmens duomenų apsaugos baudžiamajame procese poreikių.

Poreikį reformuoti asmens duomenų apsaugą atspindi ir pačių ES piliečių nuomonė: 2008 m. atlikta „Eurobarometro“ apklausa atskleidė, jog du trečdaliai apklaustų ES piliečių yra susirūpinę, ar subjektai, disponuojantys jų asmens duomenimis, tai daro tinkamai, o net 82 % asmenų jaučiasi neramūs, siūsdami asmens

¹ Oficialusis Europos Sąjungos leidinys, 2016 m. gegužės 4 d., 59 tomas, Nr. L 119.

² 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva Nr. 95/46/EB // Oficialusis leidinys L 281, 23/11/1995, p. 0031–0050.

³ 2008 m. lapkričio 27 d. Europos Parlamento ir Tarybos pamatinis sprendimas 2008/977/TVR dėl asmens duomenų, tvarkomų vykdant policijos ir teisminį bendradarbiavimą baudžiamosiose bylose, apsaugos // Oficialusis leidinys L 350, 30/12/2008, p. 60–71.

duomenis internetu, ir mano, kad duomenų apsauga nėra pakankama⁴. Viena šio nerimo priežasčių – smarkiai išaugęs asmens duomenų pasiekiamumas teisėsaugos institucijoms. Šių dienų ES teisėkūros pokyčiai apima tiek bendrąją asmens duomenų apsaugą, tiek specifinę jos dalį – asmens duomenų apsaugą baudžiamajame procese. 2016 m. balandžio 14 d. balsavimu Europos Parlamentas pritarė bendrajam duomenų apsaugos reglamentui – dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo⁵ ir Direktyvai dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, nustatymo ar traukimo baudžiamojon atsakomybėn už jas arba baudžiamųjų sankcijų vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo⁶ (toliau vadinama – **Direktyva**). Direktyvoje nustatomos asmens duomenų apsaugos taisyklės, kurios turės būti taikomos tiek nacionaliniuose baudžiamosiuose procesuose, tiek vykstant bendradarbiavimui tarp valstybių narių teisėsaugos institucijų.

Viena esminių Direktyvos, taip pat ir Reglamento naujovių – pakitęs duomenų subjekto vaidmuo asmens duomenų valdymo procese. Direktyvoje įtvirtinamos nuostatos, kuriomis siekiama užtikrinti aktyvų duomenų subjekto vaidmenį teisėsaugos institucijoms atliekant veiksmus su jo asmens duomenimis. Didesnis duomenų subjekto informuotumas, visapusiškesnis asmens įtraukimas į procesą, kurio metu disponuojama jo asmens duomenimis, neabejotinai išskirtinas vienu svarbiausių naujojo reguliavimo prioritetų. Reformos centre – taip pat ir duomenų subjekto teisė būti pamirštam, t. y. tuo atveju, kai nebėra teisėto pagrindo kaupti asmens duomenis ir subjektas to nebenori, jis turi teisę į duomenų ištrynimą. Šio vaidmens realizavimas – tiesiogiai priklausomas nuo valstybių narių nacionalinio reguliavimo ir teisės aktų įgyvendinimo praktikos. Pastebėtina, kad reforma neišsprendžia visų galimų asmens duomenų apsaugos baudžiamajame procese problemų. Vienas didžiausių Direktyvos trūkumų – taisyklių netaikymas keičiantis asmens duomenimis su tarptautinėmis institucijomis, Europolu, Eurojustu ir kt. Taip pat lieka neišspręstas ir juridinių asmenų duomenų apsaugos klausimas, kadangi Direktyva taikoma tik tvarkant fizinių asmenų duomenis.

⁴ Data Protection in the European Union-Citizens' perceptions - Analytical report, Viviane Reding Vice-President of the European Commission, EU Commissioner responsible for Justice, Fundamental Rights and Citizenship Data Protection 30 | eucrim 1 / 2010 Flash Eurobarometer Series 225, January 2008. Prieiga per internetą: <http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf>.

⁵ Pasiūlymas EUROPOS PARLAMENTO IR TARYBOS REGLAMENTAS dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (Bendrasis duomenų apsaugos reglamentas) /* COM/2012/011 final - 2012/011 (COD).

⁶ Pasiūlymas EUROPOS PARLAMENTO IR TARYBOS DIREKTYVA dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, nustatymo ar traukimo baudžiamojon atsakomybėn už jas arba baudžiamųjų sankcijų vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo /* COM/2012/010 final - 2012/0010 (COD).

Pastebėtina, kad nacionalinėje teisinėje literatūroje asmens duomenų apsauga baudžiamojo proceso metu yra aptarta minimaliai. Keletas šios srities aspektų yra apžvelgti L. Meškauskaitės monografijoje „Teisė į privatų gyvenimą“⁷, M. Gušauskienės straipsnyje „Asmens duomenų apsauga baudžiamajame procese“ aptariamais pagrindiniais nacionaliniais asmens duomenų apsaugos baudžiamajame procese aspektais, kurie, nors ir susiję, tiesiogiai nepatenka į naujojo reguliavimo apimtį, taigi šiame darbe su autorės mintimis nėra diskutuojama. Užsienio literatūroje asmens duomenų apsaugos baudžiamajame procese sritis yra tyrinėta išsamiau, tačiau ES reformos aspektai dėl jų naujumo kol kas tik pradedami nagrinėti. Šiuo klausimu išskirtinos I. Andoulsi, H. Hijamns, A. Scirocco, V. Reding, P. D. Hert ir V. Papakonstantinou mokslinės publikacijos. Straipsnio tikslas – naudojantis lyginamuoju, teleologiniu bei sisteminės analizės tyrimo metodais, aptarti esminius pokyčius, susijusius su asmens duomenų apsauga tvarkant asmens duomenis nacionaliniuose baudžiamuosiuose procesuose bei valstybių narių teisėsaugos institucijoms bendradarbiaujant baudžiamosiose bylose. Straipsniu taip pat siekiama įvertinti nacionalinio teisinio reguliavimo pakankumą, užtikrinant aktyvų duomenų subjekto vaidmenį šiame procese, bei siektinus teisinio reguliavimo pokyčius.

I. TEISINIS ASMENS DUOMENŲ APSAUGOS BAUDŽIAMAJAME PROCESU KONTEKSTAS

Asmens duomenų apsauga Europoje pripažįstama viena pagrindinių vertybių⁸. Apsauga deklaruojama Europos Sąjungos pagrindinių teisių chartijos 8 straipsnyje⁹, detalizuojama 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyvoje 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo bei 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyvoje 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje¹⁰. Asmens duomenų apsauga suprantama kaip sudėtinė teisės į privatų gyvenimą dalis¹¹,

⁷ *Meškauskaitė L.* Teisė į privatų gyvenimą // Vilnius: VĮ „Registru centras“, 2015.

⁸ *Reding V.* Data Protection in the EU – Challenges Ahead // EUCRIM, Issue 2010/1, p. 25–29.

⁹ Europos Sąjungos pagrindinių teisių chartija // Oficialusis leidinys, L 326, 26/10/2012, p. 391–407.

¹⁰ 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje // Oficialusis leidinys, L 201, 31/07/2002, p. 0037–0047.

¹¹ Literatūroje tiksliau ji įvardijama kaip vieno iš teisės į privataus gyvenimą elemento – informacijos privatumo dalis. *Meškauskaitė L.* Teisė į privatų gyvenimą, p. 8.

taigi yra saugoma Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos 8 straipsniu. Nuo 2008 m. asmens duomenų apsauga baudžiamajame procese Europos Sąjungoje yra reguliuojama Pamatiniu sprendimu 2008/977/TVR. Kaip minėta, tarptautiniame bendradarbiavime baudžiamosiose bylose asmens duomenų reguliavimas yra itin nenuoseklus, epizodiškas. Dažniausiai numatomos specifinės, nuo pagrindinio reguliuojamo klausimo priklausomos taisyklės (pavyzdžiui, Europolo, Eurojusto, Šengeno informacinės sistemos, Prum sistemos ir kt. nuostatos), kurios yra tik sudėtinė konkretaus teisės akto dalis.

Nuo Lisabonos sutarties¹² įsigaliojimo Europos Sąjungos veikimo sutartyje įtvirtintas 16 straipsnis, kuris tapo vieninteliu asmens duomenų apsaugos ES teisiniu pagrindu. Be abejo, asmens duomenų apsaugos svarba tiek bendrąja prasme, tiek siauresnėje tarptautinio bendradarbiavimo baudžiamosiose bylose srityje buvo pripažįstama ir iki Lisabonos sutarties. Nuosekliai deklaruoti esminiai duomenų apsaugos principai, tokie kaip teisėtas disponavimo duomenimis tikslas, proporcingumas, duomenų saugojimo terminas, saugumas ir konfidencialumas¹³. Europos Sąjungos veikimo sutarties 16 straipsnyje numatyta apsauga galioja tiek viešajam, tiek privačiajam sektoriui ir apima tarptautinio bendradarbiavimo baudžiamosiose bylose sritį, ankstesniame teisiniame reguliavime tai nebuvo numatyta. Be to, tiesiogiai įtvirtintas ir laisvas asmens duomenų judėjimo principas. Atsižvelgiant į tai, kad asmens duomenų apsauga baudžiamajame procese pasižymi specifika, Lisabonos sutarties sudėtinė dalimi taip pat yra Deklaracija Nr. 21 dėl asmens duomenų apsaugos teismo bendradarbiavimo baudžiamosiose bylose ir policijos bendradarbiavimo srityse. Deklaracijoje numatyta, kad dėl teismo bendradarbiavimo baudžiamosiose bylose ir policijos bendradarbiavimo sričių ypatingo pobūdžio šiose srityse gali reikėti konkrečių taisyklių dėl asmens duomenų apsaugos ir laisvo šių duomenų judėjimo, pagrįstų Sutarties dėl Europos Sąjungos veikimo 16 straipsniu. Būtent šios nuostatos ir tapo teisiniu pagrindu svarstyti naujų ES teisės aktų asmens duomenų apsaugos baudžiamajame procese srityje priėmimą.

Nacionalinėje teisėkūroje specifiškai asmens duomenų apsaugai baudžiamajame procese nėra skirta daug detalaus teisinio reguliavimo. Išskirtinos Lietuvos Respublikos baudžiamojo proceso kodekso (toliau vadinama – BPK) nuostatos, kuriomis nustatyta, jog asmens duomenys yra saugomi atskirai nuo baudžiamosios bylos medžiagos (BPK 181 straipsnio 1 dalis, 183 straipsnio 3 dalis, 218 straipsnio 3 dalis,

¹² Europos Sąjungos sutarties ir Sutarties dėl Europos Sąjungos veikimo suvestinės redakcijos // OL C 326, 2012.

