VADOVAS

Europos duomenų apsaugos teisės vadovas

2018 m. redakcija

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Šio vadovo rankraštis parengtas 2018 m. balandžio mėn.

Ateityje atnaujinta informacija bus prieinama FRA svetainėje adresu fra.europa.eu, Europos Tarybos svetainėje adresu coe.int/dataprotection, Europos Žmogaus Teisių Teismo svetainės skiltyje „Jurisprudencija“ adresu echr.coe.int ir Europos duomenų apsaugos priežiūros pareigūno svetainėje adresu edps.europa.eu.

Nuotraukos (viršelio ir leidinyje): © iStockphoto

Daugiau informacijos apie Europos Sąjungą pateikiama internete (http://europa.eu).

Liuksemburgas: Europos Sąjungos leidinių biuras, 2021

Europos Taryba:	ISBN 978-92-871-9828-0		
FRA – Print:	ISBN 978-92-9474-790-7	doi:10.2811/76398	TK-05-17-225-LT-C
FRA – PDF:	ISBN 978-92-9474-784-6	doi:10.2811/022710	TK-05-17-225-LT-N

Šis vadovas parengtas anglų kalba. Europos Taryba (ET) ir Europos Žmogaus Teisių Teismas (EŽTT) neatsako už jo vertimų į kitas kalbas kokybę. Šiame vadove išreikštos nuomonės nebūtinai atitinka ET ir EŽTT nuomonę. Jame pateikta nuorodų į kai kuriuos komentarus ir kitus vadovus. ET ir EŽTT neatsako už jų turinį, o tai, kad jie įtraukti į šį sąrašą, nereiškia, kad pritariama šiuose leidiniuose pateiktai informacijai. Daugiau leidinių išvardyta EŽTT svetainės bibliotekos puslapiuose adresu echr.coe.int.

Šio vadovo turinyje nepateikiama oficiali Europos duomenų apsaugos priežiūros pareigūno (EDAPP) nuomonė ir jis nėra privalomas EDAPP naudojantis savo kompetencija. EDAPP neprisiima jokios atsakomybės už vertimų į kitas nei anglų kalbas kokybę.

Europos duomenų apsaugos teisės vadovas

2018 m. redakcija

Pratarmė

Mūsų visuomenė tampa vis labiau skaitmenizuota. Technologinių pokyčių tempai ir duomenų tvarkymo būdai, kuriuos lemia šie pokyčiai, daro poveikį įvairiems mūsų kasdienio gyvenimo aspektams. Neseniai buvo persvarstytos Europos Sąjungos (ES) ir Europos Tarybos teisinės sistemos, kuriomis užtikrinama privatumo ir asmens duomenų apsauga.

Europa yra pasaulinė pirmūnė duomenų apsaugos srityje. ES duomenų apsaugos standartai yra pagrįsti Europos Tarybos 108-ąja konvencija, ES teisės aktais, įskaitant Bendrąjį duomenų apsaugos reglamentą ir Duomenų apsaugos policijos ir baudžiamosios teisenos institucijoms tvarkant asmens duomenis direktyvą, taip pat atitinkama Europos Žmogaus Teisių Teismo ir Europos Sąjungos Teisingumo Teismo praktika.

ES ir Europos Tarybos įvykdytos plataus masto ir kartais sudėtingos duomenų apsaugos reformos fiziniams asmenims ir įmonėms buvo naudingos įvairiais atžvilgiais ir turėjo tam tikrą poveikį. Šio vadovo paskirtis – didinti informuotumą ir gerinti žinias apie duomenų apsaugos taisykles, visų pirma tarp teisės specialistų, kurie nesispecializuoja šioje srityje ir savo darbe turi spręsti su duomenų apsauga susijusius klausimus.

Vadovą parengė ES Pagrindinių teisių agentūra (FRA) drauge su Europos Taryba (įskaitant Europos Žmogaus Teisių Teismo kanceliariją) ir Europos duomenų apsaugos priežiūros pareigūnu. Vadovu atnaujinama 2014 m. redakcija ir jis yra vienas iš daugelio FRA ir Europos Tarybos kartu rengiamų teisinių vadovų.

Norime padėkoti Airijos, Belgijos, Estijos, Gruzijos, Italijos, Jungtinės Karalystės, Monako, Prancūzijos, Šveicarijos ir Vengrijos duomenų apsaugos institucijoms už jų naudingą grįžtamąją informaciją dėl vadovo projekto. Be to, dėkojame Europos Komisijos duomenų apsaugos skyriui ir Europos Komisijos tarptautinio duomenų judėjimo ir apsaugos skyriui. Dėkojame Europos Sąjungos Teisingumo Teismui už pateiktus dokumentus, kurie buvo reikalingi rengiant šį vadovą. Galiausiai dėkojame Mykolo Romerio universiteto Teisingumo tyrimų laboratorijai už pagalbą peržiūrint šio vadovo tekstą lietuvių kalba.

Christos Giakoumopoulos

Europos Tarybos žmogaus teisių ir teisinės valstybės generalinis direktorius

Giovanni Buttarelli

Europos duomenų apsaugos priežiūros pareigūnas

Michael O'Flaherty

Europos Sąjungos pagrindinių teisių agentūros direktorius

Turinys

Santrumpos ir akronimai

AVSS	apsauginė vaizdo stebėjimo sistema
BCR	įmonėms privalomos taisyklės
BDAR	Bendrasis duomenų apsaugos reglamentas
CETS	Europos Tarybos sutarčių serija
Chartija	Europos Sąjungos pagrindinių teisių chartija
CRM	ryšių su klientais valdymas
C-SIS	centrinė Šengeno informacinė sistema
DAI	duomenų apsaugos institucija
DAP	duomenų apsaugos pareigūnas
EAO	Europos arešto orderis
EB	Europos bendrija
EBPO	Ekonominio bendradarbiavimo ir plėtros organizacija
EDAPP	Europos duomenų apsaugos priežiūros pareigūnas
EDAV	Europos duomenų apsaugos valdyba
EEE	Europos ekonominė erdvė
EFSA	Europos maisto saugos tarnyba
ELPA	Europos laisvosios prekybos asociacija
ENISA	Europos Sąjungos tinklų ir informacijos apsaugos agentūra
ENP	Europolo nacionalinis padalinys
EPPO	Europos prokuratūra
ES	Europos Sąjunga
ESMA	Europos vertybinių popierių ir rinkų institucija
ES sutartis	Europos Sąjungos sutartis
ESTT	Europos Sąjungos Teisingumo Teismas (iki 2009 m. gruodžio mėn. – Europos Teisingumo Teismas, ETT)
ET	Europos Taryba
eTEN	transeuropiniai telekomunikacijų tinklai
eu-LISA	ES Europos Sąjungos didelės apimties IT sistemų agentūra
„EuroPriSe“	Europos privatumo apsaugos ženklas
EŽTK	Europos žmogaus teisių konvencija

EŽTT	Europos Žmogaus Teisių Teismas
FRA	Europos Sąjungos pagrindinių teisių agentūra
GPS	globalinės padėties nustatymo sistema
IPT	interneto paslaugų teikėjas
IRT	informacinės ir ryšių technologijos
JSB	jungtinė priežiūros institucija
JT	Jungtinės Tautos
MIS	Muitinės informacinė sistema
N-SIS	nacionalinė Šengeno informacinė sistema
NVO	nevyriausybinė organizacija
OL	oficialusis leidinys
PIN	asmens kodas
PNR	keleivio duomenų įrašas
SCG	priežiūros koordinavimo grupė
SEPA	bendra mokėjimų eurais erdvė
SESV	Sutartis dėl Europos Sąjungos veikimo
SIS	Šengeno informacinė sistema
SWIFT	Pasaulinė tarpbankinių finansinių telekomunikacijų organizacija
TPPTP	Tarptautinis pilietinių ir politinių teisių paktas
VIS	Vizų informacinė sistema
VŽTD	Visuotinė žmogaus teisių deklaracija
108-oji konvencija	Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (Europos Taryba) 108-ąją konvenciją iš dalies keičiantį protokolą (CETS Nr. 223) (atnaujinta 108-oji konvencija) Elsinore (Danija) surengtoje 128-ojoje sesijoje (2018 m. gegužės 17–18 d.) priėmė Europos Tarybos Ministrų Komitetas. Nuorodos į atnaujintą 108-ąją konvenciją reiškia Konvenciją, kuri buvo iš dalies pakeista protokolu CETS Nr. 223.

Kaip naudotis šiuo vadovu

Šiame vadove pateikiamos teisinės normos, susijusios su Europos Sąjungos (ES) ir Europos Tarybos (ET) nustatyta duomenų apsauga. Jis parengtas siekiant padėti specialistams, kurių specializacija nėra susijusi su duomenų apsauga, įskaitant advokatus, teisėjus ir kitus teisės specialistus, taip pat kitose įstaigose, pavyzdžiui, nevyriausybinėse organizacijose (NVO), dirbantiems asmenims, kuriems gali kilti su duomenų apsauga susijusių teisinių klausimų.

Vadovas yra pirmas atskaitos taškas tais atvejais, kai sprendžiami su atitinkama ES teise, Europos žmogaus teisių konvencija (EŽTK) ir ET Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (108-oji konvencija) ir kitais ET teisės aktais susiję klausimai.

Kiekviename skyriuje pirmiausia pateikiama lentelė, kurioje nurodomos teisinės nuostatos, susijusios su temomis, kurios aptariamos konkrečiame skyriuje. Lentelėse nurodoma tiek su ET, tiek su ES teisės aktais susijusi informacija, be to, jose pateikiama atrinkta Europos Žmogaus Teisių Teismo (EŽTT) ir Europos Sąjungos Teisingumo Teismo (ESTT) praktika. Paskui paeiliui pateikiami atitinkami dviejų skirtingų Europos sistemų teisės aktai, atsižvelgiant į tai, kaip jie taikomi konkrečioms temoms. Iš to skaitytojams bus aišku, kiek abi teisės sistemos sutampa ir kiek jos skiriasi. Skaitytojams taip pat turėtų būti lengviau rasti pagrindinę informaciją, susijusią su jų padėtimi, ypač jeigu jiems taikoma tik ET teisė. Kai kuriuose skyriuose, kuriuose tai yra naudinga siekiant nuosekliai pateikti turinį, lentelėse aptariamų temų eiliškumas gali šiek tiek skirtis nuo pačiame skyriuje aptartų temų eiliškumo. Vadove taip pat pateikiama trumpa Jungtinių Tautų sistemos apžvalga.

ES nepriklausančių valstybių, kurios yra ET valstybės narės ir EŽTK ir 108-osios konvencijos šalys, specialistai su savo šalimi susijusią informaciją gali rasti tuose skirsniuose, kuriuose aptariama ET teisė. ES nepriklausančių valstybių specialistai taip pat turi atsižvelgti į tai, kad nuo ES Bendrojo duomenų apsaugos reglamento priėmimo ES duomenų apsaugos taisyklės taikomos organizacijoms ir kitiems subjektams, kurie nėra įsisteigę ES, jeigu jie asmens duomenis tvarko ir prekes bei paslaugas siūlo Sąjungoje esantiems duomenų subjektams arba stebi tokių duomenų subjektų elgesį.

ES valstybių narių specialistai turės susipažinti su abiem skirsniais, nes šios valstybės yra saistomos abiejų teisės sistemų. Reikėtų pažymėti, kad Europos duomenų apsaugos taisyklių reformos ir atnaujinimai, kurių ėmėsi Europos Taryba (atnaujinta

108-oji konvencija, iš dalies pakeista protokolu CETS Nr. 223) ir ES (Bendrojo duomenų apsaugos reglamento ir Direktyvos (ES) 2016/680 priėmimas), buvo vykdomi vienu metu. Abiejų teisinių sistemų reguliavimo institucijos daugiausia dėmesio skyrė šių dviejų teisinių sistemų nuoseklumui ir suderinamumui užtikrinti. Taigi, reformos padėjo labiau suderinti ET ir ES duomenų apsaugos teisę. Asmenims, norintiems gauti daugiau informacijos konkrečiu klausimu, labiau specializuotos medžiagos sąrašą galima rasti vadovo skirsnyje „Papildoma literatūra“. Dėl informacijos, susijusios su 108-osios konvencijos ir jos 2001 m. papildomo protokolo nuostatomis, kurios toliau taikomos iki iš dalies keičiančio protokolo įsigaliojimo, skaitytojai turėtų remtis vadovo 2014 m. redakcija.

ET teisė pateikiama naudojant trumpas nuorodas į atrinktas EŽTT bylas. Šios bylos atrinktos iš daugybės EŽTT sprendimų ir nutarčių, susijusių su duomenų apsaugos klausimais.

Atitinkama ES teisė apima priimtas teisėkūros priemones, atitinkamas Sutarčių ir Europos Sąjungos pagrindinių teisių chartijos nuostatas, atsižvelgiant į tai, kaip jos išaiškintos ESTT praktikoje. Be to, vadove pateikiamos 29 straipsnio darbo grupės, patariamosios įstaigos, kuriai pagal Duomenų apsaugos direktyvą pavesta užduotis teikti specializuotas konsultacijas ES valstybėms narėms ir kurios užduotis nuo 2018 m. gegužės 25 d. perėmė Europos duomenų apsaugos valdyba (EDAV), priimtos nuomonės ir rekomendacijos. Europos duomenų apsaugos priežiūros pareigūno nuomonėse taip pat pateikiamos svarbios įžvalgos, susijusios su ES teisės aiškinimu, ir jos yra įtrauktos į šį vadovą.

Šiame vadove aprašytose arba cituojamose bylose pateikta svarbios tiek EŽTT, tiek ESTT jurisprudencijos pavyzdžių. Vadovo pabaigoje pateikiamos gairės, kurios turi padėti skaitytojams ieškoti teismų praktikos internete. Pateikta ESTT praktika yra susijusi su anksčiau galiojusia Duomenų apsaugos direktyva. Tačiau ESTT išaiškinimai toliau taikomi atitinkamoms teisėms ir pareigoms, kurios nustatytos Bendrajame duomenų apsaugos reglamente.

Be to, teksto langeliuose mėlyname fone pateikiami praktiniai pavyzdžiai, kuriuose aptariami hipotetiniai scenarijai. Šiuose pavyzdžiuose išsamiau aptariamas praktinis Europos duomenų apsaugos taisyklių taikymas, visų pirma tais atvejais, kai nėra konkrečios susijusios EŽTT arba ESTT praktikos. Kituose pilko fono teksto langeliuose pateikiami iš kitų šaltinių nei EŽTT ir ESTT praktika paimti pavyzdžiai; tai gali būti teisės aktuose ir 29 straipsnio darbo grupės priimtose nuomonėse pateikti pavyzdžiai.

Vadovo pradžioje pateikiamas trumpas dviejų teisinių sistemų, nustatytų pagal EŽTK ir ES teisę, reikšmės apibūdinimas (1 skyrius). 2–10 skyriuose aptariami šie klausimai:

- duomenų apsaugos terminija;
- pagrindiniai Europos duomenų apsaugos teisės principai;
- Europos duomenų apsaugos teisės taisyklės;
- nepriklausoma priežiūra;
- duomenų subjektų teisės ir jų užtikrinimas;
- tarpvalstybinis duomenų perdavimas ir judėjimas;
- duomenų apsauga policijos ir baudžiamosios teisenos srityje;
- kitos Europos duomenų apsaugos taisyklės konkrečiose srityse;
- šiuolaikiniai iššūkiai asmens duomenų apsaugos srityje.

1

Europos duomenų apsaugos teisės kontekstas ir aplinkybės

ES	Reglamentuojami klausimai	ET
Teisė į duomenų apsaugą		
Sutarties dėl Europos Sąjungos veikimo 16 straipsnis Europos Sąjungos pagrindinių teisių chartijos (Chartija) 8 straipsnis (teisė į asmens duomenų apsaugą) Direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (Duomenų apsaugos direktyva), OL L 281, 1995 (galiojo iki 2018 m. gegužės mėn.) Tarybos pamatinis sprendimas 2008/977/TVR dėl asmens duomenų, tvarkomų vykdant policijos ir teisminį bendradarbiavimą baudžiamosiose bylose, apsaugos, OL L 350, 2008 (galiojo iki 2018 m. gegužės mėn.) Reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas), OL L 119, 2016		EŽTK 8 straipsnis (teisė į asmeninį ir šeimos gyvenimą, būsto neliečiamybę ir susirašinėjimo slaptumą)

ES	Reglamentuojami klausimai	ET
Direktyva (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, ir kuriuo panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR (Duomenų apsaugos policijos ir baudžiamosios teisenos institucijoms tvarkant asmens duomenis direktyva), OL L 119, 2016 Direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių), OL L 201, 2002 Reglamentas (EB) Nr. 45/2001 dėl asmenų apsaugos Bendrijos institucijoms ir įstaigoms tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo (ES institucijų duomenų apsaugos reglamentas), OL L 8, 2001		Atnaujinta Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (atnaujinta 108-oji konvencija)
Teisės į asmens duomenų apsaugą apribojimai		
Chartijos 52 straipsnio 1 dalis Bendrojo duomenų apsaugos reglamento 23 straipsnis ESTT, sujungtos bylos C-92/09 ir C-93/09, *Volker und Markus Schecke GbR ir Hartmut Eifert prieš Land Hessen* (didžioji kolegija, toliau – DK), 2010 m.		EŽTK 8 straipsnio 2 dalis Atnaujintos 108-osios konvencijos 11 straipsnis EŽTT, *S. ir Marper prieš Jungtinę Karalystę* (DK), Nr. 30562/04 ir 30566/04, 2008 m.
Teisių pusiausvyra		
ESTT, sujungtos bylos C-92/09 ir C-93/09, *Volker und Markus Schecke GbR ir Hartmut Eifert prieš Land Hessen* (DK), 2010 m.	**Bendri klausimai**	
ESTT, C-73/07, *Tietosuojavaltuutettu prieš Satakunnan Markkinapörssi Oy ir Satamedia Oy* (DK), 2008 m. ESTT, C-131/12, *Google Spain SL, Google Inc. prieš Agencia Española de Protección de Datos (AEPD), Mario Costeja González* (DK), 2014 m.	**Saviraiškos laisvė**	EŽTT, *Axel Springer AG prieš Vokietiją* (DK), Nr. 39954/08, 2012 m. EŽTT, *Mosley prieš Jungtinę Karalystę*, Nr. 48009/08, 2011 m. EŽTT, *Bohlen prieš Vokietiją*, Nr. 53495/09, 2015 m.