¹³ *De Busser E.* EU data protection in transatlantic cooperation in criminal matters. Will the EU be serving its citizens an American meal? // *Utrecht Law Review*, 2010, vol. 6, Nr. 1, p. 95.

220 straipsnio 3 dalis, 237 straipsnio 3 dalis). Bendroji asmens duomenų apsauga baudžiamajame procese kildintina iš BPK 44 straipsnio 9 dalies nuostatos, kurioje įtvirtinta asmens teisė į privataus gyvenimo gerbimą. Tačiau detalesnio reguliavimo, kaip turi būti įgyvendinta ši teisė, nėra nustatyta. Tarptautinio bendradarbiavimo baudžiamosiose bylose srityje paminėtinas specifinis teisės aktas – 2011 m. priimtas Lietuvos Respublikos asmens duomenų, tvarkomų vykdančios policijos ir teisminį bendradarbiavimą baudžiamosiose bylose, teisinės apsaugos įstatymas (toliau vadinama – Įstatymas), kuris įtvirtina gana bendro pobūdžio nuostatas. Įstatymas priimtas, įgyvendinant 2008 m. lapkričio 27 d. Tarybos pamatinį sprendimą 2008/977/TVR dėl asmens duomenų, tvarkomų vykdančios policijos ir teisminį bendradarbiavimą baudžiamosiose bylose, apsaugos, ir pabrėžtina, kad jo tekstas iš esmės atkartoja šio ES teisės akto nuostatas. Atsižvelgiant į tai, kad Pamatinis sprendimas bus pakeistas platesnio pobūdžio apsaugą suteikiančios Direktyvos, šio teisės akto reikšmė neabejotinai mažėja. Šiame kontekste, ypač atsižvelgiant į vieną pagrindinių naujojo reguliavimo tikslų – užtikrinti efektyvias teisinės gynybos priemones nuo asmens duomenų pažeidimo¹⁴, ištis kyla pagrįsta abejonė, ar duomenų subjektui yra suteikta pakankamai realių galimybių dalyvauti jo asmens duomenų tvarkymo baudžiamajame procese metu bei efektyviai įgyvendinti ir ginti savo teises. Abejonė tik dar labiau sustiprinama 2010–2011 m. „Eurobarometro“ apklausos duomenimis, pagal kuriuos net 70 % Lietuvos respondentų net nėra girdėję apie nacionalinę instituciją, į kurią jie galėtų kreiptis dėl asmens duomenų apsaugos¹⁵. Taigi šiuo metu galiojantis teisinis reguliavimas gali būti vertinamas tik kaip bazinė prielaida užtikrinti efektyvią asmens duomenų baudžiamajame procese apsaugą, kuriai įgyvendinti praktiniu lygmeniu būtinos papildomos nuostatos, pagrindžiamos naujojo reguliavimo taisyklėmis.

II. ESMINIAI ASMENS DUOMENŲ APSAUGOS BAUDŽIAMAJAME PROCESSE PRINCIPAI IR JŲ PROBLEMATIKA

Iš Direktyvos tikslo, įvardyto 1-ajame straipsnyje, matyti, kad asmens duomenų apsaugos baudžiamajame procese teisinio reguliavimo centre atsideria proporcingumo

¹⁴ KOMISIJOS KOMUNIKATAS EUROPOS PARLAMENTUI, TARYBAI, EUROPOS EKONOMIKOS IR SOCIALINIŲ REIKALŲ KOMITETUI IR REGIONŲ KOMITETUI Privatumo apsauga glaudžiai susijusiame pasaulyje Europos duomenų apsaugos reglamentavimo pagrindai XXI amžiuje /* COM/2012/09 final */ Prieiga per internetą: <<http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52012D0009>>.

¹⁵ Apklausos „Požiūris į duomenų apsaugą ir elektroninę tapatybę Europos Sąjungoje“ rezultatai. Prieiga per internetą: <http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_fact_lt_en.pdf>.

principas. Viena vertus, Direktyva siekiama užtikrinti asmens duomenų apsaugą, kaip vieną pagrindinių teisių ir laisvių, kita vertus, sudaryti sąlygas perteklinių apribojimų nevaržomam teisėsaugos institucijų keitimuisi asmens duomenimis tiek nacionaliniuose, tiek tarptautiniuose baudžiamuosiuose procesuose. Tarptautinis bendradarbiavimas baudžiamosiose bylose pagrįstas abipusio pripažinimo principu¹⁶, 2005 m. Hagos programoje¹⁷ numatytas duomenų prieinamumo principas, reiškiantis, kad, pareigūnui vienoje ES valstybėje narėje prireikus informacijos iš kitos valstybės narės, jie turi būti suteikti pareigūnui, nors ir pagal nustatytas sąlygas, tačiau kuo mažiau apsunkinant informacijos gavimą. Duomenų prieinamumo principo įtvirtinimu siekta ES panaikinti vidines sienas duomenų apsikeitimui¹⁸, pagerinti, sudaryti kuo geresnes sąlygas teisėsaugos institucijoms tarpusavyje apsikeisti reikalingais duomenimis. Tai reiškia, kad asmens duomenų perdavimas tarp teisėsaugos institucijų turėtų vykti neatliekant išsamaus prašymo pateikti duomenis tikrinimo, tikrinant tik atitiktį formaliems kriterijams, tačiau neanalizuojant tyrimo, atliekamo prašymą pateikusioje valstybėje, esmės¹⁹. Toks požiūris atitinka bendrąją abipusio pripažinimo principu grindžiamą tarptautinio bendradarbiavimo ES sistemą ir teikia prioritetą abipusiam pasitikėjimui, kartu plėtodamas sklandaus keitimosi informacija ES sistemą²⁰. Taigi duomenų subjektui privalu suteikti pakankamą teisinę atsvarą, kuri užtikrintų, kad jo interesai, teisėsaugos institucijoms disponuojant, keičiantis jo asmens duomenimis, tiek nacionaliniuose, tiek tarptautiniuose baudžiamuosiuose procesuose bus pakankamai apsaugoti. Tokiomis teisinėmis garantijomis, baziniais principais, o kartu – ir probleminėmis sritimis, sąlygiškai išskirtini keturi aspektai:

- **duomenų tvarkymas tik konkrečiai apibrėžtu tikslu; duomenų subjekto informavimas ir įtraukimas į duomenų tvarkymo procesą;**

¹⁶ Reding V. Data Protection in the EU – Challenges Ahead // EUCRIM, Issue 2010/1, p. 25.

¹⁷ Hagos programa: laisvės, saugumo ir teisingumo stiprinimas Europos Sąjungoje. 2005/C 53/01.

¹⁸ Opinion of the European Data Protection Supervisor on the Proposal for a Council Framework Decision on the protection of personal data processed in the firework of police and judicial cooperation in criminal matters (COM (2005) 475 final) (2006/C 47/12). Prieiga per internetą: <<http://www.statewatch.org/news/2006/sep/eu-com-dp-edps-opinion.pdf>>.

¹⁹ Vermeulen G. et al. Availability of Law Enforcement Information in the European Union: Between Mutual Recognition and Equivalent Right of Access. IRCP, Maklu Publishers, 2005, p. 47.

²⁰ Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions. Justice, Freedom and Security in Europe Since 2005: an Evaluation of the Hague Programme and Action Plan. An Extended report on the evaluation of the Hague Programme. SEC(2009) 766 final. Prieiga per internetą: <<http://www.statewatch.org/news/2009/jun/eu-com-sec-766-2009-hague-extended-evaluation.pdf>>.

efektyvi pažeistų asmens duomenų subjekto teisių gynyba duomenų tvarkymo procese;

- **žalos atlyginimas.**

Nurodytų garantijų realizavimas ir užtikrinimas leistų konstatuoti, kad yra laikomasi Europos Sąjungos Teisingumo Teismo (toliau vadinama – ESTT) išskiriamų penkių pagrindinių duomenų apsaugos elementų: teisė gauti duomenis, teisė būti informuotam, teisė į žalos atlyginimą, duomenų tikslumas ir aktualumas, teisinė ir specialių institucijų priežiūra²¹, taigi – sudarytų prielaidas veiksmingai asmens duomenų baudžiamajame procese apsaugai.

- **Duomenų tvarkymas konkrečiai apibrėžtu tikslu**

Direktyvos 1 straipsnio 1 dalyje apibrėžtas bendrasis duomenų tvarkymo tikslas – fizinio asmens duomenys yra tvarkomi nusikalstamų veikų prevencijos, tyrimo, nustatymo ar traukimo baudžiamojon atsakomybėn už jas arba baudžiamųjų sankcijų vykdymo tikslu. Apibendrintai – baudžiamąjo proceso tikslais. Poreikis tvarkyti asmens duomenis šiuo tikslu neturėtų kelti didesnių diskusijų – tik turėdamos visą būtiną informaciją, teisėsaugos institucijos gali veiksmingai atlikti su konkrečiomis nusikalstamomis veikomis susijusias užduotis ir užtikrinti viešojo intereso apsaugą²², o tokios informacijos dalimi yra ir asmens duomenys. Tačiau svarbu pabrėžti, kad kiekvienas asmens teisių apribojimas, kad ir kokia forma jis būtų atliktas, visais atvejais turi turėti teisėtą, būtiną tikslą ir būti proporcingas. Tokia nuostata yra nuosekliai suformuota tiek Europos Žmogaus Teisių Teismo (toliau vadinama – EŽTT), tiek ESTT jurisprudencijoje. Ji galioja ir asmens duomenų apsaugos sričiai²³. Baudžiamajame procese asmens duomenys naudojami bendrajam, neabejotinai pagrįstam, teisėtam tikslui – nusikalstamų veikų tyrimui, baudžiamųjų bylų nagrinėjimui, nusikalstamų veikų prevencijai. Iš EŽTT jurisprudencijos akivaizdu, kad informacija baudžiamajame procese turi būti renkama, kaupiama ir saugoma tiksliais, specifiniams baudžiamąjo proceso tikslams, nustatant konkrečias, detalias jos naudojimo sąlygas, turi būti aiški kaupiamos informacijos apimtis. Byloje *Amann prieš Šveicariją*²⁴ prokuratūros kaupiama informacija neatitiko šios EŽTT kartelės

²¹ *Hijmans H., Scirocco A.* Shortcomings in EU Data Protection in the Third and the Second Pillars. Can the Lisbon Treaty be Expected to Help? // *Common Market Law Review*, 2009, Nr. 46, p. 1509.

²² *Kosti E., Coudert F., Dumortier J.* Data protection in the Third Pillar: in the Aftermath of the ECJ Decision on PNR Data and the Data Retention Directive // *International view of the law computers & technology*, 2007, p. 2.