ES	Reglamentuojami klausimai	ET
ESTT, *Europos Komisija prieš The Bavarian Lager Co. Ltd* (DK), C-28/08 P, 2010 m. ESTT, C-615/13 P, *ClientEarth, PAN Europe prieš EFSA*, 2015 m.	Teisė susipažinti su dokumentais	EŽTT, *Magyar Helsinki Bizottság prieš Vengriją* (DK), Nr. 18030/11, 2016 m.
Bendrojo duomenų apsaugos reglamento 90 straipsnis	Profesinė paslaptis	EŽTT, *Pruteanu prieš Rumuniją*, Nr. 30181/05, 2015 m.
Bendrojo duomenų apsaugos reglamento 91 straipsnis	Religijos ar tikėjimo laisvė	
	Meno ir mokslo laisvė	EŽTT, *Vereinigung bildender Künstler prieš Austriją*, Nr. 68354/01, 2007 m.
ESTT, C-275/06, *Productores de Música de España (Promusicae) prieš Telefónica de España SAU* (DK), 2008 m.	Nuosavybės apsauga	
ESTT, C-131/12, *Google Spain SL, Google Inc. prieš Agencia Española de Protección de Datos (AEPD), Mario Costeja González* (DK), 2014 m. ESTT, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce prieš Salvatore Manni*, 2017 m.	Ekonominės teisės	

1.1. Teisė į asmens duomenų apsaugą

Pagrindiniai faktai

- Pagal EŽTK 8 straipsnį asmens teisė į apsaugą tvarkant asmens duomenis yra teisės į privataus ir šeimos gyvenimą, būsto neliečiamybę ir susirašinėjimo slaptumą sudedamoji dalis.
- ET 108-oji konvencija yra pirmasis ir iki šiol vienintelis tarptautinis teisiškai privalomas teisės aktas, kuriame reglamentuojama duomenų apsauga. Konvencija buvo atnaujinta priėmus iš dalies keičiantį CETS protokolą Nr. 223.
- Pagal ES teisę asmens duomenų apsauga pripažįstama kaip atskira pagrindinė teisė. Tai patvirtinama Sutarties dėl Europos Sąjungos veikimo 16 straipsnyje, taip pat ES pagrindinių teisių chartijos 8 straipsnyje.
- ES teisėje duomenų apsauga pirmą kartą reglamentuota 1995 m. priėmus Duomenų apsaugos direktyvą.

- Atsižvelgdama į sparčią technologijų raidą, ES 2016 m. priėmė naują teisės aktą, kad pritaikytų duomenų apsaugos taisykles prie skaitmeninio amžiaus. Bendrasis duomenų apsaugos reglamentas, kuriuo panaikinama Duomenų apsaugos direktyva, pradėtas taikyti 2018 m. gegužės mėn.
- Kartu su Bendruoju duomenų apsaugos reglamentu ES priėmė teisės aktą dėl valstybės institucijų atliekamo asmens duomenų tvarkymo teisėsaugos tikslais. Direktyvoje (ES) 2016/680 nustatomos duomenų apsaugos taisyklės ir principai, kuriais reglamentuojamas asmens duomenų tvarkymas nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba baudžiamųjų sankcijų vykdymo tikslais.

1.1.1. Teisė į privatų gyvenimą ir teisė į asmens duomenų apsaugą. Trumpas įvadas

Teisė į privatų gyvenimą ir teisė į asmens duomenų apsaugą yra glaudžiai susijusios, tačiau skirtingos teisės. Teisė į privatumą, kuri Europos Sąjungos teisėje nurodoma kaip teisė į privatų gyvenimą, tarptautinėje žmogaus teisių teisėje kaip viena iš pagrindinių saugomų žmogaus teisių atsirado 1948 m. priėmus Visuotinę žmogaus teisių deklaraciją (VŽTD). Netrukus po to, kai buvo priimta VŽTD, Europa taip pat patvirtino šią teisę Europos žmogaus teisių konvencijoje (EŽTK), t. y. 1950 m. parengtoje sutartyje, kuri yra teisiškai privaloma jos susitariančiosioms šalims. EŽTK nustatyta, kad kiekvienas turi teisę į privatų ir šeimos gyvenimą, būsto neliečiamybę ir susirašinėjimo slaptumą. Valdžios institucijoms draudžiama riboti šios teisės įgyvendinimą, išskyrus atvejus, kai toks ribojimas atitinka įstatymą, juo siekiama svarbių ir teisėtų viešųjų interesų ir jis yra būtinas demokratinėje visuomenėje.

VŽTD ir EŽTK buvo priimtos gerokai anksčiau, nei buvo sukurti kompiuteriai ir internetas ir prieš atsirandant informacinei visuomenei. Šie pokyčiai suteikė daug naudos asmenims ir visuomenei, pagerino gyvenimo kokybę, veiksmingumą ir našumą. Kartu jie kelia naujų pavojų teisei į privatų gyvenimą. Atsižvelgiant į konkrečių taisyklių, reglamentuojančių asmens duomenų rinkimą ir naudojimą, atsirado nauja privatumo koncepcija, kuri vienose jurisdikcijose vadinama „informaciniu privatumu“, o kitose – „teise į informacinį apsisprendimą“[1]. Ši koncepcija lėmė tai, kad buvo sukurti specialūs teisiniai reglamentai, kuriuose numatyta asmens duomenų apsauga.

1 Vokietijos Federalinis Konstitucinis Teismas patvirtino teisę į informacinį apsisprendimą 1983 m. sprendime *Volkszählungsurteil*, BVerfGE Bd. 65, S. 1ff. Teismas laikėsi nuomonės, kad informacinis apsisprendimas kyla iš Vokietijos Konstitucijoje saugomos pagrindinės teisės į asmenybės gerbimą. EŽTT 2017 m. sprendime pripažino, kad EŽTK 8 straipsnyje „numatyta teisė į informacinį apsisprendimą“. Žr. EŽTT, *Satakunnan Markkinapörssi Oy ir Satamedia Oy prieš Suomiją*, Nr. 931/13, 2017 m. birželio 27 d., 137 punktas.

Duomenų apsaugos era Europoje prasidėjo XX amžiaus 8-ajame dešimtmetyje, kai keletas valstybių priėmė teisės aktus, kuriais siekė kontroliuoti asmeninės informacijos tvarkymą valdžios institucijose ir stambiose įmonėse[2]. Tuomet duomenų apsaugos teisės aktai buvo priimti Europos lygmeniu[3] ir ilgainiui susiformavo atskira duomenų apsaugos sistema, kuri nėra priskiriama teisei į privatų gyvenimą. Atsižvelgiant į ES teisinę tvarką, duomenų apsauga pripažįstama kaip pagrindinė teisė, kuri yra atskira nuo pagrindinės teisės į privatų gyvenimą. Dėl tokio atskyrimo kyla klausimas dėl šių dviejų teisių santykio ir skirtumų.

Teisė į privatų gyvenimą ir teisė į asmens duomenų apsaugą yra glaudžiai susijusios. Abiem teisėmis stengiamasi apsaugoti panašias vertybes, t. y. asmenų savarankiškumą ir žmogaus orumą suteikiant jiems erdvę, kurioje jie galėtų laisvai ugdyti savo asmenybę, mąstyti ir formuoti savo nuomonę. Todėl tai yra esminė būtina kitų pagrindinių teisių, pavyzdžiui, saviraiškos laisvės, teisės į taikių susirinkimų ir asociacijų laisvę ir religijos laisvės, įgyvendinimo sąlyga.

Abiejų teisių formuluotė ir taikymo sritis skiriasi. Teisę į privatų gyvenimą sudaro bendras ribojimo draudimas, kuriam taikomi tam tikri viešojo intereso kriterijai, kuriais remiantis tam tikrais atvejais galima pateisinti ribojimą. Asmens duomenų apsauga vertinama kaip šiuolaikinė ir aktyvi teisė[4], kuria sukuriama stabdžių ir atsvarų sistema, padedanti apsaugoti asmenis tais atvejais, kai tvarkomi jų asmens duomenys. Duomenis privaloma tvarkyti laikantis esminių asmens duomenų apsaugos reikalavimų, t. y. nepriklausomos priežiūros ir pagarbos duomenų subjekto teisėms[5].

ES pagrindinių teisių chartijos (toliau – Chartija) 8 straipsnyje ne tik patvirtinama teisė į asmens duomenų apsaugą, bet ir išvardijamos su šia teise susijusios pagrindinės vertybės. Jame nustatyta, kad asmens duomenis privaloma tvarkyti sąžiningai,

2 1970 m. Vokietijos Heseno žemė priėmė pirmąjį įstatymą dėl duomenų apsaugos, kuris buvo taikomas tik šioje žemėje. 1973 m. Švedija priėmė pirmąjį pasaulyje nacionalinį duomenų apsaugos įstatymą. Iki XX amžiaus 9-ojo dešimtmečio pabaigos keletas Europos valstybių (Jungtinė Karalystė, Nyderlandai, Prancūzija ir Vokietija) taip pat priėmė duomenų apsaugą reglamentuojančius teisės aktus.

3 1981 m. buvo priimta Europos Tarybos konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (108-oji konvencija). ES savo pirmąjį išsamų duomenų apsaugą reglamentuojantį teisės aktą priėmė 1995 m.: Direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo.

4 Generalinė advokatė E. Sharpston apibūdino bylą kaip susijusią su dviem atskiromis teisėmis: „klasikinė“ teisė į privatumo apsaugą ir „šiuolaikiškesnė“ teisė į duomenų apsaugą. Žr. ESTT, sujungtos bylos C-92/09 ir C-93/02, *Volker und Markus Schecke GbR prieš Land Hessen*, *generalinės advokatės E. Sharpston* išvados, pateiktos 2010 m. birželio 17 d., 71 punktas.

5 P. Hustinx „EDPS Speeches & Articles“, *EU Data Protection Law: the Review of Directive 95/46/EC and the Proposed General Data Protection Regulation*, 2013 m. liepos mėn.

konkrečiais tikslais ir remiantis atitinkamo asmens sutikimu arba įstatyme nustatytu teisėtu interesu. Asmenys privalo turėti teisę susipažinti su savo asmens duomenimis ir juos ištaisyti, o šios teisės laikymąsi privalo kontroliuoti nepriklausoma institucija.

Teisė į asmens duomenų apsaugą pradeda galioti visais atvejais, kai tvarkomi asmens duomenys; todėl ši teisė yra platesnė, palyginti su teise į privatų gyvenimą. Bet kokiai asmens duomenų tvarkymo operacijai taikoma atitinkama apsauga. Duomenų apsauga yra susijusi su visų rūšių asmens duomenimis ir duomenų tvarkymu, nepaisant santykių ir poveikio privatumui. Tvarkant asmens duomenis, taip pat gali būti pažeidžiama teisė į privatų gyvenimą, kaip parodyta toliau pateiktuose pavyzdžiuose. Tačiau tam, kad būtų taikomos duomenų apsaugos taisyklės, nebūtina įrodyti, kad buvo pažeista teisė į privatų gyvenimą.

Teisė į privatumą yra susijusi su situacijomis, kai buvo pažeistas privatus interesas arba „privatus gyvenimas“. Kaip matyti šiame vadove, „privataus gyvenimo“ sąvoka teismų praktikoje aiškinama plačiai, kaip apimanti intymias situacijas, neskelbtiną ar konfidencialią informaciją, informaciją, kuri galėtų sukelti visuomenės išankstinį nusiteikimą prieš asmenį, ir net asmens profesinio gyvenimo ir visuomenės elgesio aspektus. Tačiau vertinimo, ar yra arba buvo ribojamas „privatus gyvenimas“, rezultatas priklauso nuo kiekvienos bylos konteksto ir faktinių aplinkybių.

Priešingai, bet kokiai operacijai, susijusiai su asmens duomenų tvarkymu, galėtų būti taikomos duomenų apsaugos taisyklės, taigi ir taikoma teisė į asmens duomenų apsaugą. Pavyzdžiui, jeigu darbdavys registruoja darbuotojų vardus ir pavardes ir jiems mokamą darbo užmokestį, paprasčiausias šios informacijos registravimas negali būti laikomas kišimusi į privatų gyvenimą. Tačiau jeigu, pavyzdžiui, darbdavys perduotų trečiosioms šalims darbuotojų asmens duomenis, toks kišimasis galėtų būti ginčytinas. Darbdaviai bet kuriuo atveju privalo laikytis duomenų apsaugos taisyklių, nes informacijos apie darbuotojus registravimas laikomas duomenų tvarkymu.

Pavyzdys. Byloje *Digital Rights Ireland*[6] ESTT buvo prašoma priimti sprendimą dėl Direktyvos 2006/24/EB galiojimo atsižvelgiant į ES pagrindinių teisių chartijoje įtvirtintas pagrindines teises, susijusias su asmens duomenų apsauga ir pagarba privačiam gyvenimui. Pagal direktyvą buvo reikalaujama, kad viešai prieinamų elektroninių ryšių paslaugų teikėjai arba viešieji

6 ESTT, sujungtos bylos C-293/12 ir C-594/12, *Digital Rights Ireland Ltd prieš Minister for Communications, Marine and Natural Resources ir kt.* ir Kärntner Landesregierung ir kt. (DK), 2014 m. balandžio 8 d.

ryšių tinklai saugotų piliečių telekomunikacijų duomenis ne ilgiau kaip dvejus metus ir taip užtikrintų galimybę susipažinti su duomenimis sunkių nusikaltimų prevencijos, tyrimo ir baudžiamojo persekiojimo tikslais. Priemonė buvo susijusi tik su metaduomenimis, vietos duomenimis ir duomenimis, kurie yra būtini prenumeratoriaus arba naudotojo tapatybei nustatyti. Ji nebuvo taikoma elektroninių ryšių turiniui.

ESTT laikėsi nuomonės, kad šia direktyva buvo ribojama pagrindinė teisė į asmens duomenų apsaugą, „nes joje numatytas asmens duomenų tvarkymas“[7]. Be to, jis nustatė, kad direktyva buvo ribojama teisė į privatų gyvenimą[8]. Atsižvelgiant į duomenų visumą ir tai, kad su pagal direktyvą saugomais asmens duomenimis galėjo susipažinti kompetentingos institucijos, galėjo „būti daromos labai tikslios išvados apie asmenų, kurių duomenys saugomi, privatų gyvenimą, kaip antai kasdienio gyvenimo įpročius, nuolatinę ar laikiną gyvenamąją vietą, kasdienį ir kitokį judėjimą, vykdomą veiklą, socialinius ryšius ir lankomą socialinę aplinką“[9]. Abiejų teisių ribojimas buvo plataus masto ir ypač rimtas.

ESTT pripažino Direktyvą 2006/24/EB negaliojančia ir nustatė, kad, nepaisant jos teisėto tikslo, teisių į asmens duomenų apsaugą ir privatų gyvenimą ribojimas buvo rimtas ir nesusijęs su tuo, kas buvo griežtai būtina.

1.1.2. Tarptautinė teisinė sistema: Jungtinės Tautos

Jungtinių Tautų sistemoje asmens duomenų apsauga nepripažįstama kaip pagrindinė teisė, nors teisė į privatumą, atsižvelgiant į tarptautinę teisinę tvarką, yra nusistovėjusi pagrindinė teisė. VŽTD 12 straipsnis dėl teisės į privatų ir šeimos gyvenimą[10] buvo pirmoji tarptautinio teisės akto nuostata, kurioje buvo įtvirtinta asmens teisė į jo privatų gyvenimą ir jo apsaugą nuo kitų subjektų, ypač valstybės, kišimosi. Nors VŽTD ir yra neprivaloma deklaracija, ji turėjo ypatingą reikšmę kaip pagrindinė tarptautinės žmogaus teisių teisės priemonė ir turėjo įtakos rengiant kitus žmogaus teises reglamentuojančius teisės aktus Europoje. Tarptautinis pilietinių ir politinių teisių paktas (TPPTP) įsigaliojo 1976 m. Jame teigiama, kad niekas negali patirti savavališko arba neteisėto kišimosi į jo privatumą, būsto neliečiamybę ar susirašinėjimo

7 *Ten pat*, 36 punktas.

8 *Ten pat*, 32–35 punktai.

9 *Ten pat*, 27 punktas.

10 Jungtinės Tautos (JT), Visuotinė žmogaus teisių deklaracija (VŽTD), 1948 m. gruodžio 10 d.

konfidencialumą ir neteisėto kėsinimosi į jo garbę ir reputaciją. TPPTP yra tarptautinė sutartis, kuria 169 šalys įpareigojamos gerbti ir užtikrinti asmenų pilietinių teisių, įskaitant teisę į privatumą, įgyvendinimą.

Nuo 2013 m. Jungtinės Tautos priėmė dvi rezoliucijas privatumo klausimais pavadinimu „teisės į privatumą skaitmeniniame amžiuje“[11]; jos priimtos atsižvelgiant į naujų technologijų vystymąsi ir dėl atskleisto masinio sekimo, kuris buvo vykdomas kai kuriose valstybėse (E. Snowdeno atskleista informacija). Jose griežtai smerkiamas masinis sekimas ir atkreipiamas dėmesys į poveikį, kurį toks sekimas gali turėti pagrindinėms teisėms į privatumą ir saviraiškos laisvei, taip pat gyvybingos ir demokratinės visuomenės veikimui. Rekomendacijos, nors ir neprivalomos, paskatino svarbias tarptautines aukšto lygmens politines diskusijas dėl privatumo, naujų technologijų ir sekimo. Atsižvelgiant į šias rekomendacijas, buvo sukurta specialiojo pranešėjo teisės į privatumą klausimais pareigybė, jam pavesta skatinti ir remti šią teisę. Konkrečios pranešėjo užduotys apėmė informacijos apie nacionalinę praktiką ir patirtį, susijusią su privatumu ir naujų technologijų keliamais iššūkiais, rinkimą, keitimąsi gerąja patirtimi ir jos skatinimą ir galimų kliūčių nustatymą.

Nors ankstesnėse rezoliucijose daugiausia dėmesio buvo skiriama masinio sekimo pasekmėms ir valstybių pareigai riboti žvalgybos institucijų įgaliojimus, neseniai priimtose rezoliucijose galima įžvelgti pagrindinę diskusijų dėl privatumo Jungtinėse Tautose kryptį[12]. 2016 ir 2017 m. priimtose rezoliucijose patvirtinamas poreikis riboti žvalgybos agentūrų įgaliojimus ir smerkiamas masinis sekimas. Tačiau jose taip pat aiškiai nurodyta, kad „didėjantys įmonių gebėjimai rinkti, tvarkyti ir naudoti asmens duomenis gali kelti pavojų naudojimuisi teise į privatumą skaitmeniniame amžiuje“. Todėl rezoliucijose atkreipiamas dėmesys ne tik į valdžios institucijų, bet ir į privačiojo sektoriaus pareigą gerbti žmogaus teises, o įmonės raginamos informuoti naudotojus apie asmens duomenų rinkimą, naudojimą, dalijimąsi ir saugojimą ir nustatyti skaidrią duomenų tvarkymo politiką.

11 Žr. JT Generalinės Asamblėjos rezoliuciją dėl teisės į privatumą skaitmeniniame amžiuje, A/RES/68/167, Niujorkas, 2013 m. gruodžio 18 d., ir JT Generalinės Asamblėjos pataisytą rezoliucijos dėl teisės į privatumą skaitmeniniame amžiuje projektą, A/C.3/69/L.26/Rev.1, Niujorkas, 2014 m. lapkričio 19 d.

12 JT Generalinės Asamblėjos pataisytas rezoliucijos dėl teisės į privatumą skaitmeniniame amžiuje projektas, A/C.3/71/L.39/Rev.1, Niujorkas, 2016 m. gruodžio 16 d.; JT Žmogaus teisių taryba, „Teisė į privatumą skaitmeniniame amžiuje“, A/HRC/34/L.7/Rev.1, 2017 m. kovo 22 d.

1.1.3. Europos žmogaus teisių konvencija

Europos Taryba buvo suformuota pasibaigus Antrajam pasauliniam karui, siekiant suvienyti Europos valstybes, kad jos puoselėtų teisinės valstybės principą, demokratiją, žmogaus teises ir socialinį vystymąsi. Šiuo tikslu ji 1950 m. priėmė EŽTK, kuri įsigaliojo 1953 m.

Susitariančiosios šalys turi tarptautinę pareigą laikytis EŽTK. Visos Europos Tarybos (ET) valstybės narės dabar į savo nacionalinę teisę perkėlė arba joje įgyvendino EŽTK, kurioje reikalaujama, kad ET valstybės narės veiktų laikydamosi Konvencijos nuostatų. Susitariančiosios šalys, vykdydamos bet kokią veiklą arba įgyvendindamos įgaliojimus, privalo paisyti Konvencijoje nustatytų teisių. Tai apima nacionalinio saugumo srityje vykdomą veiklą. Svarbūs Europos Žmogaus Teisių Teismo (EŽTT) sprendimai buvo susiję su valstybės veikla opiose nacionalinio saugumo teisės ir praktikos srityse[13]. EŽTT nedvejodamas patvirtino, kad stebėjimo veikla reiškia teisės į privatų gyvenimą ribojimą[14].

Siekiant užtikrinti, kad susitariančiosios šalys laikytųsi savo įsipareigojimų pagal EŽTK, 1959 m. Strasbūre (Prancūzija) buvo sukurtas EŽTT. EŽTT, nagrinėdamas asmenų, asmenų grupių, NVO arba juridinių asmenų skundus dėl tariamų Konvencijos pažeidimų, užtikrina, kad valstybės laikytųsi savo įsipareigojimų pagal Konvenciją. EŽTT taip pat gali nagrinėti tarpvalstybines bylas, kurias viena arba daugiau ET valstybių narių iškėlė kitai valstybei narei.

Nuo 2018 m. Europos Tarybą sudaro 47 susitariančiosios šalys, iš jų 28 taip pat yra ES valstybės narės. Pareiškėjas Europos Žmogaus Teisių Teisme nebūtinai turi būti vienos iš susitariančiųjų šalių pilietis, tačiau būtina, kad tariami pažeidimai būtų padaryti vienos iš susitariančiųjų šalių jurisdikcijoje.

Teisė į asmens duomenų apsaugą yra viena iš pagal EŽTK 8 straipsnį saugomų teisių, kuria garantuojama tai, kad būtų gerbiamas privatus ir šeimos gyvenimas, būsto neliečiamybė ir susirašinėjimo slaptumas, ir kurioje nustatomos leistinos šios teisės apribojimo sąlygos[15].

13 Žr., pvz., EŽTT, *Klass ir kiti prieš Vokietiją*, Nr. 5029/71, 1978 m. rugsėjo 6 d.; EŽTT, *Rotaru prieš Rumuniją* (DK), Nr. 28341/95, 2000 m. gegužės 4 d., ir EŽTT, *Szabó ir Vissy prieš Vengriją*, Nr. 37138/14, 2016 m. sausio 12 d.

14 *Ten pat*.

15 Europos Taryba, Europos žmogaus teisių konvencija, CETS Nr. 005, 1950 m.

EŽTT išnagrinėjo daugybę situacijų, susijusių su duomenų apsaugos klausimais. Tai apima ryšių perėmimą[16], įvairias stebėjimo, vykdomo privačiajame ir viešajame sektoriuose, formas[17] ir apsaugą nuo asmens duomenų saugojimo valdžios institucijose[18]. Teisė į privatų gyvenimą nėra absoliuti teisė, nes įgyvendinant teisę į privatumą gali būti ribojamos kitos teisės, pavyzdžiui, saviraiškos laisvė ir teisė susipažinti su informacija ir atvirkščiai. Taigi EŽTT stengiasi rasti skirtingų nagrinėjamų teisių pusiausvyrą. Jis paaiškino, kad pagal EŽTK 8 straipsnį valstybės ne tik įpareigojamos susilaikyti nuo bet kokių veiksmų, kuriais gali būti pažeidžiama ši Konvencijoje nustatyta teisė, bet ir tam tikromis aplinkybėmis taip pat nustatomos pozityvios pareigos aktyviai veikti užtikrinant veiksmingą teisės į privatų ir šeimos gyvenimą apsaugą[19]. Atitinkamuose skyriuose išsamiai aprašomi daugelis šių atvejų.

1.1.4. Europos Tarybos 108-oji konvencija

XX amžiaus 7-ajame dešimtmetyje pradėjus kurti informacines technologijas, atsirado vis didesnis poreikis parengti išsamesnes taisykles, kurios padėtų apsaugoti asmenis užtikrinant jų asmens duomenų apsaugą. Iki XX amžiaus 8-ojo dešimtmečio vidurio Europos Tarybos Ministrų Komitetas priėmė įvairias rezoliucijas dėl asmens duomenų apsaugos, kuriose pateikiama nuoroda į EŽTK 8 straipsnį[20]. 1981 m. Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (108-oji konvencija)[21] buvo pateikta pasirašyti. 108-oji konvencija buvo ir išlieka vienintelis teisiškai privalomas tarptautinis teisės aktas, galiojantis duomenų apsaugos srityje.

108-oji konvencija taikoma visai duomenų tvarkymo veiklai, kuri vykdoma privačiajame ir viešajame sektoriuose, įskaitant teisminių ir teisėsaugos institucijų atliekamą

16 Žr., pvz., EŽTT, *Malone prieš Jungtinę Karalystę*, Nr. 8691/79, 1984 m. rugpjūčio 2 d.; EŽTT, *Copland prieš Jungtinę Karalystę*, Nr. 62617/00, 2007 m. balandžio 3 d., arba EŽTT, *Mustafa Sezgin Tanrıkulu prieš Turkiją*, Nr. 27473/06, 2017 m. liepos 18 d.

17 Žr., pvz., EŽTT, *Klass ir kiti prieš Vokietiją*, Nr. 5029/71, 1978 m. rugsėjo 6 d.; EŽTT, *Uzun prieš Vokietiją*, Nr. 35623/05, 2010 m. rugsėjo 2 d.

18 Žr., pvz., EŽTT, *Roman Zakharov prieš Rusiją* (DK), Nr. 47143/06, 2015 m. gruodžio 4 d.; EŽTT, *Szabó ir Vissy prieš Vengriją*, Nr. 37138/14, 2016 m. sausio 12 d.

19 Žr., pvz., EŽTT, *I prieš Suomiją*, Nr. 20511/03, 2008 m. liepos 17 d.; EŽTT, *K. U. prieš Suomiją*, Nr. 2872/02, 2008 m gruodžio 2 d.

20 Europos Taryba, Ministrų Komitetas (1973 m.), Rezoliucija (73) 22 dėl asmenų privatumo apsaugos elektroninių duomenų bankų privačiame sektoriuje atžvilgiu, 1973 m. rugsėjo 26 d.; Europos Taryba, Ministrų Komitetas (1974 m.), Rezoliucija (74) 29 dėl asmenų privatumo apsaugos elektroninių duomenų bankų viešajame sektoriuje atžvilgiu, 1974 m. rugsėjo 20 d.

21 Europos Taryba, Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu, CETS Nr. 108, 1981 m.

duomenų tvarkymą. Šia Konvencija asmenys apsaugomi nuo galimų piktnaudžiavimo atvejų, susijusių su asmens duomenų tvarkymu, ir kartu siekiama reguliuoti tarpvalstybinį asmens duomenų judėjimą. Kalbant apie asmens duomenų tvarkymą, pažymėtina, kad Konvencijoje nustatyti principai visų pirma yra susiję su sąžiningu ir teisėtu duomenų rinkimu ir automatizuotu jų tvarkymu konkrečiais teisėtais tikslais. Tai reiškia, kad duomenys neturėtų būti naudojami taip, kad būtų siekiama kitų nei nustatytieji tikslų, be to, duomenis reikėtų saugoti ne ilgiau, nei tai yra būtina. Tie principai taip pat yra susiję su duomenų kokybe, visų pirma tai reiškia, kad jie turi būti tinkami, susiję ir jų turi būti ne per daug (proporcingumo principas), taip pat jie turi būti tikslūs.

Be to, juose numatytos ne tik asmens duomenų tvarkymo garantijos ir duomenų saugumo įsipareigojimai, bet ir draudžiamas neskelbtinų duomenų, pavyzdžiui, apie asmens rasę, politines pažiūras, sveikatą, religiją, seksualinį gyvenimą arba teistumą, tvarkymas, jeigu nėra tinkamų teisinių apsaugos priemonių.

Konvencijoje taip pat įtvirtinta asmenų teisė žinoti, kokia informacija apie juos saugoma, ir prireikus ją pataisyti. Konvencijoje nustatytos teisės gali būti ribojamos tik dėl už jas viršesnių interesų, kaip antai valstybės saugumo arba gynybos. Be to, Konvencijoje numatytas laisvas asmens duomenų judėjimas tarp susitariančiųjų šalių ir joje nustatyti tam tikri valstybėms taikomi duomenų judėjimo apribojimai, jeigu teisiniu reglamentavimu neužtikrinama lygiavertė apsauga.

Reikėtų pažymėti, kad 108-ąją konvenciją ratifikavusios šalys privalo jos laikytis. EŽTT nevykdo jos teisminės priežiūros, tačiau, taikydamas EŽTK 8 straipsnį, atsižvelgia į ją savo praktikoje. Ilgainiui EŽTT konstatavo, kad asmens duomenų apsauga yra svarbi teisės į privatų gyvenimą (8 straipsnis) sudedamoji dalis, o nustatydamas, ar ši pagrindinė teisė buvo ribojama, vadovavosi 108-osios konvencijos principais[22].

Siekdamas toliau plėtoti 108-ojoje konvencijoje nustatytus bendruosius principus ir taisykles, ET Ministrų Komitetas priėmė keletą teisiškai neįpareigojančių rekomendacijų. Šios rekomendacijos turėjo įtakos kuriant duomenų apsaugos teisę Europoje. Pavyzdžiui, daugybę metų vienintelis Europos teisės aktas, kuriame buvo nustatytos asmens duomenų naudojimo policijos sektoriuje gairės, buvo Rekomendacija dėl policijos[23]. Rekomendacijoje nustatyti principai, pavyzdžiui, duomenų bylų saugojimo

22 Žr., pvz., EŽTT, *Z prieš Suomiją*, Nr. 22009/93, 1997 m. vasario 25 d.

23 Europos Taryba, Ministrų Komitetas (1987 m.), Rekomendacija *Rec(87)15* valstybėms narėms, reglamentuojanti asmens duomenų naudojimą policijos sektoriuje, Strasbūras, 1987 m. rugsėjo 17 d.

priemonės ir poreikis įgyvendinti aiškias taisykles dėl asmenų, kuriems leidžiama susipažinti su tomis bylomis, buvo reglamentuojami išsamiai ir atsispindi vėlesniuose ES teisės aktuose[24]. Neseniai parengtose rekomendacijose siekiama aptarti skaitmeninio amžiaus iššūkius, pavyzdžiui, susijusius su duomenų tvarkymu įdarbinant (žr. 9 skyrių).

108-ąją konvenciją ratifikavo visos ES valstybės narės. 1999 m. buvo pasiūlyti 108-osios konvencijos pakeitimai, kad ES galėtų tapti Konvencijos šalimi, tačiau jie niekada neįsigaliojo[25]. 2001 m. buvo priimtas 108-osios konvencijos papildomas protokolas. Jame įtvirtintos nuostatos dėl tarpvalstybinio duomenų judėjimo į Konvencijos nepasirašiusias šalis, vadinamąsias trečiąsias šalis, ir dėl privalomo nacionalinių duomenų apsaugos priežiūros institucijų sukūrimo[26].

Prie 108-osios konvencijos gali prisijungti ET nepriklausančios šalys. Konvencijos, kaip visuotinio standarto, potencialas ir jos atviras pobūdis sudaro pagrindą skatinti duomenų apsaugą pasauliniu lygmeniu. Iki šiol 108-osios konvencijos susitariančiosiomis šalimis tapo 51 valstybė. Tai yra visos Europos Tarybos valstybės narės (47 šalys); pirmoji ne Europos šalis, kuri prie Konvencijos prisijungė 2013 m. rugpjūčio mėn., – Urugvajus; taip pat Mauricijus, Senegalas ir Tunisas, kurie prisijungė 2016 ir 2017 m.

Konvencija neseniai buvo atnaujinta. 2011 m. surengtose viešose konsultacijose buvo patvirtinti du pagrindiniai šio darbo tikslai – privatumo apsaugos skaitmeninėje erdvėje didinimas ir Konvencijos laikymosi stebėsenos mechanizmo stiprinimas. Per atnaujinimo procesą daugiausia dėmesio buvo skiriama šiems uždaviniams ir jis buvo užbaigtas priėmus 108-ąją konvenciją iš dalies keičiantį protokolą (protokolas CETS Nr. 223). Darbas buvo atliktas kartu su kitomis tarptautinių duomenų apsaugą reglamentuojančių teisės aktų reformomis ir ES duomenų apsaugos taisyklių reforma, kuri buvo pradėta 2012 m. Europos Tarybos ir ES lygmens reguliavimo institucijos daugiausia dėmesio skyrė šių dviejų teisinių sistemų nuoseklumui ir suderinamumui užtikrinti. Atnaujinimas padeda išsaugoti bendrą ir lankstų Konvencijos

24 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, OL L 281, 1995 m. lapkričio 23 d.

25 Europos Taryba, Konvencijos dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu pakeitimai (ETS Nr. 108), kuriuos patvirtino Ministrų Kabinetas, Strasbūras, 1999 m. birželio 15 d.

26 Europos Taryba, Konvencijos dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu papildomas protokolas dėl priežiūros institucijų ir tarpvalstybinio duomenų judėjimo, CETS Nr. 181, 2001 m. Atnaujinus 108-ąją konvenciją, šis protokolas nebetaikomas, o jo nuostatos buvo atnaujintos ir įtrauktos į atnaujintą 108-ąją konvenciją.

pobūdį ir sustiprina jos, kaip visuotinio duomenų apsaugos teisės akto, potencialą. Joje patvirtinami ir stabilizuojami svarbūs principai ir numatomos naujos teisės fiziniams asmenims, kartu padidinant asmens duomenis tvarkančių subjektų atsakomybę ir užtikrinant didesnę atskaitomybę. Pavyzdžiui, asmenys, kurių asmens duomenys tvarkomi, turi teisę gauti žinių apie tokio duomenų tvarkymo motyvus ir teisę nesutikti su tokiu tvarkymu. Siekiant kovoti su vis dažnesniu profiliavimu internetinėje erdvėje, Konvencijoje taip pat nustatyta asmens teisė, kad dėl jo nebūtų priimami sprendimai, pagrįsti vien automatizuotu duomenų tvarkymu, neatsižvelgiant į jo nuomonę. Veiksmingas duomenų apsaugos taisyklių vykdymas, kurį užtikrina nepriklausomos priežiūros institucijos susitariančiosiose šalyse, laikomas esminiu Konvencijos praktinio įgyvendinimo aspektu. Šiuo tikslu atnaujintoje Konvencijoje pabrėžiamas poreikis priežiūros institucijoms suteikti veiksmingus įgaliojimus ir funkcijas, kad jos, vykdydamos savo misiją, galėtų būti iš tikrųjų nepriklausomos.

1.1.5. Europos Sąjungos duomenų apsaugos teisė

ES teisę sudaro pirminė ir antrinė ES teisė. Sutartis, t. y. Europos Sąjungos sutartį (ES sutartis) ir Sutartį dėl Europos Sąjungos veikimo (SESV), ratifikavo visos ES valstybės narės; šios Sutartys sudaro „pirminę ES teisę“. ES reglamentus, direktyvas ir sprendimus priima ES institucijos, kurioms tokie įgaliojimai suteikti pagal Sutartis; šie teisės aktai sudaro „antrinę ES teisę“.

Duomenų apsauga pagal pirminę ES teisę

Pirminėse Europos Bendrijų sutartyse nebuvo jokių nuorodų į žmogaus teises arba jų apsaugą, nes Europos ekonominė bendrija iš pradžių buvo sukurta kaip regioninė organizacija, orientuota į ekonomikos integraciją ir bendrosios rinkos sukūrimą. Pagrindinis principas, kuriuo grindžiamas Europos Bendrijų kūrimas ir vystymas ir kuris lygiai taip pat galioja šiandien, yra kompetencijos suteikimo principas. Remiantis šiuo principu, ES veikia tik neperžengdama valstybių narių jai suteiktos kompetencijos, kuri nustatyta ES sutartyse. Priešingai nei Europos Taryboje, ES sutartyse nenumatyta aiški kompetencija pagrindinių teisių klausimais.

Kadangi ESTT buvo perduotos bylos dėl tariamų žmogaus teisių pažeidimų srityse, kurioms taikoma ES teisė, jis pateikė svarbių Sutarčių išaiškinimų. Siekdamas suteikti apsaugą asmenims, ESTT pagrindines teises įtraukė į vadinamuosius Europos teisės bendruosius principus. Pasak ESTT, šiuose bendruosiuose principuose atsispindi žmogaus teisių apsaugos turinys, kuris randamas nacionalinėse konstitucijose ir

žmogaus teisių sutartyse, visų pirma EŽTK. ESTT nurodė, kad jis užtikrins ES teisės atitiktį šiems principams.

Pripažindama, kad jos politika galėtų turėti poveikį žmogaus teisėms ir pastangoms užtikrinti, kad piliečiai jaustų „glaudesnį“ ryšį su ES, 2000 m. ES paskelbė Europos Sąjungos pagrindinių teisių chartiją (Chartija). Joje numatytos pačios įvairiausios pilietinės, politinės, ekonominės ir socialinės Europos piliečių teisės, kurių pagrindą sudaro apibendrintos valstybių narių konstitucinės tradicijos ir joms bendri tarptautiniai įsipareigojimai. Chartijoje teisės aprašomos šešiuose skirsniuose: orumas, laisvės, lygybė, solidarumas, pilietinės teisės ir teisingumas.