²³ 2003 m. gegužės 20 d. Europos Sąjungos Teisingumo Teismo sprendimas sujungtose bylose C-465/00, C-38/01 ir C-139/01.

²⁴ 2000 m. vasario 16 d. Europos Žmogaus Teisių Teismo sprendimas byloje Nr. 27798/95, *Amann prieš Šveicariją*.

– apie asmenį suformuota duomenų kortelė pripažinta pažeidžiančia asmens duomenų apsaugą, kadangi Šveicarijos teisės aktuose nebuvo detalizuojama, kokiomis sąlygomis ši kortelė turi būti kuriama, kokių procedūrų turi būti laikomasi, kokia informacija gali būti saugoma ar komentarai, kokią informaciją draudžiama rinkti. Neįvykdžius šių reikalavimų, kaip ir šioje konkrečioje byloje, gali būti konstatuotas Konvencijos 8 straipsnio pažeidimas.

Asmens duomenų tvarkymo tikslo aspektu galima identifikuoti kelias problemas. Pirmoji – *asmens duomenų tvarkymas prevencijos tikslu*, kadangi šis tikslas – itin abstraktus ir platus. Direktyvos 4 straipsnis numato, kad duomenys turi būti renkami konkrečiai nustatytais, aiškiai apibrėžtais ir teisėtais tikslais ir tvarkomi su šiais tikslais suderintais būdais. Duomenų rinkimo tikslas kartu apibrėžia ir duomenų apimtį bei turinį: duomenys turi būti adekvatūs, susiję ir savo apimtimi neviršijantys tikslų, dėl kurių jie vėliau tvarkomi, tikslūs ir prirėkūs – nuolat atnaujinami. Kiekvienu atveju tvarkant asmens duomenis, jų negali būti surenkama daugiau, nei yra reikalinga nustatytiems tvarkymo tikslams²⁵. Nusikalstamų veikų prevencijai gali būti reikšmingi įvairūs duomenys, jų kaupimas ir naudojimas gali būti aktualus neribotą, ilgą laiką²⁶. Taigi asmens duomenų tvarkymas prevencijos tikslu iš esmės gali legitimuoti itin abstraktų, neapibrėžto pobūdžio, turinio bei trukmės disponavimą asmens duomenimis, kadangi nusikalstamų veikų prevencijos tikslas yra aktualus visada²⁷. Paminėtina ir tai, kad 7-asis Direktyvos straipsnis įpareigoja atskirti tuos duomenis, kurie yra pagrįsti faktais, nuo tų, kurie yra pagrįsti asmeniniu vertinimu. Pavojus su prevencijos tikslu išvelgtinas dėl to, kad duomenys gali būti pagrįsti asmeniniu vertinimu, susiformavusiu remiantis vidiniu įsitikinimu, o ne objektyviais faktais, ir tokiu būdu nustačius, jog konkretus asmuo gali kelti pavojų, daroma išvada, kad jų kaupimas prasmingas. Toks išankstinis neigiamas vertinimas ypač tikėtinas šių dienų kontekste dėl terorizmo keliamos grėsmės, kuri itin eskaluojama Europos Sąjungoje. Pažymėtina, kad didelis pavojus dėl duomenų tvarkymo teisėtumo tikslo nustatymo aspektu kyla dėl Direktyvos 10-ajame straipsnyje numatytų ypatingų duomenų tvarkymo. Tokiais duomenimis pripažįstami asmens duomenys, kurie atskleidžia rasinę arba tautinę kilmę, politines, religines pažiūras ar tikėjimą, priklausymą profesinėms sąjungoms, taip pat genetinius duomenis arba duomenis apie sveikatą ar lytinį gy-

²⁵ *Meškauskaitė L.* Teisė į privatų gyvenimą, p. 21–22.

²⁶ *Hert P., Papakonstantinou V.* The Police and Criminal Justice Data Protection Directive: Comment and Analysis // The IT Law Community SCL Forum, 2012, p. 1.

²⁷ *Andoulsi I.* Personal Data Protection and the First Implementation Semester of the Lisbon Treaty: Achievements and Prospects // New journal of European Criminal Law, 2010, vol. 1, Nr. 3, p. 368.

venimą, pavyzdžiui, DNR informaciją²⁸. Šių duomenų tvarkymui dėl ypač jautraus jų pobūdžio turi būti nustatytas papildomas, didesnę apsaugą užtikrinantis teisinis reguliavimas. Šios kategorijos duomenų tvarkymas prevencijos tikslu lengvai gali peraugti į teisės į asmens duomenų apsaugą pažeidimą.

Antroji dilema – *duomenų tvarkymo tikslo pasikeitimas*. Surinkus ir tvarkingus asmens duomenis, pavyzdžiui, Europos arešto orderio išdavimo tikslu, šie duomenys (jų dalis) lieka Šengeno informacinėje sistemoje ir gali būti toliau naudojami jau nebe ikiteisminio tyrimo tikslu, tačiau, pavyzdžiui, prevencijos tikslu. Su analogiška situacija susiduriama ir su sukaupta informacija apie ankstesnius asmens teistumus²⁹, kuri panaudojama ne tik pradiniu, tačiau ir prevencijos bei naujų ikiteisminių tyrimų tikslais. Tokiu atveju keltinas klausimas, ar tolesnis duomenų naudojimas atitinka pradinį tikslą ir gali būti vertinamas kaip jo tęsa³⁰. Paminėtini ir tie atvejai, kai baudžiamajame procese surinkta informacija galimai naudotina, pavyzdžiui, administraciniuose procesuose³¹. Manytina, kad iš esmės pakitęs duomenų tvarkymo tikslas negali būti vertinamas kaip teisėtumo reikalavimus atitinkantis duomenų tvarkymas, jei prieš pakeičiant duomenų tvarkymo tikslą nebuvo atlikta papildoma patikra, kaip konkretūs asmens duomenys bus naudojami naujam tikslui ir kodėl būtent šių konkrečių duomenų tvarkymas yra būtinas.

Problema itin jautri kriminalinės žvalgybos metu surinktų duomenų panaudojimo kontekste. 2016 m. kovo 22 d. Lietuvos Respublikos Seimo nutarimu Nr. XII-2263 patvirtintoje Lietuvos Respublikos Seimo Teisės ir teisėtvarkos komiteto atlikto parlamentinio tyrimo dėl kriminalinės žvalgybos metu gautos informacijos panaudojimo ir saugojimo išvadoje³² konstatuota, kad daugiausia neaiškumų kyla dėl kriminalinės žvalgybos priemonėmis surinktos kitos nepanaudotos informacijos, kuri ne naudojama kriminalinės žvalgybos uždaviniams įgyvendinti, o yra saugoma nusikalstamų veikų prevencijos tikslais. Išvadoje pabrėžtas aiškesnio teisinio reguliavimo poreikis,

²⁸ *Munoz H. S., Fiodorova A.* DNA and Law Enforcement in the European Union: Tools and Human Rights Protection // *Utrecht Law Review*, vol. 10, issue 1, 2014, p. 157.

²⁹ *Andoulsi I.* Personal Data Protection and the First Implementation Semester of the Lisbon Treaty: Achievements and Prospects // *New journal of European Criminal Law*, 2010, vol. 1, Nr. 3, p. 367.

³⁰ *Kosta E., Coudert F., Dumortier J.* Data Protection in the Third Pillar: In the Aftermath of the ECJ Decision on PNR Data and the Data Retention Directive // *International Review of Law Computers & Technology*, 2007, p. 8.

³¹ *De Busser E.* EU data protection in transatlantic cooperation in criminal matters. Will the EU be serving its citizens an American meal? // *Utrecht Law Review*, 2010, vol. 6, Nr. 1, p. 95.

³² 2016 m. kovo 22 d. Lietuvos Respublikos Seimo nutarimu Nr. XII-2263 patvirtinta LRS Teisės ir teisėtvarkos komiteto atlikto parlamentinio tyrimo dėl kriminalinės žvalgybos metu gautos informacijos panaudojimo ir saugojimo išvada // *TAR*, 2016-03-25, Nr. 6329.

akcentuota, kad surinkta informacija galėtų būti naudojama tik sunkių ar labai sunkių nusikalstamų veikų (pavyzdžiui, terorizmo, prekybos žmonėmis, neteisėto disponavimo ginklais, narkotinėmis ir psichotropinėmis medžiagomis) prevencijos tikslais. Ši situacija itin pavojinga asmens teisių apsaugos požiūriu, kai yra naudojamas profiliavimas, t. y. asmens pavojingumo vertinimas pagal susistemintą asmens charakteristiką, parengtą naudojant įvairių šaltinių, duomenų bazių, informaciją³³, kuris pastaruoju metu ES naudojamas vis dažniau, siekiant kovoti su terorizmu ir kitais sunkiais nusikaltimais.

Šiuo aspektu svarbu paminėti ir asmens duomenų, gautų ne iš teisėsaugos institucijų, tačiau iš kitų, privačių ar viešųjų, subjektų, tvarkymą. Teisėsaugos institucijos gali rinkti informaciją iš komercinių bankų, gydymo įstaigų, interneto paslaugų teikėjų, mobiliojo ryšio operatorių, kuri buvo gauta komerciniais tikslais³⁴, taip pat – Valstybinės mokesčių inspekcijos, Socialinio draudimo fondo ir t. t. Komercinių skrydžių paslaugų teikėjų surinkta informacija (vadinamoji PNR informacija – *Passenger Name Record*) Europos Sąjungos Teisingumo Teismo pripažinta susijusia su saugumu³⁵, taigi – galimai teisėtai rinktina. Analogiškas pavyzdys – informacija, surinkta vizų informacinėje sistemoje VIS (*Visa Information System*). Problema kyla dėl konfrontacijos tarp įstaigų pareigos ir siekio apsaugoti kliento interesus bei teisėsaugos institucijų autoriteto. Neginčytina, kad neretais atvejais teisėsaugos institucijų kreipimasis (BPK 97 straipsnio pagrindu, t. y. nereikalaujant teismo sankcijos) į tokias įstaigas kaip komerciniai bankai, medicinos paslaugų teikėjai, privačios įmonės, kuriose dirba asmenys, kurių asmens duomenys domina teisėsaugą, sukelia nemenką psichologinį spaudimą šiems subjektams. Pastarieji kartais net nekvestionuodami, nesidomėdami apie duomenų rinkimo tikslą ir priežastis, suteikia visą turimą ir teisėsaugos institucijų prašomą pateikti informaciją apie jų klientus, darbuotojus. Apie tokį asmens duomenų rinkimą nėra pranešama jų savininkui. Pagrindinė problema šiuo atveju kyla dėl to, kad asmens duomenų subjektas informaciją pastariesiems subjektams pateikia, tikėdamasis, kad jo asmens duomenys bus naudojami specifiniais tikslais, nesusijusiais su baudžiamuoju procesu.

Taigi matyti, kad ta pati informacija gali nukeliauti labai ilgą kelią – būti panaudota tiek komerciniais, reklamos tikslais, kreditingumui vertinti ir t. t., tiek ir kovai su terorizmu ar kitais sunkiais nusikaltimais. Dėl šių priežasčių ypač svarbu kiekvienu

³³ *Hijmans H., Scirocco A.* Shortcomings in EU Data Protection in the Third and the Second Pillars. Can the Lisbon Treaty be Expected to Help? // *Common Market Law Review*, 2009, Nr. 46, p. 1491.

³⁴ *Hert P., Papakonstantinou V.* The Police and Criminal Justice Data Protection Directive: Comment and Analysis // *The IT Law Community SCL Forum*, 2012, p. 4.

³⁵ 2006 m. gegužės 30 d. Europos Sąjungos Teisingumo Teismo sprendimas sujungtose bylose Nr. C-317/04 ir C-318/04.

atveju įvertinti informacijos pobūdį ir jos rinkimo atitiktį konkrečiam tikslui. Tikslų transformacija kiekvienu atveju turi būti pagrindžiama konkrečiais objektyviais duomenimis ir nekelti abejonių dėl duomenų tvarkymo teisėtumo. Situacijos, kai asmens duomenys tvarkomi vis kitu tikslu, neatlikus papildomo naujojo tikslo vertinimo, ypač – neinformavus apie tai duomenų subjekto, vertintinos kaip neatitinkančios teisėto asmens duomenų tvarkymo reikalavimų.

- **Duomenų subjekto informavimas ir įtraukimas į duomenų tvarkymo procesą**

Vienas pagrindinių Direktyvos principų – skaidrumas, reiškiantis duomenų valdymo proceso atvirumą ir prieinamumą duomenų savininkui, duomenų apsaugos institucijoms ir tretiesiems asmenims, turintiems interesą kreiptis dėl duomenų valdymo ir efektyvumo³⁶. 13-asis Direktyvos straipsnis nustato, kokią minimalią informaciją turi gauti duomenų subjektas: duomenų valdytojo ir duomenų apsaugos pareigūno vardą, pavardę ir duomenis ryšiams; duomenų tvarkymo tikslą; duomenų saugojimo laikotarpį; informaciją apie teisę prašyti, kad duomenų valdytojas leistų susipažinti su duomenų subjekto asmens duomenimis, juos ištaisyti, ištrinti arba apriboti jų tvarkymą; apie teisę pateikti skundą priežiūros institucijai; apie asmens duomenų gavėjus; bet kokią papildomą informaciją, jeigu jos reikia užtikrinti sąžiningą su duomenų subjektu susijusių duomenų tvarkymą; apie pareigą arba galimybę savanoriškai teikti duomenis ir jų nepateikimo pasekmes.

14-asis Direktyvos straipsnis nustato detalią pareigą duomenų subjektui pateikti patvirtinimą dėl to, ar jo asmens duomenys yra tvarkomi ar ne. Jei jie tvarkomi, turi būti pateikta informacija apie: duomenų tvarkymo tikslus; atitinkamų asmens duomenų kategorijas; duomenų gavėjus, kuriems asmens duomenys buvo atskleisti, arba tokių duomenų gavėjų kategorijas, visų pirma duomenų gavėjus trečiosiose šalyse; asmens duomenų saugojimo laikotarpį; teisę reikalauti, kad duomenų valdytojas ištaisytų ar ištrintų duomenų subjekto asmens duomenis arba apribotų jų tvarkymą; teisę pateikti skundą priežiūros institucijai ir priežiūros institucijos duomenis ryšiams; tai, kokie asmens duomenys yra tvarkomi, ir visą turimą informaciją apie jų šaltinius; teisę gauti duomenų kopiją.

Vertinant Direktyvoje apibrėžtas duomenų subjekto teises, pastebėtina, kad šių teisių sąrašas yra išties platus. Direktyvos akcentas neabejotinai yra duomenų subjekto teisė visų pirma *žinoti apie tai, kad jo asmens duomenys yra tvarkomi, ir būti kuo visapusiškiau įtrauktam į duomenų tvarkymo procesą*. Šią teisę galima vertinti kaip sudėtinę teisės į informaciją baudžiamajame procese dalį, kuriai Euro-

³⁶ *Hert P., Papakonstantinou V.* The Police and Criminal Justice Data Protection Directive: Comment and Analysis // The IT Law Community SCL Forum, 2012, p. 4.

pos Sąjungos baudžiamojoje justicijoje pastaruoju metu skiriama daug dėmesio³⁷. Teisė į informaciją apima įtariamųjų ir kaltinamųjų teisę į informaciją apie jų teises baudžiamajame procese (2012 m. gegužės 22 d. Direktyvos 2012/13/ES dėl teisės į informaciją baudžiamajame procese 1 straipsnis), į kurių apimtį, manytina, turi patekti teisė dalyvauti asmens duomenų tvarkymo procese. Direktyvos dėl teisės į informaciją baudžiamajame procese 7-asis straipsnis garantuoja teisę susipažinti su bylos medžiaga, kurios neatsiejama dalis yra asmens duomenys, taigi duomenų subjekto teisė būti jo asmens duomenų tvarkymo proceso dalimi kildintina ne tik iš teisės į privatumą apsaugos, tačiau ir iš teisės susipažinti su baudžiamosios bylos medžiaga. Taip pat nurodytina, kad ESTT praktikoje esama atvejų, kai teismas naudojo asmens duomenų apsaugos elementus tam, kad būtų užtikrintos kitos pagrindinės teisės, tokios kaip teisė į gynybą bei teisminė apsauga³⁸. Taigi duomenų subjekto teisė būti informuotam ir dalyvauti asmens duomenų tvarkymo procese yra svarbi ne tik pati savaime, tačiau ir dėl to, kad ji yra itin glaudžiai susijusi su kitų pagrindinių teisių baudžiamajame procese apsauga. Šiuo aspektu prisimintinas BPK 45 straipsnis, kuriame nustatyta teisėjo, prokuroro ir ikiteisminio tyrimo pareigūno pareiga išaiškinti proceso dalyviams jų procesines teises ir užtikrinti galimybę jomis pasinaudoti. Taigi kartu su bendrąja teise į informaciją turi būti garantuojama, kad subjektas, kurio asmens duomenimis disponuojama, bus adekvačiai informuotas apie jo asmens duomenų tvarkymą.

Greta prieigos prie asmens duomenų, esminėmis duomenų subjekto teisėmis asmens duomenų tvarkymo procese išskirtinos teisės duomenis ištaisyti, ištrinti ar apriboti naudojimąsi³⁹. Šios teisės užtikrina duomenų aktualumą ir atitiktį tikrovei, taigi jų įgyvendinimas garantuoja abipusę – duomenų subjekto ir duomenų tvarkytojo – naudą, kadangi duomenų kokybė yra svarbi ne tik užtikrinant asmens teisės į privatumą apsaugą, tačiau – esminė veiksmingam jų panaudojimui teisėsaugos institucijų tikslais. Itin svarbus aspektas – duomenų ištrynimo užtikrinimas. Probleminis momentas šiuo atveju yra tai, kad sprendimas dėl duomenų reikalingumo ir jų sunaikinimo, pašalinimo iš bylos medžiagos yra išimtinai pareigūno diskrecija. Joks išorinis subjektas tokių veiksmų nekontroliuoja. Būtent dėl šios priežasties yra svarbu kiek įmanoma labiau įtraukti duomenų savininką į duomenų valdymo procesą, kadangi jis gali padėti nustatyti, ar informacija vis dar atitinka tikrovę, ar ji nėra pasikeitusi, ar realiai dar gali būti reikšminga tyrimui. Kuo senesnė informacija

³⁷ Ši tendencija matyti iš ES teisėkūros – 2012 m. gegužės 22 d. priimta Europos Parlamento ir Tarybos direktyva 2012/13/ES dėl teisės į informaciją baudžiamajame procese // OJ L 142, 1.6.2012, p. 1–10.

³⁸ *Hijmans H., Scirocco A.* Shortcomings in EU Data Protection in the Third and the Second Pillars. Can the Lisbon Treaty be Expected to Help? // *Common Market Law Review*, 2009, Nr. 46, p. 1509.

³⁹ Ten pat, p. 1488.

yra sukaupta, tuo didesnė tikimybė, kad jos naudojimas neatitiks teisėtų duomenų tvarkymo tikslų. Senos informacijos kaupimo ir jos atitikties tikrovei problema ne kartą identifiukuota EŽTT jurisprudencijoje. EŽTT byloje *Rotaru prieš Rumuniją*⁴⁰ Teismas pripažino, jog daugiau nei prieš 50 metų užfiksuota ir valstybės institucijų kaupta informacija pažeidžia Konvencijos 8-ąjį straipsnį, kadangi dalis jos buvo pripažinta neteisinga ir dėl to galimai pažeidžiančia pareiškėjo reputaciją. Taigi duomenų subjekto prieigos prie duomenų ribojimas ne tik gali tiesiogiai kenkti baudžiamojo proceso kokybei, tačiau sudaryti prielaidas pagrindinių žmogaus teisių pažeidimui.

Direktyvos 15 straipsnio 1 dalyje taip pat pateiktas išimčių sąrašas, kada informacijos teikimas duomenų subjektui gali būti atidėtas ar apribotas. Šio sąrašo apimtis, nors ir didelė, tačiau gana neapibrėžta: netrukdyti atlikti oficialius arba teisinius nagrinėjimus, tyrimus ar procedūras; nepakenkti nusikalstamų veikų prevencijai, nustatymui, tyrimui ir traukimui baudžiamajon atsakomybėn už jas arba baudžiamųjų sankcijų vykdymui; užtikrinti visuomenės saugumą; užtikrinti nacionalinį saugumą; užtikrinti kitų asmenų teisių ir laisvių apsaugą. Manytina, kad skaidrumo principui teiktinas prioritetas, ir nustatyta prieigos prie asmens duomenų ribojimo pagrindų gausa turi būti vertinama itin preciziškai, ribojimus taikant tik tais atvejais, kai egzistuoja ne prielaidomis, o objektyviais duomenimis pagrįsta pozicija, kad atskleidus informaciją duomenų subjektui kils nurodytos neigiamos pasekmės ir grėsmė. Straipsnyje numatytos išimtys, autorės požiūriu, aiškintinos siaurai, jas taikant kaip išimtį, o ne taisyklę, kadangi priešingu atveju kyla reali pagrindinių baudžiamojo proceso principų ir pagrindinių asmens teisių pažeidimo grėsmė. Pavyzdžiui, proporcingumo principo neatitiktų ilgalaikis duomenų subjekto neinformavimas, pagrįstas vien tuo, kad jis, turėdamas informaciją, galėtų padaryti išvadas apie tam tikrą teisėsaugos institucijų veikimo būdą ar teisėsaugos institucijų tikslus. Tokia išvada kyla iš EŽTT jurisprudencijos, kurioje nurodoma, kad informacijos kaupimas ir naudojimas teisėsaugos institucijose reiškia, kad yra braunamasi į asmens privataus gyvenimo sritį⁴¹, ir pabrėžiama, kad kiekvienas asmens teisių ribojimas turi būti netęsimas neproporcingai ilgą laiką⁴² bei griežtai atitikti teisės aktų nustatytus reikalavimus, būti pateisinamas konkrečiu tikslu⁴³. Itin nerekomenduotina

⁴⁰ 2000 m. gegužės 4 d. Europos Žmogaus Teisių Teismo sprendimas byloje Nr. 28341/95, *Rotaru prieš Rumuniją*.