Chartija, kuri iš pradžių buvo politinis dokumentas, tapo teisiškai privalomu[27] ES pirminės teisės aktu (žr. ES sutarties 6 straipsnio 1 dalį) 2009 m. gruodžio 1 d. įsigaliojus Lisabonos sutarčiai[28]. Chartijos nuostatos yra skirtos ES institucijoms ir įstaigoms, kurios, vykdydamos savo pareigas, privalo gerbti Chartijoje įtvirtintas teises. Chartijos nuostatos valstybėms narėms taip pat yra privalomos tais atvejais, kai jos įgyvendina ES teisę.

Chartijoje ne tik garantuojama teisė į privatų ir šeimos gyvenimą (7 straipsnis), bet ir nustatoma teisė į asmens duomenų apsaugą (8 straipsnis). Chartijoje aiškiai numatyta, kad teisė į tokią apsaugą turi būti ginama ne mažesniu lygiu nei pagrindinės teisės pagal ES teisę. ES institucijos ir įstaigos, kaip ir valstybės narės, įgyvendindamos Sąjungos teisę, privalo garantuoti ir gerbti šią teisę (Chartijos 51 straipsnis). Chartijos 8 straipsnis, kuris buvo suformuluotas praėjus keleriems metams nuo Duomenų apsaugos direktyvos priėmimo, turi būti suprantamas kaip apimantis iki tol galiojusią ES duomenų apsaugos teisę. Todėl Chartijos 8 straipsnio 1 dalyje ne tik aiškiai minima teisė į duomenų apsaugą, bet ir 8 straipsnio 2 dalyje pateikiama nuoroda į pagrindinius duomenų apsaugos principus. Galiausiai pagal Chartijos 8 straipsnio 3 dalį reikalaujama, kad nepriklausoma institucija kontroliuotų šių principų įgyvendinimą.

Lisabonos sutarties priėmimas yra svarbus įvykis plėtojant duomenų apsaugos teisę ir ja ne tik sustiprinamas Chartijos kaip privalomo pirminės teisės lygmens teisinio dokumento statusas, bet ir numatoma teisė į asmens duomenų apsaugą. Ši teisė yra konkrečiai nustatyta SESV 16 straipsnyje, t. y. toje Sutarties dalyje, kurioje aptariami ES bendrieji principai. 16 straipsnyje taip pat sukuriamas naujas teisinis pagrindas,

27 ES (2012 m.), Europos Sąjungos pagrindinių teisių chartija, OL C 326, 2012.

28 Žr. Europos Bendrijų (2012 m.), Europos Sąjungos sutarties, OL C 326, 2012, ir Europos Bendrijų (2012 m.), SESV, OL C 326, 2012, suvestines redakcijas.

kuriuo ES suteikiama kompetencija priimti teisės aktus duomenų apsaugos klausimais. Tai yra svarbus pokytis, nes ES duomenų apsaugos taisyklės, visų pirma Duomenų apsaugos direktyva, iš pradžių buvo pagrįstos vidaus rinkos teisiniu pagrindu ir poreikiu suderinti nacionalinius įstatymus, kad nebūtų varžomas laisvas duomenų judėjimas ES. Dabar SESV 16 straipsnyje nustatytas nepriklausomas šiuolaikinio ir išsamaus požiūrio į duomenų apsaugą pagrindas, kuris apima visus ES kompetencijai priklausančius klausimus, įskaitant policijos ir teisminį bendradarbiavimą baudžiamosiose bylose. SESV 16 straipsnyje taip pat patvirtinama, kad pagal jį priimtų duomenų apsaugos taisyklių laikymąsi privalo kontroliuoti nepriklausomos priežiūros institucijos. 16 straipsnis buvo naudojamas kaip teisinis pagrindas 2016 m. patvirtinant išsamią duomenų apsaugos taisyklių reformą, t. y. Bendrąjį duomenų apsaugos reglamentą ir Duomenų apsaugos policijos ir baudžiamosios teisenos institucijoms tvarkant asmens duomenis direktyvą (žr. toliau).

Bendrasis duomenų apsaugos reglamentas

Nuo 1995 m. iki 2018 m. gegužės mėn. pagrindinis ES duomenų apsaugos teisės aktas buvo 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva 95/46/EB dėl asmenų apsaugos Bendrijos institucijoms ir įstaigoms tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo (Duomenų apsaugos direktyva)[29]. Ji buvo priimta 1995 m., kai keletas valstybių narių jau buvo priėmusios nacionalinius duomenų apsaugos įstatymus[30], atsižvelgiant į poreikį suderinti šiuos įstatymus ir taip užtikrinti aukštą apsaugos lygį ir laisvą asmens duomenų judėjimą tarp įvairių valstybių narių. Laisvam prekių, kapitalo, paslaugų ir žmonių judėjimui vidaus rinkoje buvo reikalingas laisvas duomenų judėjimas, kurio nebuvo galima užtikrinti tol, kol valstybės narės negalėjo remtis vienoda aukšto lygio duomenų apsauga.

Duomenų apsaugos direktyvoje atsispindėjo duomenų apsaugos principai, kurie jau buvo nustatyti nacionaliniuose įstatymuose ir 108-ojoje konvencijoje, be to, jie dažnai buvo reglamentuojami išsamiau. Joje buvo numatyta 108-osios konvencijos 11 straipsnyje įtvirtinta galimybė papildyti apsaugos teisės aktus. Visų pirma direktyvoje numatyta nuostata dėl nepriklausomos priežiūros, kuria buvo siekiama pagerinti duomenų apsaugos taisyklių laikymąsi, iš tikrųjų buvo svarbi didinant

29 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (Duomenų apsaugos direktyva), OL L 281, 1995.

30 1970 m. Vokietijos Heseno žemė priėmė pirmąjį įstatymą dėl duomenų apsaugos, kuris buvo taikomas tik šioje žemėje. Švedija *Datalagen* priėmė 1973 m.; Vokietija *Bundesdatenschutzgestez* priėmė 1976 m., o Prancūzija *Loi relatif à l'informatique, aux fichiers et aux libertés* priėmė 1977 m. Jungtinėje Karalystėje Duomenų apsaugos aktas buvo priimtas 1984 m. Galiausiai Nyderlandai *Wet Persoonregistraties* priėmė 1989 m.

veiksmingą Europos duomenų apsaugos teisės veikimą. Todėl ši nuostata 2001 m. buvo įtraukta į ET teisę priimant 108-osios konvencijos papildomą protokolą. Tai parodo glaudžią abiejų teisės aktų sąveiką ir teigiamą įtaką vienas kitam per daugybę metų.

Duomenų apsaugos direktyvoje buvo nustatyta išsami ir visapusiška ES duomenų apsaugos sistema. Tačiau pagal ES teisinę sistemą direktyvos tiesiogiai netaikomos ir jos turi būti perkeltos į valstybių narių nacionalinę teisę. Neišvengiama, kad valstybės narės, perkeldamos į nacionalinę teisę direktyvos nuostatas, turi tam tikrą diskrecijos teisę. Nors direktyva buvo siekiama užtikrinti visišką suderinamumą[31] (ir visišką apsaugos lygį), praktikoje valstybės narės ją į nacionalinę teisę perkėlė skirtingai. Todėl ES buvo nustatytos skirtingos duomenų apsaugos taisyklės, o nacionaliniuose įstatymuose apibrėžtys ir taisyklės buvo aiškinamos nevienodai. Vykdymo užtikrinimo lygis ir sankcijų griežtumas valstybėse narėse taip pat buvo nevienodas. Galiausiai nuo XX amžiaus 10-ojo dešimtmečio, kai buvo parengta direktyva, gerokai pasikeitė informacinės technologijos. Apskritai šios priežastys paskatino imtis ES duomenų apsaugos teisės aktų reformos.

Po daugybę metų trukusių intensyvių diskusijų ir įgyvendinus reformą, 2016 m. balandžio mėn. buvo priimtas Bendrasis duomenų apsaugos reglamentas. Diskusijos dėl poreikio atnaujinti ES duomenų apsaugos taisykles prasidėjo 2009 m., kai Komisija pradėjo viešas konsultacijas dėl būsimos pagrindinės teisės į asmens duomenų apsaugą teisinės sistemos. Pasiūlymą dėl reglamento Komisija paskelbė 2012 m. sausio mėn. ir taip pradėjo ilgą Europos Parlamento ir ES Tarybos derybų procesą vykdant teisėkūros procedūrą. Priimtame Bendrajame duomenų apsaugos reglamente buvo numatytas dvejų metų pereinamasis laikotarpis. Jis visapusiškai pradėtas taikyti 2018 m. gegužės 25 d., kai buvo panaikinta Duomenų apsaugos direktyva.

2016 m. priėmus Bendrąjį duomenų apsaugos reglamentą, buvo atnaujinti ES duomenų apsaugos teisės aktai, kad jais būtų galima apsaugoti pagrindines teises atsižvelgiant į skaitmeninio amžiaus ekonominius ir socialinius iššūkius. BDAR išsaugomi ir plėtojami Duomenų apsaugos direktyvoje nustatyti pagrindiniai principai ir duomenų subjekto teisės. Be to, jame nustatytos naujos prievolės, pagal kurias reikalaujama, kad organizacijos įgyvendintų pritaikytąją ir standartizuotąją duomenų apsaugą; tam tikromis aplinkybėmis paskirtų duomenų apsaugos pareigūną;

31 ESTT, sujungtos bylos C-468/10 ir C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) ir Federación de Comercio Electrónico y Marketing Directo (FECEMD) prieš Administración del Estado*, 2011 m. lapkričio 24 d., 29 punktas.

paisytų naujos teisės į duomenų perkeliamumą ir laikytųsi atskaitomybės principo. Pagal ES teisę, reglamentai yra taikomi tiesiogiai; nėra jokio poreikio juos įgyvendinti nacionaliniu lygmeniu. Todėl Bendrajame duomenų apsaugos reglamente nustatytas bendras ES galiojančių duomenų apsaugos taisyklių rinkinys. Taip nustatomos nuoseklios duomenų apsaugos taisyklės visoje ES ir sukuriama teisiniu tikrumu grindžiama aplinka, kuri gali būti naudinga ekonominės veiklos vykdytojams ir asmenims, kurie yra „duomenų subjektai".

Vis dėlto, nepaisant to, kad Bendrasis duomenų apsaugos reglamentas yra tiesiogiai taikomas, tikimasi, kad valstybės narės atnaujins savo galiojančius nacionalinius duomenų apsaugos įstatymus, kad jie būtų visiškai suderinti su reglamentu, ir kartu atsižvelgs į 10 konstatuojamojoje dalyje suteiktą diskrecijos teisę, susijusią su konkrečiomis nuostatomis. Reglamente nustatytos pagrindinės taisyklės ir principai, taip pat tvirtos teisės, kurios asmenims suteikiamos reglamentu, sudaro nemažą vadovo turinio dalį ir yra aptariamos kituose skyriuose. Reglamente nustatytos išsamios teritorinės taikymo srities taisyklės. Jis taikomas ES įsteigtoms įmonėms ir ne ES įsisteigusiems duomenų valdytojams ir duomenų tvarkytojams, kurie ES duomenų subjektams siūlo prekes arba paslaugas arba stebi jų elgesį. Keletas užsienio technologijų įmonių užima didelę Europos rinkos dalį ir turi milijonus ES klientų, dėl kurių šioms organizacijoms taikomos ES duomenų apsaugos taisyklės, todėl svarbu užtikrinti asmenų apsaugą ir sudaryti vienodas veiklos sąlygas.

Duomenų apsauga teisėsaugos srityje – Direktyva (ES) 2016/680

Panaikintoje Duomenų apsaugos direktyvoje buvo nustatyta išsami duomenų apsaugos tvarka. Ši tvarka dabar dar labiau sugriežtinta priėmus Bendrąjį duomenų apsaugos reglamentą. Panaikinta Duomenų apsaugos direktyva buvo išsami, tačiau ji taikyta tik vidaus rinkoje vykdomai veiklai ir valdžios institucijų, išskyrus teisėsaugos institucijas, veiklai. Todėl siekiant reikalingo aiškumo ir duomenų apsaugos ir kitų teisėtų interesų pusiausvyros, taip pat išspręsti uždavinius, kurie yra ypač aktualūs konkrečiuose sektoriuose, reikėjo priimti specialius teisės aktus. Tai galima pasakyti apie taisykles, kuriomis reglamentuojamas teisėsaugos institucijų vykdomas asmens duomenų tvarkymas.

Pirmas ES teisės aktas, kuriame buvo reglamentuojamas šis klausimas, buvo Tarybos pamatinis sprendimas 2008/977/TVR dėl asmens duomenų, tvarkomų vykdant policijos ir teisminį bendradarbiavimą baudžiamosiose bylose, apsaugos. Jame nustatytos taisyklės buvo taikomos tik policijos ir teisminiams duomenims, kuriais

buvo keičiamasi tarp valstybių narių. Sprendimas nebuvo taikomas teisėsaugos institucijų vykdomam asmens duomenų tvarkymui vidaus reikmėms.

Ši padėtis buvo ištaisyta priėmus Direktyvą (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo[32], kuri vadinama Duomenų apsaugos policijos ir baudžiamosios teisenos institucijoms tvarkant asmens duomenis direktyva. Direktyva, kuri buvo priimta kartu su Bendruoju duomenų apsaugos reglamentu, buvo panaikintas Pamatinis sprendimas 2008/977/TVR ir nustatyta išsami asmens duomenų apsaugos sistema, galiojanti teisėsaugos srityje, be to, joje buvo pripažįstami su visuomenės saugumu susijusio duomenų tvarkymo ypatumai. Nors Bendrajame duomenų apsaugos reglamente nustatytos bendrosios taisyklės, kuriomis užtikrinama asmenų apsauga atsižvelgiant į jų asmens duomenų tvarkymą, ir užtikrinamas laisvas tokių duomenų judėjimas ES, tačiau direktyvoje įtvirtintos konkrečios duomenų apsaugos taisyklės, galiojančios teisminio bendradarbiavimo baudžiamosiose bylose ir policijos bendradarbiavimo srityse. Jeigu kompetentinga institucija tvarko asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas tikslais, bus taikoma Direktyva (ES) 2016/680. Jeigu kompetentingos institucijos asmens duomenis tvarko kitais nei pirmiau minėti tikslais, taikoma bendra tvarka pagal Bendrąjį duomenų apsaugos reglamentą. Direktyva (ES) 2016/680, kitaip nei prieš ją galiojęs Tarybos pamatinis sprendimas 2008/977/TVR, taip pat taikoma ir nacionaliniam asmens duomenų tvarkymui, kurį vykdo teisėsaugos institucijos ir kuris neapima tik keitimosi tokiais duomenimis tarp valstybių narių. Be to, direktyva siekiama nustatyti asmenų teisių ir teisėtų tikslų, susijusių su duomenų tvarkymu saugumo tikslais, pusiausvyrą.

Šiuo tikslu direktyvoje patvirtinama teisė į asmens duomenų apsaugą ir pagrindiniai principai, kurie turėtų apimti duomenų tvarkymą, kartu atidžiai stebint, kaip laikomasi Bendrajame duomenų apsaugos reglamente nustatytų taisyklių ir principų. Asmenų teisės ir duomenų valdytojams nustatytos prievolės, pavyzdžiui, susijusios su duomenų saugumu, pritaikytąja ir standartizuotąja duomenų apsauga ir pranešimais apie asmens duomenų saugumo pažeidimus, yra panašios į Bendrajame duomenų apsaugos reglamente nustatytas teises ir prievoles. Direktyvoje taip pat

32 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, OL L 119, 2016 m. gegužės 4 d.

atsižvelgiama ir bandoma aptarti rimtus naujus technologinius uždavinius, kurie gali turėti ypač neigiamą poveikį asmenims, pavyzdžiui, profiliavimo metodų naudojimas teisėsaugos institucijose. Iš esmės vien automatizuotu duomenų tvarkymu, įskaitant profiliavimą, pagrįsti sprendimai turi būti draudžiami[33]. Be to, jie negali būti grindžiami neskelbtinais duomenimis. Tokiems principams taikomos tam tikros direktyvoje nustatytos išimtys. Be to, dėl tokio duomenų tvarkymo negali būti diskriminuojamas kuris nors asmuo[34].

Direktyvoje taip pat nustatytos taisyklės, kuriomis užtikrinama duomenų valdytojų atskaitomybė. Jie privalo paskirti duomenų apsaugos pareigūną, kuris kontroliuotų, kaip laikomasi duomenų apsaugos taisyklių, informuotų duomenų tvarkymą vykdančius subjektus ir darbuotojus apie jų prievoles ir jiems teiktų konsultacijas, taip pat bendradarbiautų su priežiūros institucija. Dabar nepriklausomos priežiūros institucijos prižiūri, kaip asmens duomenys tvarkomi policijos ir baudžiamosios teisenos sektoriuje. Tiek bendroji duomenų apsaugos teisinė sistema, tiek specialioji duomenų apsaugos sistema, kuri taikoma teisėsaugos ir baudžiamųjų bylų srityje, privalo atitikti ES pagrindinių teisių chartijos reikalavimus.

Specialioji duomenų tvarkymo vykstant policijos ir teisminiam bendradarbiavimui tvarka, nustatyta Duomenų apsaugos policijos ir baudžiamosios teisenos institucijoms tvarkant asmens duomenis direktyvoje, išsamiai aprašyta 8 skyriuje.

Direktyva dėl privatumo ir elektroninių ryšių

Buvo manoma, kad taip pat būtina nustatyti specialias duomenų apsaugos taisykles, kurios galiotų elektroninių ryšių sektoriuje. Plėtojant internetą, fiksuotojo ir judriojo ryšio telefoniją, svarbu užtikrinti, kad būtų gerbiamos vartotojų teisės į privatumą ir konfidencialumą. Direktyvoje 2002/58/EB[35] dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių, arba E. privatumo direktyva) nustatytos taisyklės, kuriomis reglamentuojamas asmens duomenų saugumas šiuose tinkluose, pranešimas apie asmens duomenų saugumo pažeidimus ir ryšių konfidencialumas.

33 Duomenų apsaugos policijos ir baudžiamosios teisenos institucijoms tvarkant asmens duomenis direktyva, 11 straipsnio 1 dalis.

34 *Ten pat*, 11 straipsnio 2 ir 3 dalys.

35 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių), OL L 201.

Saugumo požiūriu elektroninių ryšių paslaugų operatoriai, be kita ko, privalo užtikrinti, kad su asmens duomenimis galėtų susipažinti tik įgalioti asmenys, ir imtis priemonių siekdami užkirsti kelią tam, kad asmens duomenys būtų sunaikinti, prarasti arba atsitiktinai sugadinti[36]. Jeigu yra konkreti rizika, kad bus pažeistas viešojo ryšių tinklo saugumas, operatoriai privalo informuoti abonentus apie šį pavojų[37]. Jeigu, nepaisant įgyvendintų saugumo priemonių, nustatomas saugumo pažeidimas, operatoriai privalo apie asmens duomenų saugumo pažeidimą informuoti kompetentingą nacionalinę instituciją, kuriai pavesta įgyvendinti direktyvą ir užtikrinti jos vykdymą. Kartais reikalaujama, kad operatoriai apie asmens duomenų saugumo pažeidimus taip pat praneštų asmenims; tai daroma būtent tais atvejais, kai tikėtina, kad pažeidimas darys neigiamą poveikį asmens duomenims arba privatumui[38]. Pagal ryšių konfidencialumo principą reikalaujama, kad iš esmės būtų draudžiama klausytis, slapta klausytis, saugoti arba kitaip sekti ar perimti ryšius ir metaduomenis. Pagal direktyvą taip pat draudžiami neužsakyti pranešimai (dažnai vadinami brukalais), išskyrus atvejus, kai naudotojai davė sutikimą, ir joje taip pat nustatytos slapukų saugojimo kompiuteriuose ir prietaisuose taisyklės. Iš šių pagrindinių neigiamų prievolių aiškiai matyti, kad ryšių konfidencialumas yra gana glaudžiai susijęs su Chartijos 7 straipsnyje nustatytos teisės į privatų gyvenimą ir Chartijos 8 straipsnyje nustatytos teisės į asmens duomenų apsaugą apsauga.

2017 m. sausio 1 d. Komisija paskelbė reglamento dėl teisės į privatų gyvenimą ir asmens duomenų apsaugos elektroninių ryšių sektoriuje pasiūlymą, kuriuo buvo siekiama panaikinti E. privatumo direktyvą. Reforma siekiama elektroninius ryšius reglamentuojančias taisykles suderinti su nauja duomenų apsaugos sistema, nustatyta Bendrajame duomenų apsaugos reglamente. Naujasis reglamentas bus tiesiogiai taikomas visoje ES; visiems asmenims bus užtikrinama vienoda jų elektroninių ryšių apsauga, o telekomunikacijos operatoriams ir įmonėms bus naudingas aiškumas, teisinis tikrumas ir bendras visoje ES galiojančių taisyklių rinkinys. Pasiūlytos elektroninių ryšių konfidencialumo taisyklės taip pat bus taikomos naujiems dalyviams, teikiantiems elektroninių ryšių paslaugas, kurioms netaikoma E. privatumo direktyva. Pastaroji buvo taikoma tik įprastiems telekomunikacijų paslaugų teikėjams. Atsižvelgiant į masinį tokių pranešimų siuntimo ar skambinimo paslaugų kaip *Skype*, *WhatsApp*, *Facebook Messenger* ir *Viber* naudojimą, pažymėtina, kad šioms virštinklinėms (angl. *over-the-top*, OTT) paslaugoms dabar taikomas reglamentas ir jos turės atitikti jame nustatytus duomenų apsaugos, privatumo ir saugumo

36 Direktyvos dėl privatumo ir elektroninių ryšių 4 straipsnio 1 punktas.

37 *Ten pat*, 4 straipsnio 2 punktas.

38 *Ten pat*, 4 straipsnio 3 punktas.

reikalavimus. Tuo metu, kai buvo paskelbtas šis vadovas, teisėkūros procesas dėl e. privatumo taisyklių tebevyko.

Reglamentas (EB) Nr. 45/2001

Kadangi Duomenų apsaugos direktyva galėjo būti taikoma tik ES valstybėms narėms, siekiant užtikrinti duomenų apsaugą ES institucijoms ir įstaigoms tvarkant duomenis, reikėjo priimti papildomą teisės aktą. Ši užduotis įvykdyta priėmus Reglamentą (EB) Nr. 45/2001 dėl asmenų apsaugos Bendrijos institucijoms ir įstaigoms tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo (ES institucijų duomenų apsaugos reglamentas)[39].

Reglamente (EB) Nr. 45/2001 atidžiai laikomasi bendros ES duomenų apsaugos sistemos principų ir tie principai taikomi duomenų tvarkymui, kurį ES institucijos ir įstaigos atlieka vykdydamos savo funkcijas. Be to, juo įsteigiama nepriklausoma priežiūros institucija – Europos duomenų apsaugos priežiūros pareigūnas, kuris stebi, kaip taikomos reglamento nuostatos. EDAPP suteikti priežiūros įgaliojimai ir nustatyta pareiga stebėti, kaip ES institucijose ir įstaigose tvarkomi asmens duomenys, taip pat nagrinėti ir tirti skundus dėl tariamų duomenų apsaugos taisyklių pažeidimų. Jis taip pat pataria ES institucijoms ir įstaigoms visais klausimais, susijusiais su asmens duomenų apsauga, pradedant pasiūlymų dėl naujų teisės aktų teikimu, baigiant nacionalinių taisyklių, susijusių su duomenų tvarkymu, rengimu.

2017 m. sausio mėn. Europos Komisija pateikė naujo reglamento dėl duomenų tvarkymo ES institucijose pasiūlymą, kuriuo bus panaikintas dabartinis reglamentas. Kaip ir iš dalies keičiant E. privatumo direktyvą, taip ir iš dalies pakeitus Reglamentą (EB) Nr. 45/2001, jame nustatytos taisyklės bus atnaujintos ir suderintos su nauja Bendrajame duomenų apsaugos reglamente nustatyta duomenų apsaugos sistema.

ESTT vaidmuo

ESTT turi jurisdikciją nuspręsti, ar valstybė narė įvykdė savo prievoles pagal ES duomenų apsaugos teisę, ir, aiškindamas ES teisės aktus, turi užtikrinti veiksmingą ir vienodą jų taikymą visose valstybėse narėse. Nuo Duomenų apsaugos direktyvos priėmimo 1995 m. susikaupė nemažai jurisprudencijos, kurioje aiškinama duomenų apsaugos principų ir pagrindinės teisės į asmens duomenų apsaugą, kaip nustatyta Chartijos 8 straipsnyje, taikymo sritis ir reikšmė. Nepaisant to, kad direktyva

39 2000 m. gruodžio 18 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 45/2001 dėl asmenų apsaugos Bendrijos institucijoms ir įstaigoms tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo, OL L 8, 2001.

panaikinta ir dabar galioja naujas teisės aktas, t. y. Bendrasis duomenų apsaugos reglamentas, iki tol suformuota teismų praktika išlieka svarbi ir galioja aiškinant bei taikant ES duomenų apsaugos principus tiek, kiek Bendrajame duomenų apsaugos reglamente išlaikyti pagrindiniai Duomenų apsaugos direktyvos principai ir koncepcijos.

1.2. Teisės į asmens duomenų apsaugą apribojimai

Pagrindiniai faktai

- Teisė į asmens duomenų apsaugą nėra absoliuti teisė; prireikus ji gali būti ribojama atsižvelgiant į objektyvų bendrąjį interesą arba siekiant apsaugoti kitų asmenų teises ir laisves.
- Teisių į privatų gyvenimą ir asmens duomenų apsaugą ribojimo sąlygų sąrašai pateikti EŽTK 8 straipsnyje ir Chartijos 52 straipsnio 1 dalyje. Jie parengti ir aiškinami remiantis EŽTT ir ESTT praktika.
- Pagal ET duomenų apsaugos teisę asmens duomenų tvarkymas reiškia teisėtą teisės į privatų gyvenimą ribojimą ir gali būti vykdomas, jeigu:
  - toks tvarkymas atitinka teisės aktus;
  - juo siekiama teisėto tikslo;
  - taip tvarkant duomenis gerbiama pagrindinių teisių ir laisvių esmė;
  - toks tvarkymas yra būtinas ir proporcingas demokratinėje visuomenėje siekiant teisėto tikslo.
- Pagal ES teisinę tvarką pagrindinių teisių, kurių apsauga užtikrinama Chartijoje, įgyvendinimo apribojimams taikomos panašios sąlygos. Bet koks bet kurios pagrindinės teisės, įskaitant asmens duomenų apsaugą, apribojimas gali būti teisėtas, tik jeigu:
  - toks tvarkymas atitinka teisės aktus;
  - taip tvarkant duomenis gerbiama teisės esmė;
  - toks tvarkymas yra būtinas ir laikomasi proporcingumo principo, ir
  - taip tvarkant duomenis siekiama bendrąjį interesą atitinkančio tikslo, kurį pripažino ES, arba patenkinti poreikį apsaugoti kitų asmenų teises.

Chartijos 8 straipsnyje nustatyta pagrindinė teisė į asmens duomenų apsaugą nėra absoliuti teisė „ir turi būti vertinama atsižvelgiant į jos socialinį tikslą“[40]. Todėl Chartijos 52 straipsnio 1 dalyje pripažįstama, kad teisių, kurios, pavyzdžiui, nustatytos Chartijos 7 ir 8 straipsniuose, įgyvendinimui gali būti nustatyti apribojimai, jeigu jie yra numatyti teisės akte, jais gerbiama šių teisių ir laisvių esmė ir jeigu jie, atsižvelgiant į proporcingumo principą, yra būtini ir iš tikrųjų atitinka ES pripažįstamus bendrojo intereso tikslus arba poreikį apsaugoti kitų asmenų teises ir laisves[41]. Panašiai EŽTK sistemoje duomenų apsauga garantuojama 8 straipsnyje ir tos teisės įgyvendinimas gali būti ribojamas, jei tai yra būtina siekiant teisėto tikslo. Šiame skirsnyje nurodomos apribojimo pagal EŽTK sąlygos, atsižvelgiant į tai, kaip jos išaiškintos EŽTT praktikoje, taip pat teisėtų apribojimų pagal Chartijos 52 straipsnį sąlygos.

1.2.1. Reikalavimai pagrįstam apribojimui pagal EŽTK

Asmens duomenų tvarkymas gali reikšti duomenų subjekto teisės į privatų gyvenimą, kuri saugoma pagal EŽTK 8 straipsnį, ribojimą[42]. Kaip paaiškinta pirmiau (žr. 1.1.1 skirsnį ir 1.1.4 skirsnį), priešingai nei pagal ES teisinę tvarką, EŽTK nepatvirtinama, kad asmens duomenų apsauga yra atskira pagrindinė teisė. Asmens duomenų apsauga veikiau sudaro dalį teisių, kurios saugomos kartu su teise į privatų gyvenimą. Taigi ne kiekviena operacija, susijusi su asmens duomenų tvarkymu, patenka į EŽTK 8 straipsnio taikymo sritį. Kad 8 straipsnis būtų taikomas, pirmiausia reikia nustatyti, ar buvo pažeistas privatus interesas arba asmens privatus gyvenimas. Savo praktikoje EŽTT sąvoką „privatus gyvenimas“ aiškino plačiai ir įtraukė net su profesiniu gyvenimu ir viešu elgesiu susijusius aspektus. Jis taip pat nusprendė, kad asmens duomenų apsauga yra svarbi teisės į privatų gyvenimą dalis. Tačiau nepaisant plataus sąvokos „privatus gyvenimas“ aiškinimo, ne visų rūšių duomenų tvarkymas *per se* reikštų pagal 8 straipsnį saugomų teisių pažeidimą.

Jeigu EŽTT mano, kad nagrinėjama duomenų tvarkymo operacija daro poveikį asmenų teisei į privatų gyvenimą, jis išnagrinės, ar ribojimas yra pateisinamas. Teisė į privatų gyvenimą nėra absoliuti teisė, tačiau ji turi būti subalansuota ir suderinta su kitais teisėtais interesais ir teisėmis, nepaisant to, ar tai kitų asmenų (privatūs interesai), ar visos visuomenės (viešieji interesai) interesai ir teisės.

40 Žr., pvz., ESTT, sujungtos bylos C-92/09 ir C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert prieš Land Hessen* (DK), 2010 m. lapkričio 8 d., 48 punktas.

41 *Ten pat*, 50 punktas.

42 EŽTT, *S. ir Marper prieš Jungtinę Karalystę* (DK), Nr. 30562/04 ir 30566/04, 2008 m. gruodžio 8 d., 67 punktas.

Toliau išvardijamos sąlygos, kurias visas įvykdžius, galima pateisinti apribojimą.

Apribojimas atitinka teisės aktus

Remiantis EŽTT praktika, ribojimas atitinka teisės aktus, jeigu jis yra pagrįstas tam tikrus požymius turinčio nacionalinio teisės akto nuostata. Teisės aktas turi būti „prieinamas atitinkamiems asmenims ir turi būti įmanoma numatyti jo padarinius“[43]. Taisyklė yra numatoma „jeigu ji yra pakankamai tiksliai suformuluota, kad bet kuris asmuo, jei reikalinga, gavęs tinkamą konsultaciją, galėtų atitinkamai elgtis“[44]. Be to, „šiuo atveju reikalaujamas „teisės akto“ tikslumo laipsnis priklausys nuo konkretaus dalyko“[45].

Pavyzdžiai. Byloje *Rotaru prieš Rumuniją*[46] pareiškėjas teigė, kad buvo pažeista jo teisė į privatų gyvenimą, nes Rumunijos žvalgybos tarnyba turėjo ir naudojo bylą, kurioje buvo jo asmens duomenys. EŽTT nusprendė, kad nors pagal nacionalinį teisės aktą buvo leidžiama rinkti, įrašyti ir slaptose bylose archyvuoti nacionaliniam saugumui įtakos turinčius duomenis, jame nebuvo nustatytos kokios nors naudojimosi šiais įgaliojimais ribos, kuriuos institucijos nustatydavo savo nuožiūra. Pavyzdžiui, nacionaliniame teisės akte nebuvo apibrėžta duomenų, kuriuos būtų galima tvarkyti, rūšis, asmenų, kurių atžvilgiu būtų galima imtis sekimo priemonių, kategorijos, aplinkybės, kuriomis tokių priemonių būtų galima imtis, arba taikytina procedūra. Todėl EŽTT padarė išvadą, kad nacionalinės teisės aktas neatitiko EŽTT 8 straipsnyje nustatyto nuspėjamumo reikalavimo, todėl šis straipsnis buvo pažeistas.

43 EŽTT, *Amann prieš Šveicariją* (DK), Nr. 27798/95, 2000 m. vasario 16 d., 50 punktas; taip pat žr. EŽTT, *Kopp prieš Šveicariją*, Nr. 23224/94, 1998 m. kovo 25 d., 55 punktas, ir EŽTT, *Iordachi ir kiti prieš Moldovą*, Nr. 25198/02, 2009 m. vasario 10 d., 50 punktas.

44 EŽTT, *Amann prieš Šveicariją* (DK), Nr. 27798/95, 2000 m. vasario 16 d., 56 punktas; taip pat žr. EŽTT, *Malone prieš Jungtinę Karalystę*, Nr. 8691/79, 1984 m. rugpjūčio 2 d., 66 punktas; EŽTT, *Silver ir kiti prieš Jungtinę Karalystę*, Nr. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 1983 m. kovo 25 d., 88 punktas.

45 EŽTT, *The Sunday Times prieš Jungtinę Karalystę*, Nr. 6538/74, 1979 m. balandžio 26 d., 49 punktas; taip pat žr. EŽTT, *Silver ir kiti prieš Jungtinę Karalystę*, Nr. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 1983 m. kovo 25 d., 88 punktas.

46 EŽTT, *Rotaru prieš Rumuniją* (DK), Nr. 28341/95, 2000 m. gegužės 4 d., 57 punktas; taip pat žr. EŽTT, *Association for European Integration and Human Rights ir Ekimdzhiev prieš Bulgariją*, Nr. 62540/00, 2007 m. birželio 28 d.; EŽTT, *Shimovolos prieš Rusiją*, Nr. 30194/09, 2011 m. birželio 21 d., ir EŽTT, *Vetter prieš Prancūziją*, Nr. 59842/00, 2005 m. gegužės 31 d.

Byloje *Taylor-Sabori prieš Jungtinę Karalystę*[47] pareiškėją sekė policija. Naudodama pareiškėjo pranešimų gaviklio „kloną“, policija galėjo perimti jam siunčiamas žinutes. Pareiškėjas buvo suimtas ir apkaltintas bendrininkavimu tiekiant kontroliuojamą narkotiką. Dalį baudžiamojo persekiojimo prieš jį bylos sudarė žinučių gavimo metu daromos rašytinės pastabos dėl pranešimų gaviklio žinučių, kurias perrašė policija. Tačiau teisiant pareiškėją Britanijos teisės akte nebuvo jokios nuostatos, reglamentuojančios ryšių, perduodamų per privačią telekomunikacijų sistemą, perėmimą. Todėl jo teisių apribojimas „neatitiko teisės akto“. EŽTT padarė išvadą, kad taip buvo pažeistas EŽTK 8 straipsnis.

Byla *Vukota-Bojić prieš Šveicariją*[48] buvo susijusi su slaptu socialinio draudimo pareiškėjo sekimu, kurį vykdė draudimo įmonės pasamdyti privatūs tyrėjai. EŽTT nusprendė, kad nors skunde nagrinėjamą priežiūros priemonę nurodė taikyti privati draudimo įmonė, šiai įmonei valstybė suteikė teisę mokėti privalomojo sveikatos draudimo išmokas ir rinkti draudimo įmokas. Valstybė, perduodama savo įsipareigojimus privatiems subjektams ar asmenims, negalėtų būti atleista nuo atsakomybės pagal Konvenciją. Nacionalinėje teisėje turi būti nustatytos tinkamos apsaugos priemonės, kurios padėtų užtikrinti, kad EŽTK 8 straipsnyje nustatytų teisių apribojimai „atitiktų teisės aktus“. Nagrinėjamoje byloje EŽTT padarė išvadą, kad EŽTK 8 straipsnis buvo pažeistas, nes nacionalinės teisės akte nebuvo pakankamai aiškiai nurodyta draudimo įmonėms, veikiančioms kaip valdžios institucijos draudimo ginčuose, suteiktos diskrecijos vykdyti slaptą apdraustojo asmens sekimą taikymo sritis ir būdas. Visų pirma nacionalinės teisės aktuose nebuvo nustatytos tinkamos apsaugos nuo piktnaudžiavimo priemonės.

Apribojimu siekiama teisėto tikslo

Teisėtas interesas gali būti vienas iš įvardytų viešųjų interesų arba kitų asmenų teisių ir laisvių apsauga. Pagal EŽTK 8 straipsnio 2 dalį apribojimas galėtų būti pateisinamas tokiais teisėtais interesais, kaip nacionalinis saugumas, visuomenės saugumas ar šalies ekonominė gerovė, viešosios tvarkos pažeidimų ar nusikaltimų prevencija, sveikatos ar moralės apsauga ir kitų asmenų teisių ir laisvių apsauga.