⁴¹ 1987 m. kovo 26 d. Europos Žmogaus Teisių Teismo sprendimas byloje Nr. 48, serija A, Nr. 116, *Leander prieš Švediją*.

⁴² 2006 m. gruodžio 7 d. Europos Žmogaus Teisių Teismo sprendimas byloje Nr. 29514/05, *Van der Velden prieš Nyderlandus*; 2013 m. balandžio 18 d. Europos Žmogaus Teisių Teismo sprendimas byloje Nr. 19522/09, *M. K. prieš Prancūziją*.

⁴³ 2010 m. rugsėjo 2 d. Europos Žmogaus Teisių Teismo sprendimas byloje Nr. 5623/05, *Uzun prieš Vokietiją*.

duomenų subjekto atžvilgiu taikyti neribotos apimties ir trukmės priegios prie duomenų ribojimą asmens duomenis tvarkant prevenciniu tikslu. Tokia praktika neatitiktų nei teisinio reguliavimo nuostatų, nei nuoseklios EŽTT jurisprudencijos.

Pabrėžtina, kad ribojimo atvejais turi būti nustatyti efektyvūs saugikliai, kaip užtikrinama asmens duomenų apsauga, kai duomenų subjektas nėra įtrauktas į duomenų tvarkymo procesą. Vienas iš tokių saugiklių visų pirma galėtų būti automatinis duomenų sunaikinimas, kuris šiuo metu yra taikomas kai kuriose automatinėse duomenų tvarkymo sistemose, pavyzdžiui, *Visa Information System*, kai sukaupti duomenys yra automatiškai sunaikinami po penkerių metų⁴⁴. Tokiu būdu užtikrinama, kad duomenys nebus naudojami nepagrįstai ilgą laiką, nepersvarsčius jų naudojimo tikslingumo. Tačiau šis būdas, manytina, sėkmingai panaudotinas tik dalyje atvejų, dažniausiai, kai tvarkomi ne ypač jautrūs asmens duomenys. Pažymėtina, kad duomenų kokybė bei asmens duomenų subjekto teisių apsauga gali būti užtikrinama naudojant tam tikrą kompromisinį variantą: duomenų subjektui turėtų būti sudaroma galimybė pateikti, jo požiūriu, aktualius asmens duomenis ir prašyti jais pakeisti teisėsaugos institucijų turimus duomenis, net ir tiksliai nežinant pastarųjų turinio ir apimties. Šią teisę įtariamasis ar kaltinamasis gali realizuoti, naudodamasis BPK 21 ir 22 straipsniuose įtvirtintomis bendrosiomis teisėmis pateikti reikšmingus dokumentus ir daiktus bei pateikti prašymus. Šie prašymai vertintini pagal bendrąsias baudžiamojo proceso taisykles, tačiau akcentuojant specifinį klausimo pobūdį.

Atkreiptinas dėmesys į Direktyvos nuostatą, kad, atsisakius leisti susipažinti su duomenimis arba apribojus tokią teisę, turi būti nurodoma atsisakymo priežastis bei išaiškintos galimybės pateikti skundą priežiūros institucijai ir imtis teisių gynimo teisminių priemonių. Apskundimo galimybė turėtų būti suteikiama ir tais atvejais, kai yra netenkinamas subjekto prašymas papildyti ar pakeisti asmens duomenis. Atsisakymo priežastis visgi neturėtų būti nurodoma, jei informacijos pateikimas pakenktų tikslui, kurio siekiama nustatyti ribojimu. Tačiau tokiu atveju turi būti pateikiami motyvai, kodėl nenurodomos faktinės ar teisinės priežastys, pagrindžiančios sprendimą. Vis dėlto nors pareiga motyvuoti atsisakymą leisti susipažinti su duomenimis yra ypač svarbi procesinių asmens teisių garantija, tačiau visais atvejais prioritetas turi būti teikiamas informacijos teikimui, o ne priegios prie jos ribojimui.

- **Efektyvi pažeistų asmens duomenų subjekto teisių gynyba duomenų tvarkymo procese**

Siekiant įgyvendinti Direktyvos tikslus ir užtikrinti realią asmens duomenų subjekto teisių apsaugą, turi būti užtikrinama efektyvi galimai pažeistų teisių gynyba.

⁴⁴ 2008 m. liepos 9 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 767/2008 dėl Vizų informacinės sistemos (VIS) ir apskaitimo duomenimis apie trumpalaikes vizas tarp valstybių narių (VIS reglamentas) // Oficialusis leidinys, L 218, 13/8/2008, p. 60–81.

Laisvas asmens duomenų judėjimas nacionalinėse teisėsaugos institucijose ir tarp valstybių narių teisėsaugos institucijų neabejotinai yra skirtas užtikrinti efektyvų teisėsaugos darbą, tačiau kartu būtina nesumažinti duomenų subjekto teisių neteisingu ir neproporcingu būdu⁴⁵. Reali gynyba ypač svarbi tais atvejais, kai teisėsaugos institucijos tvarko tokius asmens duomenis, kurie tik nuo Direktyvos priėmimo visais atvejais pripažįstami ypatingais, jautriais asmens duomenimis ir faktiškai atskleidžia labai daug informacijos apie duomenų subjektą, pavyzdžiui, DNR, pirštų atspaudai ir biometriniai duomenys⁴⁶. Direktyvoje numatyta konkreti sistema, kurios laikantis šis tikslas gali būti pasiektas. Sistemą galima sąlygiškai suskirstyti į kelias dalis: i) nepriklausomos priežiūros institucijos ir duomenų apsaugos pareigūno įtraukimas į asmens duomenų tvarkymą baudžiamajame procese, ii) galimybė duomenų subjektui pateikti skundą, susijusį su asmens duomenų tvarkymu, iii) žalos, padarytos neteisėtai tvarkant asmens duomenis, atlyginimas.

Nepriklausomos priežiūros institucijos dalyvavimas asmens duomenų tvarkymo procese nėra naujas reiškinys ES. ESTT jurisprudencijoje nuosekliai aiškinta, kad „nepriklausomų priežiūros institucijų įsteigimas valstybėse narėse yra esminis asmens apsaugos tvarkant asmens duomenis elementas. <...> Nacionalinių priežiūros institucijų nepriklausomumo garantija siekiama užtikrinti veiksmingą ir patikimą nuostatų, susijusių su fizinių asmens apsauga tvarkant asmens duomenis, laikymosi kontrolę ir ji turi būti aiškinama atsižvelgiant į šį tikslą. Ši garantija buvo nustatyta, kad būtų sustiprinta su šių institucijų sprendimais susijusių asmens ir organizacijų apsauga. <...> Siekdamas garantuoti šių apsaugą nacionalinės priežiūros institucijos turi, be kita ko, užtikrinti teisingą, pirma, pagrindinės teisės į privatų gyvenimą ir, antra, laisvo asmens duomenų judėjimo interesų pusiausvyrą“⁴⁷. Nors pagal ES teisės aktus ši institucija yra būtina, ji turi būti veiksminga ir turėti realias priemones reaguoti į nuo įstatymų reikalavimų nukrypstantį teisėsaugos institucijų elgesį, efektyviai ginti besikreipiančiųjų interesus, šio subjekto įtraukimas į baudžiamąjį procesą yra sudėtingas dėl baudžiamojo proceso specifikos, dažnai – nenoro įtraukti pašalinius subjektus į teisėsaugos institucijų vykdomą veiklą. Nepaisant to, Direktyvos 41 straipsnyje nustatyta, kad valstybėse narėse turi veikti atskira valdžios instituci-

⁴⁵ Kosti E., Coudert F., Dumortier J. Data protection in the Third Pillar: in the Aftermath of the ECJ Decision on PNR Data and the Data Retention Directive // International view of the law computers & technology, 2007, p. 6.

⁴⁶ Ten pat, p. 8.

⁴⁷ 2012 m. spalio 16 d. Europos Sąjungos Teisingumo Teismo sprendimas byloje *Komisija prieš Austriją*, Nr. C-614/10; 2014 m. balandžio 8 d. Europos Sąjungos Teisingumo Teismo sprendimas byloje *Komisija prieš Vengriją*, Nr. C-288/12; 2009 m. lapkričio 12 d. generalinio advokato Jano Mazako išvada ESTT byloje *Komisija prieš Vokietijos Federacinę Respubliką*, Nr. C-518/07.

ja, kuri stebėtų, kaip taikomos pagal Direktyvą priimtos nuostatos, ir padėtų jas nuosekliai taikyti visoje Sąjungoje, apsaugant fizinių asmenų pagrindines teises ir laisves tvarkant jų duomenis bei palengvinant laisvą asmens duomenų judėjimą Sąjungoje. Būtent tokios institucijos nepriklausomumas nuo bet kokių išorės veiksnių garantuoja objektyvią duomenų subjekto apsaugą⁴⁸. Direktyvos preambulės 63 punkte nurodoma, kad visiškai nepriklausomai savo funkcijas vykdančių priežiūros institucijų įsteigimas valstybėse narėse yra esminė fizinių asmenų apsaugos tvarkant jų asmens duomenis dalis.

Ši priežiūros institucija gali būti tiek specializuota baudžiamąjo proceso srityje, tiek bendroji, konkrečioje valstybėje atsakinga už visus asmens duomenų apsaugos klausimus. Nacionaliniame kontekste tokia institucija yra Valstybinė duomenų apsaugos inspekcija (toliau vadinama – Inspekcija), kuri atlieka asmens duomenų apsaugos priežiūros funkcijas visose srityse. Pastebėtina, kad Inspekcijos reikšmė su baudžiamuoju procesu susijusiais klausimais yra minimali. Praktikoje į Inspekciją nėra kreipiamasi dėl asmens duomenų tvarkymo nei nacionaliniame baudžiamajame procese, nei vykstant tarptautiniam bendradarbiavimui baudžiamosiose bylose. Nacionalinių teismų praktikoje nėra atvejų, kuriose būtų nagrinėti klausimai, susiję su Inspekcijos teisių ir pareigų įgyvendinimu minėtoje srityje. Taigi nacionaliniame kontekste Institucijos vaidmuo baudžiamąjo proceso srityje yra formalus ir neefektyvus. Direktyva neabejotinai akcentuoja nepriklausomos priežiūros institucijos vaidmenį, taigi tokia nacionalinė praktika laikytina sisteminiu trūkumu, kuris turi būti ištaisytas, siekiant įgyvendinti Direktyvos nuostatas nacionaliniame reguliavime. Direktyvos 17 straipsnis įtvirtina itin svarbų nepriklausomos priežiūros institucijos vaidmens aspektą: apribojus duomenų subjekto teisę tiesiogiai susipažinti su duomenimis, jis privalo būti informuotas apie galimybę netiesiogiai su jais susipažinti per priežiūros instituciją, kuri ta teise turėtų naudotis duomenų subjekto vardu ir privalo jį informuoti apie patikrinimų rezultatus. Taigi nepriklausoma institucija tampa vieninteliu nešališku subjektu, turinčiu teisę įvertinti surinktus asmens duomenis bei jų apsaugą, kai asmens duomenų subjektas neturi prieigos prie tvarkomų jo asmens duomenų. Svarbus nepriklausomos institucijos vaidmuo numatytas ir Direktyvos 28 straipsnyje, pagal kurį teisėsaugos institucijos turi konsultuotis su priežiūros institucija prieš tvarkydamos asmens duomenis, kurie bus įtraukti į susistemintą rinkinį, jei turi būti tvarkomi ypatingų kategorijų duomenys arba dėl naujų technologijų ar mechanizmų naudojimo ar naujų procedūrų taikymo kyla konkreți grėsmė duomenų subjektų pagrindinėms teisėms ir laisvėms. Taigi nepriklausoma institucija

⁴⁸ *Kosti E., Coudert F., Dumortier J.* Data protection in the Third Pillar: in the Aftermath of the ECJ Decision on PNR Data and the Data Retention Directive // *International view of the law computers & technology*, 2007, p. 9.

Direktyvos požiūriu turėtų tapti svarbiu saugikliu, naudojant profiliavimo metodą.

Be to, Direktyva nustato, kad į asmens duomenų tvarkymo procesą turi būti įtraukta ne tik nepriklausoma priežiūros institucija, bet ir duomenų apsaugos pareigūnas. Šio pareigūno statusas Direktyvoje išsamiai nedetalizuojamas. Jo funkcijas galima vertinti kaip pagalbines, jų esmė – teikti teisėsaugos institucijoms informaciją apie jų teises ir pareigas, susijusias su asmens duomenų tvarkymu, stebėti, kaip yra laikomasi Direktyvos reikalavimų, ir tarpininkauti tarp teisėsaugos institucijos bei nepriklausomos priežiūros institucijos. Tikėtina, kad praktikoje tokio pareigūno funkcijas atliks teisėsaugos institucijos pareigūnas, tvarkantis konkrečius asmens duomenis, t. y. bus praplėstos pareigūno darbo funkcijos, o ne sukurta nauja pareigybė, kuri atliktų nurodytus veiksmus.

Pabrėžtina, kad nepriklausomos priežiūros institucijos dalyvavimas gali būti priemonė, kuri padėtų užtikrinti tiek asmens duomenų saugumą, tiek teisėsaugos atliekamų užduočių efektyvumą tais atvejais, kai duomenų subjekto informavimas apie su jo asmens duomenų tvarkymu susijusias aplinkybes gali pakenkti baudžiamajam procesui ir šio fakto atskleidimas yra stipriai ribojamas. Iliustratyvus tokio požiūrio pavyzdys – Direktyvos 30 straipsnis, kuriame įtvirtinta duomenų subjekto teisė būti informuotam apie tai, kad tvarkant jo asmens duomenis užfiksuotas duomenų saugumo pažeidimas. Ši teisė gali būti apribota papildomu ribojimo pagrindu – esant nepriklausomos priežiūros institucijos patvirtinimui, kad įdiegtos tinkamos apsaugos priemonės.

Atkreiptinas dėmesys ir į tai, kad Direktyvos 45 straipsnio 2 dalyje nustatyta, kad nepriklausoma priežiūros institucija neturi teisės kontroliuoti asmens duomenų tvarkymo, kurį atlieka teismai, vykdydami teisingumą, t. y. teismo nagrinėjimo metu asmens duomenų apsaugą turi užtikrinti pats teismas. Kita vertus, Direktyva tyli dėl to, ar į asmens duomenų tvarkymo teisme procesą gali įsitraukti duomenų apsaugos pareigūnas. Tokia situacija vertintina dviprasmiškai, viena vertus, tokiu būdu siekiama apsaugoti teismų nepriklausomumą nuo bet kokios pašalinės įtakos, kita vertus, toks tikslas siekiamas asmens duomenų subjekto teisių apsaugos sąskaita. Šiuo atveju, siekiant užtikrinti efektyvią duomenų subjekto teisių gynybą, teisme turi būti ypač atidžiai vertinami argumentai, išsakomi dėl galimo asmens duomenų tvarkymo pažeidimo, kadangi teismas tampa vienintele institucija, vertinančia galimą asmens duomenų pažeidimą.

Nepriklausomos priežiūros institucijos dalyvavimas asmens duomenų tvarkymo procese yra itin reikšmingas realizuojant *duomenų subjekto teisę pateikti skundą* dėl galimo pažeidimo, padaryto tvarkant asmens duomenis. Šiuo atveju kaip rimta problema vertintina tai, kad asmuo, kurio asmens duomenys tvarkyti tiek nacionalinių teisėsaugos institucijų, tiek perduoti užsienio valstybių teisėsaugos institucijoms,

dažniausiai apskritai nežino apie jo asmens duomenų tvarkymo faktą⁴⁹, nežino, kokia apimtimi, kokio turinio duomenys yra perduoti, kokie veiksmai bus su jais atliekami ir pan. Be to, net ir tais atvejais, kai asmeniui visgi yra žinoma apie jo asmens duomenų tvarkymą, nėra aiškaus reguliavimo, kam turi būti pateikiamas skundas dėl galimų pažeidimų, tvarkant asmens duomenis. Taigi dar kartą pabrėžtina būtinybė visų pirma užtikrinti, kad asmuo būtų tinkamai informuotas apie jo asmens duomenų tvarkymą. Turėdamas šią informaciją ir nustatęs pagrindą teikti skundą dėl galimo neteisėto jo asmens duomenų tvarkymo, duomenų subjektas faktiškai turi du variantus, kam gali būti pateikiamas skundas: teisėsaugos institucijai arba nepriklausomai priežiūros institucijai. Tokia pasirinkimo galimybė matyti ir iš Direktyvos 52-ojo bei 54-ojo straipsnių, kuriais duomenų subjektui paliekama alternatyva skųsti jo asmens duomenų tvarkymą, neatitinkantį Direktyvos nuostatų tiek nepriklausomai priežiūros institucijai, tiek teisminės gynybos keliu. Manytina, kad sprendimas priklauso nuo to, kaip turėtų būti traktuojamas skundo pobūdis. Taikant teisminės gynybos priemones, skundo dalykas bus vertinamas kaip proceso veiksmo apskundimas, taikant BPK 62–65 straipsnių tvarką, t. y. tikrinama, ar proceso veiksmas, tvarkant asmens duomenis, buvo atliktas pagal teisės aktų reikalaujamas taisykles. Vadinasi, tikėtinas gilinimasis ne tiek į informacijos pobūdį, turinį, kiek į jos tvarkymo teisėtumo faktą. O tai savo ruožtu lemia galimai gana siaurą situacijos esmės analizę ir formalų jos vertinimą, atsietą nuo asmens duomenų apsaugos esmės. Tuo atveju, jei asmens duomenų tvarkymo problematikos vertinimas būtų atliekamas nepriklausomos institucijos, manytina, kad daugiau dėmesio būtų skiriama tam, kokia būtent informacija yra tvarkoma, koks jos turinys, apimtis, kokią įtaką asmens teisėms gali turėti šis tvarkymas, t. y. koncentruojamasi ne į procesinį, tačiau būtent į asmens duomenų apsaugos aspektą. Taigi teikdamas skundą duomenų subjektas turėtų įvertinti, kuris aspektas dominuoja konkrečiu kreipimosi atveju: asmens duomenų, kaip sudedamosios teisės į privatumą dalies, pažeidimas ar asmens duomenų tvarkymo reikalavimų pažeidimas daugiau procesine formos prasme, ir atitinkamai rinktis instituciją, į kurią kreiptis dėl pažeistų teisių gynybos. Taip pat atkreiptinas dėmesys, kad asmuo, matydamas objektyvų pagrindą ir dvejopą problemos prigimtį, gali lygiagrečiai kreiptis tiek į vieną, tiek į kitą instituciją.

Paminėtina ir skundo teikimo tarptautinio bendradarbiavimo atveju baudžiamosiose bylose specifiška. Tarptautinio bendradarbiavimo atveju asmens duomenų tvarkymas atliekamas užsienio valstybėje, joje vykstančio ikiteisminio tyrimo ar baudžiamosios bylos nagrinėjimo tikslais. Taigi logiška manyti, kad proceso opera-

⁴⁹ *Backer M., Hornung G. Data Processing by Police and Criminal Justice Authorities in Europe – the Influence of the Commission’s draft on the national police laws and laws of criminal procedure // Computer law & security Report, 2012, 28, p. 631.*

tyvumo principas geriausiai būtų realizuotas skundą tokiu atveju pateikiant būtent šios kitos užsienio valstybės teisėsaugos institucijoms. Kita vertus, reikalavimas, kad asmuo skundą pateiktų užsienio valstybei, gali būti vertinamas kaip neproporcingai didelė našta. Taigi skundas, atsižvelgiant į proceso greitumą, ekonomiškumą, teiktinas nacionalinei teisėsaugos institucijai arba nepriklausomai priežiūros institucijai, laikantis nurodytos strategijos dėl skundo pobūdžio.