47 EŽTT, *Taylor-Sabori prieš Jungtinę Karalystę*, Nr. 47114/99, 2002 m. spalio 22 d.

48 EŽTT, *Vukota-Bojić prieš Šveicariją*, Nr. 61838/10, 2016 m. spalio 18 d., 77 punktas.

Pavyzdys. Byloje *Peck prieš Jungtinę Karalystę*[49] pareiškėjas bandė nusižudyti gatvėje persipjaudamas riešus, tačiau nežinojo, kad jį filmavo AVSS kamera. AVSS kamerose rodomą vaizdą stebėjusi policija jį išgelbėjo ir paskui perdavė AVSS įrašą žiniasklaidai, kuri jį paskelbė nepaslėpusi pareiškėjo veido. EŽTT nusprendė, kad nebuvo jokių susijusių ar pakankamų priežasčių, kuriomis būtų galima pateisinti tai, kad valdžios institucijos, negavusios pareiškėjo sutikimo arba nepaslėpdamos jo tapatybės, atskleidė įrašą visuomenei. EŽTT padarė išvadą, kad buvo pažeistas EŽTK 8 straipsnis.

Apribojimas yra būtinas demokratinėje visuomenėje

EŽTT pareiškė, kad „būtinumo sąvoka reiškia, kad apribojimas atitinka neatidėliotiną socialinį poreikį ir visų pirma yra proporcingas siekiamam teisėtam tikslui“[50]. Vertindamas, ar priemonė yra būtina neatidėliotinam socialiniam poreikiui patenkinti, EŽTT nagrinėja jos svarbą ir tinkamumą siekiamo tikslo atžvilgiu. Šiuo tikslu ji gali atsižvelgti į tai, ar apribojimas padeda spręsti problemą, kuri, jei nebus išspręsta, galėtų turėti žalingą poveikį visuomenei, ar yra įrodymų, kad apribojimas gali sušvelninti tokį žalingą poveikį, ir koks yra platesnis visuomenės požiūris šiuo klausimu[51]. Pavyzdžiui, jeigu saugumo tarnybos renka ir saugo konkrečių asmenų, kurie, kaip nustatyta, turi ryšių su teroristiniais judėjimais, asmens duomenis, tai reikštų asmenų teisės į privatų gyvenimą apribojimą, kuriuo siekiama patenkinti rimtą ir neatidėliotiną socialinį poreikį, susijusį su nacionaliniu saugumu ir kova su terorizmu. Kad būtų įvykdytas būtinumo kriterijus, apribojimas taip pat turi būti proporcingas. EŽTT praktikoje proporcingumas vertinamas atsižvelgiant į būtinumo koncepciją. Pagal proporcingumo principą reikalaujama, kad pagal EŽTK saugomų teisių apribojimas neturėtų viršyti to, kas būtina teisėtam tikslui pasiekti. Svarbūs veiksniai, į kuriuos reikia atsižvelgti atliekant proporcingumo testą, yra susiję su apribojimo mastu, visų pirma asmenų, kuriems daromas poveikis, skaičiumi, ir apsaugos priemonėmis arba perspėjimais, kurie nustatomi siekiant kontroliuoti apribojimo taikymo sritį arba žalingus padarinius asmenų teisėms[52].

49 EŽTT, *Peck prieš Jungtinę Karalystę*, Nr. 44647/98, 2003 m. sausio 28 d., 85 punktas.

50 EŽTT, *Leander prieš Švediją*, Nr. 9248/81, 1987 m. kovo 26 d., 58 punktas.

51 29 straipsnio duomenų apsaugos darbo grupė (29 straipsnio darbo grupė) (2014 m.), *Nuomonė dėl būtinumo ir proporcingumo sąvokų taikymo ir duomenų apsaugos teisėsaugos sektoriuje*, WP 211, Briuselis, 2014 m. vasario 27 d., p. 7–8.

52 *Ten pat*, p. 9–11.

Pavyzdys. Byloje *Khelili prieš Šveicariją*[53] per policijos patikrinimą pas pareiškėją rastos vizitinės kortelės, kuriose buvo toks tekstas: „Puiki, graži moteris, kuriai per trisdešimt, norėtų susitikti su vyru ir kartu išgerti kavos ar retkarčiais susitikti. Telefono numeris <...>." Pareiškėja teigė, kad, aptikusi šias korteles, policija įrašė jos vardą ir pavardę į prostitucija besiverčiančių asmenų sąrašą, tačiau pareiškėja tai nuolat neigė. Pareiškėja prašė policijos kompiuteriniuose įrašuose išbraukti žodį „prostitutė". EŽTT iš esmės pripažino, kad asmens duomenų saugojimas, remiantis tuo, kad asmuo gali padaryti kitą nusikaltimą, tam tikromis aplinkybėmis gali būti proporcingas. Tačiau pareiškėjos byloje įtarimai dėl neteisėto vertimosi prostitucija pasirodė pernelyg neaiškūs ir bendri, jie nebuvo pagrįsti konkrečiais faktais, nes pareiškėja niekada nebuvo nuteista už vertimąsi neteisėta prostitucija, todėl negalėjo būti laikoma, kad jos duomenų saugojimas tenkina „neatidėliotiną socialinį poreikį" pagal EŽTK 8 straipsnį. Atsižvelgdamas į tai, kad būtent valdžios institucijos turi įrodyti saugomų pareiškėjos duomenų tikslumą ir pareiškėjos teisių apribojimo rimtumą, EŽTT nusprendė, kad žodžio „prostitutė" vartojimas policijos daugybę metų saugomose bylose nebuvo būtinas demokratinėje visuomenėje. EŽTT padarė išvadą, kad buvo pažeistas EŽTK 8 straipsnis.

Pavyzdys. Byloje *S. ir Marper prieš Jungtinę Karalystę*[54] buvo sulaikyti du pareiškėjai ir apkaltinti nusikalstamų veikų padarymu. Policija paėmė jų pirštų atspaudus ir DNR mėginius, kaip numatyta Policijos ir kriminalinių įrodymų įstatyme. Pareiškėjai niekada nebuvo nuteisti už nusikaltimus: vienas pareiškėjas buvo išteisintas teisme, o baudžiamoji byla prieš kitą pareiškėją buvo nutraukta. Vis dėlto jų pirštų atspaudus, DNR profilius ir ląstelių mėginius policija laikė ir saugojo duomenų bazėje, o pagal nacionalinės teisės aktus šiuos duomenis buvo galima saugoti neribotą laiką. Nors Jungtinė Karalystė teigė, kad duomenų saugojimas padėjo išaiškinti būsimus nusikaltėlius ir kad taip buvo siekiama teisėto nusikaltimų prevencijos ir nustatymo tikslo, EŽTT manė, kad pareiškėjų teisės į privatų gyvenimą apribojimas buvo nepagrįstas. Jis priminė, kad pagal pagrindinius duomenų apsaugos principus reikalaujama, kad asmens duomenų laikymas būtų proporcingas atsižvelgiant į duomenų rinkimo principą ir kad saugojimo terminai turi būti riboti. EŽTT pripažino, kad duomenų bazės išplėtimas, kad ji apimtų ne tik nuteistų asmenų, bet ir

53 EŽTT, *Khelili prieš Šveicariją*, Nr. 16188/07, 2011 m. spalio 18 d.

54 EŽTT, *S. ir Marper prieš Jungtinę Karalystę* (DK), Nr. 30562/04 ir 30566/04, 2008 m. gruodžio 4 d.

visų įtariamų, bet nenuteistų asmenų DNR profilius, galėjo padėti atskleisti nusikaltimus Jungtinėje Karalystėje ir užkirsti jiems kelią. Tačiau tokiam išplėtimui „pakenkė bendri ir neaiškūs saugojimo įgaliojimai“[55].

Atsižvelgiant į ląstelių mėginiuose esančios genetinės informacijos ir informacijos apie sveikatą gausą, pareiškėjų teisės į privatų gyvenimą ribojimas buvo ypač didelis. Suimtų asmenų pirštų atspaudai ir pavyzdžiai galėtų būti imami ir saugomi policijos duomenų bazėje neribotą laiką, neatsižvelgiant į nusikalstamos veikos pobūdį ir sunkumą, taip pat ir nesunkių nusikalstamų veikų, už kurias nebaudžiama laisvės atėmimo bausme, atveju. Be to, išteisintų asmenų galimybės pašalinti savo duomenis iš duomenų bazės buvo ribotos. Galiausiai EŽTT ypač atsižvelgė į tai, kad suėmimo metu vienas pareiškėjas buvo vienuolikos metų amžiaus. Nepilnamečio, kuris nėra nuteistas, asmens duomenų laikymas gali būti ypač žalingas atsižvelgiant į šių asmenų pažeidžiamumą ir jų vystymosi ir integracijos į visuomenę svarbą[56]. EŽTT vienbalsiai nusprendė, kad laikant duomenis buvo neproporcingai ribojama teisė į privatų gyvenimą ir toks ribojimas negalėjo būti laikomas būtinu demokratinėje visuomenėje.

Pavyzdys. Byloje *Leander prieš Švediją*[57] EŽTT nusprendė, kad asmenų, pretenduojančių į nacionalinio saugumo požiūriu svarbias pareigas, slaptas tikrinimas savaime neprieštarauja būtinumo demokratinėje visuomenėje reikalavimui. Atsižvelgdamas į specialias nacionalinėje teisėje nustatytas priemones, kuriomis apsaugomi duomenų subjekto interesai, pavyzdžiui, parlamento ir Teisingumo kanclerio įgyvendinamos kontrolės priemonės, EŽTT priėjo prie išvados, kad Švedijos darbuotojų kontrolės sistema atitiko EŽTK 8 straipsnio 2 dalies reikalavimus. Atsižvelgiant į plačią valstybės atsakovės diskrecijos laisvę, ji turėjo teisę manyti, kad pareiškėjo byloje nacionalinio saugumo interesai buvo viršesni už asmeninius interesus. EŽTT padarė išvadą, kad EŽTK 8 straipsnis nebuvo pažeistas.

55 *Ten pat*, 119 punktas.

56 *Ten pat*, 124 punktas.

57 EŽTT, *Leander prieš Švediją*, Nr. 9248/81, 1987 m. kovo 26 d., 59 ir 67 punktai.

1.2.2. Teisėtų apribojimų sąlygos pagal ES pagrindinių teisių chartiją

Chartijos struktūra ir formuluotė skiriasi nuo EŽTK. Chartijoje nevartojama garantuojamų teisių ribojimo sąvoka, tačiau joje yra nuostata dėl naudojimosi Chartijoje pripažintomis teisėmis ir laisvėmis apribojimo (-ų).

Pagal 52 straipsnio 1 dalį Chartijoje pripažįstamų teisių ir laisvių įgyvendinimo apribojimai, taigi ir teisės į asmens duomenų apsaugą įgyvendinimo apribojimai, yra priimtini, tik jeigu jie:

- numatyti teisės akte
- ir jais gerbiama teisės į duomenų apsaugą esmė,
- ir jie atitinka proporcingumo principą, yra būtini[58], ir
- atitinka Sąjungos pripažinto bendrojo intereso tikslus arba yra reikalingi siekiant apsaugoti kitų asmenų teises ir laisves.

Kadangi asmens duomenų apsauga yra atskira ir savarankiška ES teisinėje tvarkoje galiojanti pagrindinė teisė, kuri saugoma pagal Chartijos 8 straipsnį, bet koks asmens duomenų tvarkymas savaime reiškia šios teisės apribojimą. Nesvarbu, ar atitinkami asmens duomenys yra susiję su asmens privačiu gyvenimu, ar jie yra neskelbtini, arba ar duomenų subjektams sukelta kokių nors nepatogumų. Kad būtų teisėtas, apribojimas turi atitikti visas Chartijos 52 straipsnio 1 dalyje nustatytas sąlygas.

Apribojimas numatytas teisės akte

Teisės į asmens duomenų apsaugą apribojimai turi būti numatyti teisės akte. Šis reikalavimas reiškia, kad apribojimai turi būti grindžiami teisiniu pagrindu, kuris yra tinkamai prieinamas, numatomas ir suformuluotas pakankamai tiksliai, kad asmenys galėtų suprasti savo pareigas ir reguliuoti savo elgesį. Teisiniame pagrinde taip pat turi būti aiškiai apibrėžta kompetentingų institucijų naudojimosi įgaliojimais apsaugoti asmenis nuo savavališko kišimosi taikymo sritis ir būdas. Šis aiškinimas yra

58 Dėl priemonių, kuriomis ribojama pagrindinė teisė į asmens duomenų apsaugą, būtinumo vertinimo žr. EDAPP (2017 m.), *Būtinumo vertinimo priemonių rinkinys*, Briuselis, 2017 m. balandžio 11 d.

panašus į „teisėto apribojimo“ reikalavimą pagal EŽTT praktiką[59] ir buvo teigiama, kad Chartijoje vartojamos sąvokos „nustatyta teisės akte“ reikšmė turėtų būti tokia pat, kaip ji išaiškinta EŽTK[60]. EŽTT praktika, ypač sąvoka „teisės akto kokybė“, kurią jis išplėtojo per daugybę metų, yra svarbus aspektas, į kurį turi atsižvelgti ESTT aiškindamas Chartijos 52 straipsnio 1 dalies taikymo sritį[61].

Apribojimu paisoma teisės esmės

Pagal ES teisinę tvarką nustatant bet kokius pagal Chartiją saugomų pagrindinių teisių apribojimus privaloma paisyti šių teisių esmės. Tai reiškia, kad negali būti pateisinami tokie apribojimai, dėl kurių didelio masto ir intervencinio pobūdžio pagrindinė teisė praranda savo turinį. Jeigu pažeidžiama teisės esmė, būtinai laikoma, kad apribojimas yra neteisėtas, ir tokiu atveju nereikia papildomai vertinti, ar juo siekiama bendrojo intereso tikslo ir ar jis atitinka būtinumo ir proporcingumo kriterijus.

Pavyzdys. Byla *Schrems*[62] buvo susijusi su asmenų apsauga atsižvelgiant į jų asmens duomenų perdavimą trečiosioms šalims, šiuo atveju tai buvo Jungtinės Amerikos Valstijos. Austrijos pilietis Schrems, kuris keletą metų naudojosi *Facebook*, Airijos duomenų apsaugos priežiūros institucijai pateikė skundą, kuriame prašė paskelbti negaliojančiu jo asmens duomenų perdavimą iš *Facebook* Airijos patronuojamosios įmonės *Facebook Inc.* įmonei ir JAV, kur jie buvo tvarkomi, esantiems serveriams. Jis teigė, kad, atsižvelgiant į 2003 m. JAV informatoriaus Edwardo Snowdeno atskleistą informaciją, susijusią su JAV sekimo tarnybų vykdoma sekimo veikla, JAV teisėje ir praktikoje nebuvo numatyta pakankama į JAV teritoriją perduodamų asmens duomenų apsauga. E. Snowdenas atskleidė, kad Nacionalinė saugumo agentūra tiesiogiai patekdavo į įmonių, pavyzdžiui, *Facebook*, serverius ir galėjo perskaityti pokalbių ir asmeninių pranešimų turinį.

59 EDAPP (2017 m.), *Būtinumo vertinimo priemonių rinkinys*, Briuselis, 2017 m. balandžio 11 d., p. 4; taip pat žr. ESTT *Teismo (didžiosios kolegijos) nuomonę 1/15*, 2017 m. liepos 26 d.

60 ESTT, sujungtos bylos C-203/15 ir C-698/15, *Tele2 Sverige AB prieš Post- och telestyrelsen* ir *Secretary of State for the Home Department prieš Tom Watson, Peter Brice, Geoffrey Lewis*, *Generalinio advokato H. Saugmandsgaard Øe išvados*, pateiktos 2016 m. liepos 19 d., 140 punktas.

61 ESTT, C-70/10, *Scarlet Extended SA prieš Société belge des auteurs compositeurs et éditeurs (SABAM)*, *generalinio advokato P. Cruz Villalón išvados*, pateiktos 2011 m. balandžio 14 d., 100 punktas.

62 ESTT, C-362/14, *Maximillian Schrems prieš Data Protection Commissioner* (DK), 2015 m. spalio 6 d.

Duomenys į JAV buvo perduodami remiantis 2000 m. Komisijos priimtu sprendimu dėl tinkamumo, pagal kurį buvo leidžiama duomenis perduoti JAV įmonėms, kurios pačios patvirtino, kad apsaugos iš ES perduotus duomenis ir laikysis vadinamųjų „saugaus uosto" principų. Kai byla buvo perduota ESTT, jis nagrinėjo Komisijos sprendimo galiojimą atsižvelgdamas į Chartiją. ESTT priminė, kad pagrindinių teisių apsauga ES reiškia, kad nuo šių teisių leidžiančios nukrypti nuostatos ir apribojimai taikomi tik tiek, kiek tai griežtai būtina. ESTT laikėsi nuomonės, kad teisės aktai, kuriais valdžios institucijoms leidžiama bendrai susipažinti su elektroninių ryšių turiniu, „kelia pavojų Chartijos 7 straipsnyje garantuotos pagrindinės teisės į privataus gyvenimo gerbimą esmei". Ši teisė taptų beprasmė, jeigu JAV valdžios institucijos turėtų įgaliojimus nereguliariai susipažinti su pranešimais be jokio objektyvaus pateisinimo, pagrįsto konkrečiomis su nacionaliniu saugumu arba nusikaltimų prevencija susijusiomis aplinkybėmis, kurios yra būdingos atitinkamam asmeniui, ir jeigu tokia sekimo praktika būtų vykdoma neužtikrinant tinkamų apsaugos nuo piktnaudžiavimo įgaliojimais priemonių.

Be to, ESTT pažymėjo, kad „teisės aktai, kuriuose nenumatyta jokia galimybė asmeniui pasinaudoti teisių gynimo priemonėmis, kad galėtų susipažinti su savo asmens duomenimis arba kad tokie duomenys būtų ištaisyti ar ištrinti", yra nesuderinami su pagrindine teise į veiksmingą teisminę apsaugą (Chartijos 47 straipsnis). Todėl „saugaus uosto" sprendimas neužtikrino atitinkamo pagrindinių teisių apsaugos lygio JAV, kuris iš esmės būtų lygiavertis ES garantuojamai apsaugai pagal direktyvą, skaitant ją kartu su Chartija. Todėl ESTT paskelbė sprendimą negaliojančiu[63].

Pavyzdys. Byloje *Digital Rights Ireland*[64] ESTT nagrinėjo, ar Direktyva 2006/24/EB (Duomenų saugojimo direktyva) atitinka Chartijos 7 ir 8 straipsnius. Pagal direktyvą elektroninių ryšių paslaugų teikėjai turėjo saugoti srauto ir vietos nustatymo duomenis ne trumpiau kaip šešis ir ne ilgiau kaip 24 mėnesius ir leisti kompetentingoms nacionalinėms institucijoms susipažinti

63 ESTT sprendimas pripažinti Komisijos sprendimą 520/2000/EB negaliojančiu taip pat buvo grindžiamas kitais motyvais, kurie bus nagrinėjami kituose šio vadovo skirsniuose. Visų pirma ESTT laikėsi nuomonės, kad sprendimu buvo neteisėtai apriboti nacionalinių duomenų apsaugos priežiūros institucijų įgaliojimai. Be to, pagal „saugaus uosto" sistemą asmenys negalėjo pasinaudoti jokiomis teisių gynimo priemonėmis tais atvejais, kai norėjo susipažinti su savo asmens duomenimis ir (arba) juos ištaisyti arba ištrinti. Todėl Chartijos 47 straipsnyje nustatyta pagrindinė teisė į veiksmingą teisinę gynybą taip pat buvo pažeista.