Skundą dėl neteisėto disponavimo asmens duomenimis turi teisę pateikti ne tik tiesiogiai baudžiamajame procese dalyvaujantis asmuo, tačiau ir trečiasis asmuo, jei nustatoma, kad jo asmens duomenys buvo neteisėtai tvarkyti. Tokia pozicija pagrindžiama EŽTT jurisprudencija. *Rotaru prieš Rumuniją* byla⁵⁰ yra puikus pavyzdys, koks yra svarbus asmens dalyvavimas jo asmens duomenų valdymo procese. Šiuo atveju dalis surinktos informacijos buvo surinkta ne apie pareiškėją, tačiau apie kitą asmenį, turintį tokį patį vardą ir pavardę. Taigi šiuo atveju pažeista ne tik pareiškėjo, tačiau galimai ir kito asmens, kurio duomenimis disponavo teisėsauga, asmens duomenų apsauga. Kiekvienu atveju, kai yra nustatoma, jog nesant teisinio pagrindo (galimai per klaidą) buvo tvarkomi trečiojo asmens duomenys, šiam asmeniui privaloma pranešti apie tokį disponavimo faktą ir tokiu būdu suteikti galimybę ginti pažeistas procesines teises.

- **Žalos atlyginimas**

Galiausiai pabrėžtina asmens duomenų savininko teisė kreiptis dėl žalos, padarytos neteisėtai tvarkant jo asmens duomenis, atlyginimo. Ši teisė įtvirtinta Direktyvos 56-ajame straipsnyje, numatant bet kurio asmens, patyrusio žalą dėl neteisėtos duomenų tvarkymo operacijos ar bet kokio veiksmo, nesuderinamo su Direktyva, teisę reikalauti patirtos žalos atlyginimo. Duomenų subjektas turi teisę kreiptis tiek dėl turtinės, tiek dėl neturtinės žalos atlyginimo. Nacionaliniame reguliavime pagrindas kreiptis dėl žalos atlyginimo asmens duomenų pažeidimo atveju baudžiamajame procese tiesiogiai nustatytas tik dėl tokio pažeidimo, padaryto tarptautinio bendradarbiavimo metu. Ši duomenų subjekto teisė reguliuojama Įstatymo 16-ame straipsnyje⁵¹. Tačiau BPK ar kiti teisės aktai tiesiogiai nenumato duomenų subjekto teisės ir galimybės kreiptis dėl asmens duomenų apsaugos pažeidimo išimtinai na-

⁵⁰ Europos Žmogaus Teisių Teismas. 2000 m. gegužės 4 d. sprendimas byloje Nr. 28341/95, *Rotaru prieš Rumuniją*.

⁵¹ **16 straipsnis. Žalos atlyginimas.** 1. Turtinė ir neturtinė žala, atsiradusi dėl neteisėto asmens duomenų tvarkymo arba duomenų valdytojo ar duomenų tvarkytojo, taip pat dėl kitų asmenų veiksmų (neveikimo), pažeidžiančių šio įstatymo nuostatas, atlyginama įstatymų nustatyta tvarka. Ginčus dėl žalos atlyginimo sprendžia teismas. 2. Lietuvos kompetentinga institucija negali gindamasi pareikšti asmeniui, kuris kreipėsi į ją dėl žalos, patirtos dėl neteisėtų, neišsamių, netikslių duomenų tvarkymo, atlyginimo, kad jai neteisėtingus, netikslius, neišsamius asmens duomenis teikė valstybės narės kompetentinga institucija.

cionalinio pobūdžio baudžiamajame procese. Tokia teisė realizuotina tik sistemiškai aiškinant teisės aktų nuostatas. Svarbu pažymėti, kad, pagal Įstatymo 16 straipsnio 1 dalį, ginčus dėl žalos atlyginimo sprendžia teismas. Taigi galimo asmens duomenų apsaugos pažeidimo nagrinėjime pagal šiuo metu galiojančią teisinę reguliavimą privalomai nedalyvauja nepriklausoma institucija ir tai vėlgi tam tikrais atvejais gali būti vertintina kaip reguliavimo trūkumas, kadangi specializuotoje srityje veikiantis subjektas gali teikti kvalifikuotą pagalbą teismui, sprendžiančiam klausimą dėl konkretaus pažeidimo. Vis dėlto duomenų subjekto teisė kreiptis dėl žalos, padarytos pažeidimu tvarkant jo asmens duomenis baudžiamajame procese, atlyginimo kildintina iš bendrojo žalos atlyginimo principo. Taigi žala atlygintina visais atvejais, kai nustatomas pažeidimas, nepaisant to, ar jis buvo padarytas išimtinai tarptautinio bendradarbiavimo atveju, ar vykstant nacionaliniam baudžiamajam procesui. Taigi siekiant žalos atlyginimo dėl pažeidimo, padaryto asmens duomenis tvarkant išimtinai nacionalinio pobūdžio baudžiamajame procese, pagal šiuo metu galiojančią teisinę reguliavimą, taikomos bendrosios žalos atlyginimo civilinėje teisėje taisyklės.

Asmens duomenys gali būti tvarkomi ir panaudojami itin įvairiais tikslais, taigi atsainumas, neatidumas duomenų tvarkymo srityje yra ypač pavojingas. Teisės saugos institucijoms gali būti sudėtinga priimti tinkamą sprendimą, susijusį su asmens duomenų tvarkymu, pavyzdžiui, nuspręsti, koks perduotinos informacijos kiekis yra ne per didelis, bet pakankamas. Tai ypač svarbu atsižvelgiant į galimą tolesnę informacijos panaudojimą. Problema iliustruotina gana senu, tačiau turinio prasme aktuali pavyzdžiu Lietuvos vyriausiojo administracinio teismo 2004 m. gruodžio 16 d. nutartyje administracinėje byloje Nr. N-12-1541-04, kurioje teisės saugos institucijų Seimo Antikorupcijos komisijai buvo perduota informacija apie baudžiamąją bylą, o Seimo Antikorupcijos komisija priėmė sprendimą pavišinti konkrečius ikiteisminio tyrimo duomenis – pranešimą apie įtarimą bei liudytojo apklausos protokolą, kuriuose buvo užfiksuoti pertekliniai asmens duomenys⁵². Institucijoms apsikeitus sukauptais netiksliais, tikrovės neatitinkančiais, pertekliniais asmens duomenimis, taip pat – netinkamai juos tvarkant nacionaliniuose baudžiamuosiuose procesuose gali kilti neprognozuojami neigiami padariniai ir būti padaroma įvairaus pobūdžio žala. Dėl šios priežasties užtikrinti efektyvų žalos atlyginimo mechanizmą yra itin svarbu.

Valstybėms narėms nustatytas dvejų metų pereinamasis laikotarpis, per kurį Direktyva turės būti įgyvendinta nacionalinėje teisėje. Per šį laikotarpį Direktyvos reguliuojami klausimai turi būti aiškinami taip, kad jie atitiktų Direktyvos nuostatas. Atsižvelgiant į Lisabonos sutartimi išplėstą ESTT kompetenciją, svarbu atkreipti

⁵² Lietuvos vyriausiasis administracinis teismas. 2004 m. gruodžio 16 d. nutartis administracinėje byloje Nr. N-12-1541-04.

dėmesį į tai, kad valstybėms narėms neįgyvendinus ar netinkamai įgyvendinus Direktyvos nuostatas nacionalinėje teisėje, ar netinkamai jas taikant praktikoje asmenys įgyja teisę kreiptis į ESTT ir buvusio vadinamojo III ramsčio (Policijos ir teismų bendradarbiavimas) rėmuose⁵³, taigi – ir dėl Direktyvos. Šis kreipimasis taip pat gali būti vertinamas kaip dar vienas, tiesa – gana kraštutinis, būdas siekti tvarkant asmens duomenis padarytos žalos atlyginimo. Taigi asmens duomenų subjektui yra suteiktos teisinės priemonės kreiptis dėl žalos atlyginimo, tačiau joms realizuoti yra būtinas adekvatus duomenų subjekto informavimas apie jo asmens duomenų tvarkymo faktą. Manytina, kad nacionalinis reguliavimas turėtų būti papildomas specialiomis nuostatomis, pagal kurias asmenims būtų tiesiogiai suteikta teisė kreiptis dėl žalos atlyginimo, kai ji buvo padaryta baudžiamajame procese tvarkant jų asmens duomenis.

IŠVADOS

1. Siekiant maksimalios asmens duomenų apsaugos kiekvieno baudžiamąjo proceso metu turi būti tvarkomas minimalus asmens duomenų kiekis, kurio pakaktų siekiamiems proceso tikslams, tačiau nesukeliama proporcingumo principo pažeidimo rizika. Asmens duomenų tvarkymas turi vykti tik konkrečiai apibrėžtu tikslu, ribojant duomenų tvarkymą prevencijos tikslu, o keičiant duomenų tvarkymo tikslą – iš naujo peržiūrint duomenų tvarkymo teisėtumo sąlygas.
2. Europos Sąjungos teisėkūroje vykstančia asmens duomenų apsaugos baudžiamajame procese reforma išplečiamos duomenų subjekto teisės, visų pirma akcentuojamas duomenų subjekto informavimas apie jo duomenų tvarkymo faktą ir jo įtraukimas į duomenų tvarkymo procesą, griežtai ribojant atvejus, kai toks informavimas yra neatliekamas dėl baigtinio sąrašo Direktyvoje įvardijamų priežasčių. Duomenų subjektui turi būti užtikrinama reali galimybė pasinaudoti teise pašalinti perteklinius asmens duomenis, pakeisti aktualumą praradusius duomenis, pateikti naujus.
3. Esminis naujojo teisinio reguliavimo aspektas, kuris šiuo metu nacionaliniame reguliavime neužtikrintas, yra nepriklausomos priežiūros institucijos įtraukimas į baudžiamajame procese vykstantį asmens duomenų tvarkymo procesą. Šios institucijos vaidmens išryškinimas, kartu su suinteresuoto asmens teise pateikti skundą dėl neteisėto duomenų tvarkymo, kreiptis dėl žalos atlyginimo bei apskritai – kuo visapusiškesnio įtraukimo į asmens duomenų tvarkymo procesą, vertintini kaip pagrindiniai saugikliai, kuriuos pasitelkus gali būti suderinama baudžiamąjo proceso specifiška ir asmens duomenų subjekto privatumo apsauga.

⁵³ *Hijmans H., Scirocco A.* Shortcomings in EU Data Protection in the Third and the Second Pillars. Can the Lisbon Treaty be Expected to Help? // *Common Market Law Review*, 2009, Nr. 46, p. 1523.