64 ESTT, sujungtos bylos C-293/12 ir C-594/12, *Digital Rights Ireland Ltd prieš Minister for Communications, Marine and Natural Resources ir kt.* ir Kärntner Landesregierung ir kt. (DK), 2014 m. balandžio 8 d.

su tais duomenimis sunkių nusikaltimų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už juos tikslais. Pagal direktyvą nebuvo leidžiama saugoti elektroninių ryšių turinio. ESTT pažymėjo, kad duomenys, kuriuos paslaugų teikėjai turėjo saugoti pagal direktyvą, apėmė duomenis, kurie yra būtini siekiant atsekti ir nustatyti pranešimo šaltinį ir paskirties vietą, datą, laiką ir trukmę, numerį, kuriuo skambinama, numerius, kuriais skambinama, ir IP adresus. Iš šių duomenų „vertinamų kaip visuma, gali būti daromos labai tikslios išvados apie asmenų, kurių duomenys saugomi, privatų gyvenimą, kaip antai kasdienio gyvenimo įpročius, nuolatinę ar laikiną gyvenamąją vietą, kasdienį ir kitokį judėjimą, vykdomą veiklą, socialinius ryšius ir lankomą socialinę aplinką“.

Todėl asmens duomenų saugojimas pagal direktyvą reiškė ypač rimtą teisių į privatumą ir asmens duomenų apsaugą apribojimą. Tačiau ESTT nusprendė, kad apribojimas neturėjo neigiamos įtakos šių teisių esmei. Kalbant apie teisę į privatumą, pažymėtina, kad jos esmei nebuvo pakenkta, nes pagal direktyvą nebuvo leidžiama įgyti žinių apie pačių elektroninių ryšių turinį. Panašiai, teisė į asmens duomenų apsaugą nebuvo pažeista, nes pagal direktyvą buvo reikalaujama, kad elektroninių ryšių paslaugų teikėjai gerbtų tam tikrus duomenų apsaugos ir duomenų saugumo principus ir šiuo tikslu įgyvendintų atitinkamas technines ir organizacines priemones.

Būtinumas ir proporcingumas

Chartijos 52 straipsnio 1 dalyje nustatyta, kad, atsižvelgiant į proporcingumo principą, Chartijoje pripažįstamų pagrindinių teisių ir laisvių įgyvendinimo apribojimai gali būti nustatomi, tik jeigu jie yra būtini.

Apribojimas gali būti **būtinas**, jeigu yra poreikis priimti priemones, kurios padėtų siekti viešojo intereso tikslo, tačiau būtinumas, kaip jį išaiškino ESTT, taip pat reiškia, kad priimtos priemonės turi būti mažiau ribojančio pobūdžio, palyginti su kitomis galimybėmis siekti to paties tikslo. Kalbant apie teisių į privatų gyvenimą ir asmens duomenų apsaugą apribojimus, pažymėtina, kad ESTT taiko griežtą būtinumo testą, pagal kurį „nukrypti leidžiančios nuostatos ir apribojimai turi būti taikomi tik tiek, kiek tai tikrai būtina“. Jeigu manoma, kad apribojimas yra griežtai būtinas, taip pat reikia įvertinti, ar jis yra proporcingas.

Proporcingumas reiškia, kad apribojimo teikiama nauda turėtų nusverti trūkumus, kuriuos jis sukelia naudojimuisi atitinkamomis pagrindinėmis teisėmis[65]. Siekiant sumažinti su teisių į privatumą ir duomenų apsaugą susijusius trūkumus ir riziką, svarbu, kad kartu su apribojimais būtų nustatytos tinkamos apsaugos priemonės.

Pavyzdys. Byloje *Volker und Markus Schecke*[66] ESTT padarė išvadą, kad Taryba ir Komisija viršijo joms pagal proporcingumo principą suteiktus įgaliojimus, nustatydamos pareigą skelbti asmens duomenis, susijusius su kiekvienu fiziniu asmeniu, kuris gavo paramą iš tam tikrų žemės ūkio fondų, nedarant atitinkamais kriterijais grindžiamo skirtumo, pavyzdžiui, dėl laikotarpių, kuriais šie asmenys gavo tokią paramą, tokios paramos dažnumo arba paramos pobūdžio ir sumos.

Todėl ESTT nustatė, kad tam tikras Tarybos reglamento (EB) Nr. 1290/2005 nuostatas buvo būtina paskelbti negaliojančiomis, o Reglamentas Nr. 259/2008 turėjo būti paskelbtas negaliojančiu visa apimtimi[67].

Pavyzdys. Byloje *Digital Rights Ireland*[68] ESTT nusprendė, kad teisės į privatumą apribojimas, kuris buvo nustatytas Duomenų saugojimo direktyvoje, nepažeidė tos teisės esmės, nes juo buvo draudžiama saugoti elektroninių ryšių turinį. Tačiau jis padarė išvadą, kad direktyva neatitiko Chartijos 7 ir 8 straipsnių, ir paskelbė ją negaliojančia. Kadangi srauto ir vietos nustatymo duomenis, juos apibendrinus ir vertinant jų visumą, galima analizuoti ir taip susidaryti išsamų vaizdą apie asmenų privatų gyvenimą, tai reiškė rimtą šių teisių ribojimą. ESTT atsižvelgė į tai, kad pagal direktyvą buvo reikalaujama saugoti visus metaduomenis, susijusius su fiksuotąja ir mobiliąja telefonija, prieiga prie interneto, interneto e. paštu ir interneto telefonija, kurie taikomi visoms elektroninio ryšio priemonėms, kurių naudojimas žmonių kasdieniame gyvenime yra labai paplitęs. Praktiškai tai reiškė ribojimą, kuris darė

65 EDAPP (2017 m.), *Būtinumo vertinimo priemonių rinkinys*, p. 5.

66 ESTT, sujungtos bylos C-92/09 ir C-93/09, *Volker und Markus Schecke GbR ir Hartmut Eifert prieš Land Hessen* (DK), 2010 m. lapkričio 9 d., 89 ir 86 punktai.

67 2005 m. birželio 21 d. Tarybos reglamentas (EB) Nr. 1290/2005 dėl bendrosios žemės ūkio politikos finansavimo, OL L 209, 2005; 2008 m. kovo 18 d. Komisijos reglamentas (EB) Nr. 259/2008, kuriuo nustatomos išsamios Tarybos reglamento (EB) Nr. 1290/2005 nuostatų dėl informacijos apie Europos žemės ūkio garantijų fondo (EŽŪGF) ir Europos žemės ūkio fondo kaimo plėtrai (EŽŪFKP) paramos gavėjus skelbimo taikymo taisyklės, OL L 76, 2008.

68 ESTT, sujungtos bylos C-293/12 ir C-594/12, *Digital Rights Ireland Ltd prieš Minister for Communications, Marine and Natural Resources ir kt. Kärntner Landesregierung ir kt.* (DK), 2014 m. balandžio 8 d., 39 punktas.

poveikį visiems Europos gyventojams. Atsižvelgiant į šio ribojimo mastą ir rimtumą, srauto ir vietos nustatymo duomenis, pasak ESTT, būtų galima pagrįstai saugoti, tik jeigu siekiama kovoti su sunkiais nusikaltimais. Be to, direktyvoje nenustatyti jokie objektyvūs kriterijai, kurie padėtų užtikrinti, kad kompetentingų nacionalinių institucijų galimybė susipažinti su saugomais duomenimis neviršytų to, kas griežtai būtina. Be to, joje nebuvo esminių ir procedūrinių sąlygų, reglamentuojančių nacionalinių institucijų galimybę susipažinti su saugomais duomenimis ir juos naudoti, kurios nepriklausė nuo išankstinės teismo arba kitos nepriklausomos įstaigos peržiūros.

ESTT prie panašios išvados priėjo ir sujungtose bylose *Tele2 Sverige AB prieš Post- och telestyrelsen* ir *Secretary of State for the Home Department prieš Tom Watson ir kt.*[69]. Šios bylos buvo susijusios su „vis[ai]s abonent[ai]s ir registruot[ai]s naudotoj[ai]s, bet koki[iomi]s elektroninio ryšio priemon[ėmi]s ir vis[ai]s metaduomeni[mi]s“ nenumatant „jokio skirtumo, apribojimo arba išimties atsižvelgiant į siekiamą tikslą“[70]. Nagrinėjamoje byloje faktas, ar asmuo tiesiogiai arba netiesiogiai buvo susijęs su sunkiomis nusikalstamomis veikomis, arba ar jo pranešimai buvo svarbūs nacionaliniam saugumui, nebuvo sąlyga, kuria remiantis būtų galima saugoti jų duomenis. Atsižvelgdamas į tai, kad nėra reikalaujamo ryšio tarp saugomų duomenų ir grėsmės visuomenės saugumui arba laiko ar geografinės vietovės apribojimų, ESTT padarė išvadą, kad nacionalinės teisės aktuose viršytos ribos, kurios buvo griežtai būtinos siekiant kovoti su sunkiais nusikaltimais[71].

Panašaus požiūrio dėl būtinumo Europos duomenų apsaugos priežiūros pareigūnas laikosi savo parengtame *Būtinumo vertinimo priemonių rinkinyje*[72]. Priemonių rinkinio paskirtis – padėti įvertinti siūlomų priemonių atitiktį ES duomenų apsaugos teisės aktams. Jis buvo parengtas siekiant geriau parengti ES politikos formuotojus ir teisės aktų leidėjus, kurie rengia arba tikrina priemones, susijusias su asmens duomenų tvarkymu ir teisės į asmens duomenų apsaugą arba kitų asmenų teisių ir laisvių, nustatytų Chartijoje, apribojimu.

69 ESTT, sujungtos bylos C-203/15 ir C-698/15, *Tele2 Sverige AB prieš Post- och telestryrelsen ir Secretary of State for the Home Department prieš Tom Watson ir kt.* (DK), 2016 m. gruodžio 21 d., 105–106 punktai.

70 *Ten pat*, 105 punktas.

71 *Ten pat*, 107 punktas.

72 EDAPP (2017 m.), *Būtinumo vertinimo priemonių rinkinys*, Briuselis, 2017 m. balandžio 11 d.

Su bendruoju interesu susiję tikslai

Kad būtų galima pateisinti bet kokį Chartijoje pripažįstamų teisių įgyvendinimo apribojimą, jis taip pat turi iš tikrųjų atitikti Sąjungos pripažinto bendrojo intereso tikslus arba būti reikalingas siekiant apsaugoti kitų asmenų teises ir laisves. Kalbant apie poreikį apsaugoti kitų asmenų teises ir laisves, pažymėtina, kad teisė į asmens duomenų apsaugą dažnai sąveikauja su kitomis pagrindinėmis teisėmis. 1.3 skyriuje pateikiama išsami tokios sąveikos analizė. Kalbant apie bendrojo intereso tikslus, pažymėtina, kad jie apima bendruosius ES tikslus, patvirtintus Sutarties dėl Europos Sąjungos veikimo (SESV) 3 straipsnyje, pavyzdžiui, skatinti taiką ir jos tautų gerovę, socialinį teisingumą bei apsaugą ir kurti laisvės, saugumo ir teisingumo erdvę, kurioje būtų užtikrinamas laisvas asmenų judėjimas, kartu užtikrinant atitinkamas nusikalstamumo prevencijos ir kovos su juo priemones, taip pat kitus tikslus ir interesus, kurių apsauga užtikrinama konkrečiomis Sutarčių nuostatomis[73]. Šiuo požiūriu Chartijos 52 straipsnio 1 dalis išsamiau paaiškinama Bendrajame duomenų apsaugos reglamente: reglamento 23 straipsnio 1 dalyje išvardijami įvairūs bendrojo intereso tikslai, kurie laikomi teisėtu pagrindu apriboti asmenų teises, jeigu tuo apribojimu paisoma teisės į asmens duomenų apsaugą esmės ir jis yra būtinas ir proporcingas. Nacionalinis saugumas ir gynyba, nusikalstamumo prevencija, svarbių ES ar valstybių narių ekonominių ir finansinių interesų apsauga, visuomenės sveikata ir socialinė apsauga yra minėtųjų viešojo intereso tikslų pavyzdžiai.

Svarbu pakankamai išsamiai apibrėžti ir paaiškinti bendrojo intereso tikslą, kurio siekiama apribojimu, nes apribojimo būtinumas bus vertinamas atsižvelgiant būtent į šį paaiškinimą. Labai svarbu aiškiai ir išsamiai aprašyti apribojimo tikslą ir siūlomas priemones, kad būtų galima įvertinti, ar apribojimas yra būtinas[74]. Tikslas, kurio siekiama apribojimu, ir apribojimo būtinumas ir proporcingumas yra glaudžiai susiję.

Pavyzdys. Byla *Schwarz prieš Stadt Bochum*[75] buvo susijusi su teisės į privatų gyvenimą ir teisės į asmens duomenų apsaugą apribojimais, susijusiais su pirštų atspaudais, kuriuos valstybių narių institucijos ėmė ir saugojo siekdamos išduoti pasus[76]. Pareiškėjas kreipėsi į *Stadt Bochum* prašydamas išduoti pasą, tačiau atsisakė duoti savo pirštų atspaudus; paskui *Stadt Bochum* atmetė jo prašymą išduoti pasą. Tuomet jis pareiškė ieškinį Vokietijos teisme

73 Su Pagrindinių teisių chartija susiję išaiškinimai (2007/C 303/02), OL 2007, Nr. C 303, p. 17–35.

74 EDAPP (2017 m.), Būtinumo vertinimo priemonių rinkinys, 2017 m. balandžio 11 d., p. 4.

75 ESTT, C-291/12, *Michael Schwarz prieš Stadt Bochum*, 2013 m. spalio 17 d.

76 *Ten pat*, 33–36 punktai.

reikalaudamas išduoti jam pasą neimant piršto atspaudų. Vokietijos teismas perdavė klausimą ESTT klausdamas, ar Reglamento (EB) Nr. 2252/2004 dėl valstybių narių išduodamų pasų ir kelionės dokumentų apsauginių savybių ir biometrikos standartų 1 straipsnio 2 dalis turi būti laikoma galiojančia.

ESTT nurodė, kad pirštų atspaudai **yra asmens duomenys**, nes jie objektyviai apima unikalią informaciją apie fizinius asmenis ir leidžia tiksliai nustatyti jų tapatybę, o pirštų atspaudų ėmimas ir saugojimas reiškia duomenų tvarkymą. Toks duomenų tvarkymas, kuris reglamentuojamas pagal Reglamento (EB) Nr. 2252/2004 1 straipsnio 2 dalį, kelia grėsmę teisėms į privatų gyvenimą ir asmens duomenų apsaugą[77]. Tačiau pagal Chartijos 52 straipsnio 1 dalį šių teisių įgyvendinimui leidžiama nustatyti apribojimus, jeigu jie yra numatyti teisės akte, jais paisoma šių teisių esmės ir jeigu jie atitinka proporcingumo principą, yra būtini ir iš tikrųjų atitinka Sąjungos pripažįstamus bendrojo intereso tikslus arba poreikį apsaugoti kitų asmenų teises ir laisves.

Šioje byloje ESTT pirmiausia pažymėjo, kad turi būti laikoma, kad apribojimas, kuris atsiranda imant ir saugant pirštų atspaudus siekiant išduoti pasą, **yra nustatytas teisės akte**, nes šios operacijos numatytos Reglamento (EB) Nr. 2252/2004 1 straipsnio 2 dalyje. Antra, pastarasis reglamentas buvo skirtas užkirsti kelią pasų klastojimui ir nesąžiningam jų naudojimui. Todėl 1 straipsnio 2 dalimi, be kita ko, siekiama užkirsti kelią neteisėtam atvykimui į ES, taigi ir Sąjungos pripažinto bendrojo intereso tikslui. Trečia, iš ESTT prieinamų įrodymų nebuvo akivaizdu ir nebuvo teigiama, kad šioje byloje šių teisių įgyvendinimui nustatytais apribojimais nebuvo paisoma šių teisių esmės. Ketvirta, pirštų atspaudų laikymui labai saugioje laikmenoje, kaip numatyta šioje nuostatoje, reikalinga sudėtinga technologija. Tikėtina, kad toks saugojimas gali sumažinti pasų klastojimo riziką ir palengvinti institucijų, atsakingų už pasų autentiškumo tikrinimą prie ES sienų, darbą. Aplinkybė, kad metodas nėra visiškai patikimas, nėra lemiama. Nors šis metodas ir nevisiškai panaikina galimybę praleisti leidimo neturinčius asmenis, pakanka, kad jis reikšmingai sumažintų tokio praleidimo riziką. Atsižvelgdamas į tai, kas išdėstyta, ESTT nusprendė, kad Reglamento (EB) Nr. 2252/2004 1 straipsnio 2 dalyje nurodytų pirštų atspaudų ėmimas ir saugojimas buvo tinkamas siekiant to reglamento tikslų ir, žvelgiant plačiau, siekiant užkirsti kelią neteisėtam atvykimui į ES[78].

77 *Ten pat*, 27–30 punktai.

78 *Ten pat*, 35–45 punktai.

ESTT toliau vertino, ar toks tvarkymas yra **būtinas**, ir pažymėjo, kad nagrinėjamas ieškinys buvo susijęs su ne daugiau nei dviejų pirštų atspaudų ėmimu, kuriuos, be kita ko, paprastai gali matyti kiti asmenys, todėl tai nėra intymaus pobūdžio operacija. Ji atitinkamam asmeniui taip pat nesukelia fizinio ar psichologinio pobūdžio nepatogumų, kurie yra ne didesni nei darant jo veido nuotrauką. Taip pat reikėtų pažymėti, kad vienintelė reali alternatyva pirštų atspaudams imti, kuri buvo pateikta nagrinėjant bylą ESTT, buvo rainelės skenavimas. Iš ESTT pateiktos bylos medžiagos nematyti, kad pastaroji procedūra mažiau pažeistų Chartijos 7 ir 8 straipsniuose pripažintas teises nei pirštų atspaudų ėmimas. Be to, kalbant apie šių dviejų metodų veiksmingumą, neginčijama, kad rainelės atpažinimo technologija dar nėra tokia pažangi kaip pirštų atspaudų atpažinimo technologija ir ji šiuo metu yra gerokai brangesnė nei pirštų atspaudų palyginimo procedūra, todėl yra mažiau tinkama bendram naudojimui. Todėl ESTT nebuvo pranešta apie jokias priemones, kurios būtų pakankamai veiksmingos, kad padėtų pasiekti apsaugos nuo nesąžiningo pasų naudojimo tikslo ir keltų mažesnį pavojų Chartijos 7 ir 8 straipsniuose pripažįstamoms teisėms, palyginti su priemonėmis, susijusiomis su pirštų atspaudų naudojimu grindžiamu metodu[79].