LITERATŪRA

I. Teisės aktai, jurisprudencija ir lydimoji medžiaga

1. 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva Nr. 95/46/EB // Oficialusis leidinys L 281, 23/11/1995, p. 0031–0050.
2. 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje // Oficialusis leidinys L 201, 31/07/2002, p. 0037–0047.
3. 1987 m. kovo 26 d. Europos Žmogaus Teisių Teismo sprendimas byloje Nr. 48, serija A, Nr. 116, *Leander prieš Švediją*.
4. 2000 m. vasario 16 d. Europos Žmogaus Teisių Teismo sprendimas byloje Nr. 27798/95, *Amann prieš Šveicariją*.
5. 2000 m. gegužės 4 d. Europos Žmogaus Teisių Teismo sprendimas byloje Nr. 28341/95, *Rotaru prieš Rumuniją*.
6. 2003 m. gegužės 20 d. Europos Žmogaus Teisių Teismo sprendimas sujungtose bylose C-465/00, C-38/01 ir C-139/01.
7. 2006 m. gegužės 30 d. Europos Sąjungos Teisingumo Teismo sprendimas sujungtose bylose Nr. C-317/04 ir C-318/04.
8. 2006 m. gruodžio 7 d. Europos Žmogaus Teisių Teismo sprendimas byloje Nr. 29514/05, *Van der Velden prieš Nyderlandus*.
9. 2008 m. liepos 9 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 767/2008 dėl Vizų informacinės sistemos (VIS) ir apsikeitimo duomenimis apie trumpalaikes vizas tarp valstybių narių (VIS reglamentas) // Oficialusis leidinys, L 218, 13/8/2008.
10. 2008 m. lapkričio 27 d. Europos Parlamento ir Tarybos pamatinis sprendimas 2008/977/TVR dėl asmens duomenų, tvarkomų vykdant policijos ir teisminių bendradarbiavimą baudžiamosiose bylose // Oficialusis leidinys L 350, 30/12/2008, p. 60–71.
11. 2009 m. lapkričio 12 d. generalinio advokato Jano Mazako išvada ESTT byloje *Komisija prieš Vokietijos Federacinę Respubliką* byloje Nr. C-518/07.
12. 2010 m. rugsėjo 2 d. Europos Žmogaus Teisių Teismo sprendimas byloje Nr. 5623/05, *Uzun prieš Vokietiją*.
13. Europos Sąjungos sutarties ir Sutarties dėl Europos Sąjungos veikimo suvestinės redakcijos // OL C 326, 2012.
14. 2012 m. spalio 16 d. Europos Sąjungos Teisingumo Teismo sprendimas byloje *Komisija prieš Austriją*, Nr. C-614/10.

15. 2012 m. gegužės 22 d. Europos Parlamento ir Tarybos direktyva 2012/13/ES dėl teisės į informaciją baudžiamajame procese // OJ L 142.
16. 2013 m. balandžio 13 d. Europos Žmogaus Teisių Teismo sprendimas byloje Nr. 19522/09, *M. K. prieš Prancūziją*.
17. 2014 m. balandžio 8 d. Europos Sąjungos Teisingumo Teismo sprendimas byloje *Komisija prieš Vengriją*, Nr. C-288/12.
18. 2016 m. kovo 22 d. Lietuvos Respublikos Seimo nutarimu Nr. XII-2263 patvirtinta LRS Teisės ir teisėtvarkos komiteto atlikto parlamentinio tyrimo dėl kriminalinės žvalgybos metu gautos informacijos panaudojimo ir saugojimo išvada // Teisės aktų registras, 2016-03-25, Nr. 6329.
19. Oficialusis Europos Sąjungos leidinys, 2016 m. gegužės 4 d., 59 tomas, Nr. L 119.
20. Asmens duomenų, tvarkomų vykdam policijos ir teisminių bendradarbiavimą baudžiamosiose bylose, teisinės apsaugos įstatymas // Valstybės žinios, Nr. 52-2511, 2011 (su vėlesniais pakeitimais ir papildymais).
21. Europos Sąjungos pagrindinių teisių chartija // Oficialusis leidinys L 326, 26/10/2012, p. 391–407.
22. Hagos programa: laisvės, saugumo ir teisingumo stiprinimas Europos Sąjungoje. 2005/C 53/01.
23. KOMISIJOS KOMUNIKATAS EUROPOS PARLAMENTUI, TARYBAI, EUROPOS EKONOMIKOS IR SOCIALINIŲ REIKALŲ KOMITETUI IR REGIONŲ KOMITETUI Privatumo apsauga glaudžiai susijusiame pasaulyje Europos duomenų apsaugos reglamentavimo pagrindai XXI amžiuje /* COM/2012/09 final */ Prieiga per internetą: <<http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52012DC0009>>.
24. Lietuvos Respublikos baudžiamojo proceso kodeksas // Valstybės žinios, Nr. 37-1341, 2002 (su vėlesniais pakeitimais ir papildymais).
25. Lietuvos Respublikos asmens duomenų, tvarkomų vykdam policijos ir teisminių bendradarbiavimą baudžiamosiose bylose, teisinės apsaugos įstatymo 2 straipsnio pakeitimo įstatymas // Valstybės žinios, 2012-10-20, Nr. 122-6096.
26. Pasiūlymas EUROPOS PARLAMENTO IR TARYBOS REGLAMENTAS dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (Bendrasis duomenų apsaugos reglamentas) /* COM/2012/011 final - 2012/011 (COD).
27. Pasiūlymas EUROPOS PARLAMENTO IR TARYBOS DIREKTYVA dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, nustatymo ar traukimo baudžiamojon atsakomybėn už jas arba baudžiamųjų sankcijų vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo /* COM/2012/010 final - 2012/0010 (COD).

II. Mokslinė literatūra

28. *Andoulsi I.* Personal Data Protection and the First Implementation Semester of the Lisbon Treaty: Achievements and Prospects // *New journal of European Criminal Law*, 2010, vol. 1, Nr. 3.
29. *Backer M., Hornung G.* Data Processing by Police and Criminal Justice Authorities in Europe – the Influence of the Commission’s draft on the national police laws and laws of criminal procedure // *Computer law & security Report*, 2012, 28.
30. *De Busser E.* EU data protection in transatlantic cooperation in criminal matters. Will the EU be serving its citizens an American meal? // *Utrecht Law Review*, 2010, vol. 6, Nr. 1.
31. *Hert P., Papakonstantinou V.* The Police and Criminal Justice Data Protection Directive: Comment and Analysis // *The IT Law Community SCL Forum*, 2012.
32. *Hijmans H., Scirocco A.* Shortcomings in EU Data Protection in the Third and the Second Pillars. Can the Lisbon Treaty be Expected to Help? // *Common Market Law Review*, 2009, Nr. 46, 1485–1529.
33. *Kosti E., Coudert F., Dumortier J.* Data protection in the Third Pillar: in the Aftermath of the ECJ Decision on PNR Data and the Data Retention Directive // *International view of the law computers & technology*, 2007.
34. *Meškauskaitė L.* Teisė į privatų gyvenimą // VI „Registūrų centras“, 2015.
35. *Munoz H. S., Fiodorova A.* DNA and Law Enforcement in the European Union: Tools and Human Rights Protection // *Utrecht Law Review*, 2014, vol. 10, issue 1.
36. *Reding V.* Data Protection in the EU – Challenges Ahead // *EUCRIM*, Issue 2010/1.
37. *Vermeulen G., Beken T. V., Puyenbroeck L. V., Malderen S. V.* Availability of Law Enforcement Information in the European Union: Between Mutual Recognition and Equivalent Right of Access // *IRCP*, Maklu Publishers, 2005.

III. Kiti šaltiniai

38. Data Protection in the European Union-Citizens’ perceptions- Analytical report, Viviane Reding Vice-President of the European Commission, EU Commissioner responsible for Justice, Fundamental Rights and Citizenship Data Protection 30 | eucrim 1 / 2010 Flash Eurobarometer Series 225, January 2008. Prieiga per internetą: <http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf>.
39. Apklauso „Požiūris į duomenų apsaugą ir elektroninę tapatybę Europos Sąjungoje“ rezultatai. Prieiga per internetą: <http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_fact_lt_en.pdf>.
40. Opinion of the European Data Protection Supervisor on the Proposal for a Council

Framework Decision on the protection of personal data processed in the firework of police and judicial cooperation in criminal matters (COM (2005) 475 final) (2006/C 47/12) Prieiga per internetą: <<http://www.statewatch.org/news/2006/sep/eu-com-dp-edps-opinion.pdf>>.

41. Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions. Justice, Freedom and Security in Europe Since 2005: an Evaluation of the Hague Programme and Action Plan. An Extended report on the evaluation of the Hague Programme. SEC(2009) 766 final. Prieiga per internetą: <<http://www.statewatch.org/news/2009/jun/eu-com-sec-766-2009-hague-extended-evaluation.pdf>>.

Justina DEŠRIŪTĖ
Law Institute of Lithuania

MAIN ASPECTS OF PERSONAL DATA PROTECTION DURING CRIMINAL PROCEEDINGS REFORM AND THEIR INFLUENCE TO THE NATIONAL LEGISLATION

Summary

Personal data protection in the field of criminal proceedings and cooperation between law enforcement institutions has been undergoing fundamental changes since the year 2012 in the European Union. On the 16th April, 2016 European Parliament has voted for legislative reform package which includes Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data. Article analysis the main aspects of this new EU level legal act in the light of the national legislation and highlights principal issues in the area.

The center of the reform undoubtedly becomes the subject of personal data as the baseline of the changes in EU legislation is the necessity to enhance its involvement in the processing of data subject's personal data. The right to personal data protection is a part of a general protection of persons's privacy but in the field of criminal justice it can also be related to the right of information during criminal proceedings. It also relates to other procedural rights, such as the right to effective legal defense, and as a result – becomes one of the main areas of protection during national and especially international criminal proceedings. Data subject is granted with the main right to be informed about the fact that his personal data has been processed and with several coherent rights – to rectify, erase, restrict the use of his personal data. However, all of these rights can be restricted in compliance with the aims of criminal proceedings so it is necessary to provide effective tools for the protection of one's personal data even under such complicated conditions.

As one of the main shortcoming in the national legislation could be singled out the lack of information with which data subject is provided during criminal proceedings. National law enforcement authorities often fail to inform data subject about his rights related to personal data protection, the fact about processing of personal data itself is often not being disclosed even after the period during which personal data has been processed. Really sensitive matter is also the aim of personal data processing. Personal data are often being processed too extensively for the prevention of crimes, the period of data retention is mostly undefined, changes of the aim for processing of personal data are done without any additional review of its lawfulness. Another serious problem is that the independent supervisory authority is not involved in the personal data processing in the criminal proceedings in any manner. Such an authority, along with the subject's rights to launch a complaint and seek the reparation for damage done during the unlawful personal data processing, are the main safeguards which can guarantee the balance between personal data protection and the peculiarities of criminal proceedings. All of the above mentioned problems can only be resolved with corresponding legislative changes and a proper application of legal norms in practice.