ESTT pažymėjo, kad Reglamento (EB) Nr. 2252/2004 4 straipsnio 3 dalyje aiškiai nustatyta, kad pirštų atspaudai gali būti naudojami tik siekiant patikrinti paso autentiškumą ir jo turėtojo tapatybę, o reglamento 1 straipsnio 2 dalyje nenumatyta galimybė saugoti pirštų atspaudus, išskyrus jų saugojimą pačiame pase, kuris priklauso tik jo turėtojui. Taigi reglamente nebuvo numatytas pagal jį surinktų duomenų centralizuoto saugojimo arba tokių duomenų naudojimo siekiant kitų tikslų nei neteisėto atvykimo į ES prevencija teisinis pagrindas[80]. Atsižvelgdamas į visą tai, kas išvardyta, ESTT padarė išvadą, kad išnagrinėjus pateiktą prejudicinį klausimą nenustatyta nieko, kas galėtų turėti įtakos Reglamento (EB) Nr. 2252/2004 1 straipsnio 2 dalies galiojimui.

Chartijos ir EŽTK ryšiai

Nepaisant skirtingų formuluočių, Chartijos 52 straipsnio 1 dalyje nustatytų teisių teisėtų apribojimų sąlygos primena EŽTK 8 straipsnio 2 dalį, susijusią su teise į privatų gyvenimą. Savo jurisprudencijoje ESTT ir EŽTT dažnai remiasi vienas kito sprendimais ir taip palaiko nuolatinį tarpusavio dialogą, siekdami suderinto duomenų apsaugos

79 ESTT, C-291/12, *Michael Schwarz prieš Stadt Bochum*, 2013 m. spalio 17 d., 46–53 punktai.

80 *Ten pat*, 56–61 punktai.

taisyklių aiškinimo. Chartijos 52 straipsnio 3 dalyje nustatyta, kad „[š]ioje Chartijoje nurodytų teisių, atitinkančių Žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos garantuojamas teises, esmė ir taikymo sritis yra tokia, kaip nustatyta toje Konvencijoje“. Tačiau Chartijos 8 straipsnis nėra tiesiogiai susijęs su EŽTK straipsniu[81]. Chartijos 52 straipsnio 3 dalis yra susijusi su pagal kiekvieną teisinę tvarką saugomų teisių turiniu ir apimtimi, o ne jų apribojimo sąlygomis. Tačiau, atsižvelgdamas į platesnį abiejų teismų dialogo ir bendradarbiavimo kontekstą, ESTT atlikdamas analizę gali atsižvelgti į teisėto apribojimo kriterijus pagal EŽTK 8 straipsnį, kaip juos išaiškino EŽTT. Galimas ir priešingas scenarijus, pagal kurį EŽTT gali remtis teisėto apribojimo pagal Chartiją sąlygomis. Bet kuriuo atveju taip pat reikėtų atsižvelgti į tai, kad EŽTK nėra tobulo Chartijos 8 straipsnio atitikmens, kuriame būtų nurodyta asmens duomenų apsauga, visų pirma duomenų subjekto teisės, teisėti duomenų tvarkymo pagrindai ir nepriklausomos institucijos vykdoma priežiūra. Kai kurie Chartijos 8 straipsnio elementai gali būti grindžiami EŽTT praktika, parengta pagal EŽTK 8 straipsnį ir susijusia su 108-ąja konvencija[82]. Šis ryšys padeda užtikrinti galimybę ESTT ir EŽTT sprendžiant su duomenų apsauga susijusius klausimus atsižvelgti į vienas kito patirtį.

1.3. Sąveika su kitomis teisėmis ir teisėtais interesais

Pagrindiniai faktai

- Teisė į duomenų apsaugą dažnai yra susijusi su kitomis teisėmis, pavyzdžiui, saviraiškos laisve ir teise gauti bei perduoti informaciją.
- Ši sąsaja dažnai yra dvilypė: nors yra situacijų, kuriose teisė į asmens duomenų apsaugą prieštarauja konkrečiai teisei, tačiau taip pat yra situacijų, kuriose teisė į asmens duomenų apsaugą padeda užtikrinti veiksmingą tos pačios konkrečios teisės laikymąsi. Pavyzdžiui, taip yra saviraiškos laisvės atveju, atsižvelgiant į tai, kad profesinės paslapties išsaugojimas yra teisės į privatų gyvenimą sudedamoji dalis.
- Poreikis apsaugoti kitų asmenų teises ir laisves yra vienas iš kriterijų, naudojamų vertinant teisės į asmens duomenų apsaugą apribojimo teisėtumą.
- Kai kyla pavojus skirtingoms teisėms, teismai privalo nustatyti jų pusiausvyrą, kad jas suderintų.

81 EDAPP (2017 m.), *Būtinumo vertinimo priemonių rinkinys*, Briuselis, 2017 m. balandžio 11 d., p. 6.

82 Su Europos pagrindinių teisių chartija susijusių išaiškinimų (2007/C 303/02) 8 straipsnis.

- Pagal Bendrąjį duomenų apsaugos reglamentą reikalaujama, kad valstybės narės teisę į asmens duomenų apsaugą suderintų su žodžio ir informacijos laisve.
- Valstybės narės savo nacionalinėje teisėje taip pat gali nustatyti konkrečias taisykles, kad suderintų teisę į asmens duomenų apsaugą su visuomenės galimybe susipažinti su oficialiais dokumentais ir pareigomis saugoti profesinę paslaptį.

Teisė į asmens duomenų apsaugą nėra absoliuti teisė; teisėto šios teisės apribojimo sąlygos išsamiai išdėstytos pirmiau. Vienas iš teisėto teisių apribojimo kriterijų, kuris pripažįstamas pagal ET ir ES teisę, yra tai, kad duomenų apsaugą būtina apriboti siekiant apsaugoti kitų asmenų teises ir laisves. Jeigu teisė į duomenų apsaugą yra susijusi su kitomis teisėmis, EŽTT ir ESTT ne kartą konstatavo, kad taikant ir aiškinant EŽTK 8 straipsnį ir Chartijos 8 straipsnį būtina nustatyti pusiausvyrą atsižvelgiant į kitas teises[83]. Keletas svarbių pavyzdžių padės atskleisti, kaip nustatoma ši pusiausvyra.

Be šių teismų atliekamo teisių pusiausvyros nustatymo, valstybės prireikus gali priimti teisės aktus, kad teisę į duomenų apsaugą suderintų su kitomis teisėmis. Todėl Bendrajame duomenų apsaugos reglamente numatytos įvairios sritys, kuriose galima numatyti nacionalines nukrypti leidžiančias nuostatas.

Kalbant apie saviraiškos laisvę, pažymėtina, kad pagal BDAR reikalaujama, kad valstybės narės teisėje „teisė į asmens duomenų apsaugą pagal šį reglamentą turi būti suderinta su teise į saviraiškos ir informacijos laisvę, įskaitant duomenų tvarkymą žurnalistikos tikslais ir akademinės, meninės ar literatūrinės saviraiškos tikslais“[84]. Valstybės narės taip pat gali priimti teisės aktus, kad duomenų apsaugą suderintų su visuomenės galimybe susipažinti su oficialiais dokumentais ir pareigomis saugoti profesinę paslaptį, kurios yra teisės į privatų gyvenimą sudedamoji dalis[85].

1.3.1. Saviraiškos laisvė

Viena iš teisių, kuri labiausiai sąveikauja su teise į duomenų apsaugą, yra teisė į saviraiškos laisvę.

83 EŽTT, *Von Hannover prieš Vokietiją (Nr. 2)* (DK), Nr. 40660/08 ir 60641/08, 2012 m. vasario 7 d.; ESTT, sujungtos bylos C-468/10 ir C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) ir Federación de Comercio Electrónico y Marketing Directo (FECEMD) prieš Administración del Estado*, 2011 m. lapkričio 24 d., 48 punktas; ESTT, C-275/06, *Productores de Música de España (Promusicae) prieš Telefónica de España SAU* (DK), 2008 m. sausio 29 d., 68 punktas.

84 Bendrojo duomenų apsaugos reglamento 85 straipsnis.

85 *Ten pat*, 86 ir 90 straipsniai.

Saviraiškos laisvė saugoma pagal Chartijos 11 straipsnį („Saviraiškos ir informacijos laisvė“). Ši teisė apima „laisvę turėti savo įsitikinimus, gauti bei perduoti informaciją ir idėjas valdžios institucijoms nekliudant ir nepaisant valstybių sienų“. Informacijos laisvė pagal Chartijos 11 straipsnį ir EŽTK 10 straipsnį apima ne tik teisės perduoti informaciją, bet ir ją *gauti* apsaugą.

Saviraiškos laisvės apribojimai turi atitikti pirmiau aprašytus Chartijos 52 straipsnio 1 dalyje nustatytus kriterijus. Be to, 11 straipsnis yra susijęs su EŽTK 10 straipsniu. Chartijos 52 straipsnio 3 dalyje nustatyta, kad joje nurodytų teisių, atitinkančių EŽTK garantuojamas teises, „esmė ir taikymo sritis yra tokia, kaip nustatyta šioje Konvencijoje“. Todėl apribojimai, kurie gali būti teisėtai nustatyti Chartijos 11 straipsnyje garantuojamai teisei, negali viršyti EŽTK 10 straipsnio 2 dalyje nustatytų apribojimų, t. y. jie turi būti nustatyti teisės akte ir būti būtini demokratinėje visuomenėje „siekiant <...> apsaugoti <...> kitų asmenų garbę ar teises“. Tokios teisės visų pirma apima teisę į privatų gyvenimą ir teisę į asmens duomenų apsaugą.

Asmens duomenų apsaugos ir saviraiškos laisvės santykis reglamentuojamas Bendrojo duomenų apsaugos reglamento 85 straipsnyje „Duomenų tvarkymas ir saviraiškos ir informacijos laisvė“. Pagal šį straipsnį reikalaujama, kad valstybės narės teisę į asmens duomenų apsaugą suderintų su teise į saviraiškos ir informacijos laisvę. Visų pirma konkrečių Bendrojo duomenų apsaugos reglamento skyrių išimtys ir nukrypti leidžiančios nuostatos daromos atsižvelgiant į žurnalistikos tikslus arba akademinės, meninės ar literatūrinės raiškos tikslą, jeigu jos yra būtinos siekiant suderinti teisę į asmens duomenų apsaugą su saviraiškos ir informacijos laisve.

Pavyzdys. Byloje *Tietosuojavaltuutettu prieš Satakunnan Markkinapörssi Oy ir Satamedia Oy*[86] ESTT buvo prašoma apibūdinti santykį tarp duomenų apsaugos ir spaudos laisvės[87]. Jis turėjo išnagrinėti, kaip įmonė, naudodamasi SMS paslauga, skleidžia teisėtai iš Suomijos mokesčių institucijų gautus mokestinius duomenis apie maždaug 1,2 mln. fizinių asmenų. Suomijos duomenų apsaugos priežiūros institucija priėmė sprendimą, kuriuo reikalaujama, kad įmonė nustotų skleisti šiuos duomenis. Įmonė ginčijo šį sprendimą

86 ESTT, C-73/07, *Tietosuojavaltuutettu prieš Satakunnan Markkinapörssi Oy ir Satamedia Oy* (DK), 2008 m. gruodžio 16 d., 56, 61 ir 62 punktai.

87 Byla buvo susijusi su Duomenų apsaugos direktyvos 9 straipsnio, kurį dabar pakeitė Bendrojo duomenų apsaugos reglamento 85 straipsnis, aiškinimu. Tame 9 straipsnyje nustatyta: „Valstybės narės numato išimtis ir nukrypimus nuo šio skyriaus bei IV ir VI skyriaus, kai asmens duomenys tvarkomi tik žurnalistiniais sumetimais arba meninės ar literatūrinės raiškos tikslais, bet tiktai tuomet, jeigu šios išimtys reikalingos, norint privatumo teisę suderinti su laisv[ę] reikšti savo mintis ir įsitikinimus reglamentuojančiomis taisyklėmis.“

nacionaliniame teisme, kuris kreipėsi į ESTT prašydamas patikslinti Duomenų apsaugos direktyvos išaiškinimą. Visų pirma ESTT turėjo patikrinti, ar asmens duomenų tvarkymas, kurį mokesčių institucijos suteikė tam, kad mobiliųjų telefonų naudotojai galėtų gauti mokesčių duomenis, susijusius su kitais fiziniais asmenimis, turi būti laikomas veikla, vykdoma tik žurnalistiniais tikslais. Padaręs išvadą, kad įmonės veikla yra „asmens duomenų tvarkymas“, kaip tai suprantama pagal Duomenų apsaugos direktyvos 3 straipsnio 1 dalį, ESTT analizavo direktyvos 9 straipsnį (dėl asmens duomenų tvarkymo ir saviraiškos laisvės). Jis pirmiausia atkreipė dėmesį į teisės į saviraiškos laisvę svarbą kiekvienoje demokratinėje visuomenėje ir nusprendė, kad su ta laisve susijusios sąvokos, pavyzdžiui, žurnalistika, turėtų būti aiškinamos plačiai. Paskui jis pastebėjo, kad, siekiant dviejų pagrindinių teisių pusiausvyros, nukrypti nuo teisės į duomenų apsaugą leidžiančios nuostatos ir šios teisės apribojimai turi būti taikomi tik tiek, kiek tai griežtai būtina. Tokiomis aplinkybėmis ESTT nusprendė, kad veikla, kurią, pavyzdžiui, vykdė atitinkamos įmonės ir kuri buvo susijusi su viešuose dokumentuose pateiktais duomenimis, pagal nacionalinės teisės aktus gali būti klasifikuojama kaip „žurnalistinė veikla“, jeigu jos tikslas yra atskleisti visuomenei informaciją, nuomones arba idėjas, nepaisant to, kokiomis priemonėmis jos perduodamos. Jis taip pat nusprendė, kad ši veikla neapsiriboja žiniasklaidos įmonėmis ir gali būti vykdoma siekiant pelno. Tačiau ESTT paliko nacionaliniam teismui nuspręsti, ar taip buvo konkrečių šios bylos aplinkybių atveju.

Tą pačią bylą taip pat nagrinėjo EŽTT po to, kai nacionalinis teismas, remdamasis ESTT rekomendacijomis, nusprendė, kad priežiūros institucijos nutarimas nutraukti visos mokestinės informacijos skelbimą buvo pagrįstas įmonės saviraiškos laisvės apribojimu. EŽTT pritarė šiam požiūriui[88]. Jis nustatė, kad net jeigu įmonių teisė perduoti informaciją buvo apribota, toks apribojimas atitiko teisės aktą, juo buvo siekiama teisėto tikslo ir jis buvo būtinas demokratinėje visuomenėje.

EŽTT priminė teismo praktikos kriterijus, kuriais turėtų vadovautis nacionalinės valdžios institucijos ir pats EŽTT tais atvejais, kai nustatoma saviraiškos laisvės ir teisės į privatų gyvenimą pusiausvyra. Kylant klausimų dėl politinių kalbų ar diskusijų viešojo intereso klausimais, nėra daug galimybių apriboti teisę gauti ir perduoti informaciją, nes visuomenė turi teisę būti informuota, „ir demokratinėje visuomenėje tai yra esminė teisė“[89]. Tačiau nereikėtų

88 EŽTT, *Satakunnan Markkinapörssi Oy ir Satamedia Oy prieš Suomiją*, Nr. 931/13, 2017 m. birželio 27 d.

89 *Ten pat*, 169 punktas.

manyti, kad straipsniai spaudoje, kuriais siekiama tik patenkinti tam tikro skaitytojo smalsumą, susijusį su asmens privataus gyvenimo aplinkybėmis, gali paskatinti diskusijas viešojo intereso klausimais. Nuo duomenų apsaugos taisyklių žurnalistikos tikslais leidžiančia nukrypti nuostata siekiama sudaryti sąlygas žurnalistams susipažinti su duomenimis, juos rinkti ir tvarkyti, kad jie galėtų vykdyti savo žurnalistinę veiklą. Taigi iš tiesų buvo viešasis interesas suteikti galimybę susipažinti su dideliu mokesčių duomenų kiekiu ir leisti įmonėms pareiškėjoms juos rinkti ir tvarkyti. Tačiau EŽTT konstatavo, kad nėra viešojo intereso laikraščiuose masiškai platinti tokius neapdorotus duomenis nepakeista forma ir be jokios analitinės analizės. Informacija apie apmokestinimą galėjo padėti besidomintiems visuomenės nariams suklasifikuoti asmenis pagal jų ekonominę padėtį ir pasiekti, kad visuomenė gautų kuo daugiau informacijos apie kitų asmenų privatų gyvenimą. Tačiau nemanytina, kad tai galėjo paskatinti diskusijas viešojo intereso klausimais.

Pavyzdys. Byloje *Google Spain*[90] ESTT nagrinėjo, ar *Google* buvo įpareigota iš paieškos sąrašo rezultatų pašalinti pasenusią informaciją apie pareiškėjo finansinius sunkumus. Atlikus paiešką *Google* paieškos sistemoje naudojant pareiškėjo vardą ir pavardę, paieškos rezultatuose buvo pateiktos nuorodos į senus laikraščio straipsnius, kuriuose buvo nurodytas jo ryšys su bankroto procedūra. Pareiškėjas manė, kad tai yra jo teisės į privatų gyvenimą ir asmens duomenų apsaugą pažeidimas, nes procedūra buvo baigta prieš daugelį metų, todėl tokios nuorodos yra nereikšmingos.

ESTT pirmiausia paaiškino, kad interneto paieškos sistemos ir paieškos rezultatai, kuriuose pateikiami asmens duomenys, gali padėti nustatyti išsamų asmens profilį. Atsižvelgiant į vis didesnį visuomenės skaitmeninimą, reikalavimas, kad asmens duomenys būtų tikslūs ir kad jie nebūtų skelbiami daugiau nei būtina, t. y. teikti informaciją visuomenei, yra labai svarbus siekiant užtikrinti aukštą asmens duomenų apsaugos lygį. „Duomenų valdytojas, kiek tai susiję su tuo duomenų tvarkymu, neviršydamas savo pareigų, įgaliojimų ir gebėjimų, turi užtikrinti, kad tas duomenų tvarkymas atitiktų ES teisės reikalavimus“, kad nustatytos teisinės garantijos būtų visiškai veiksmingos. Tai reiškia, kad asmens teisė ištrinti savo asmens duomenis tais atvejais, kai jų tvarkyti nebebūtina arba jie yra pasenę, taip pat taikoma paieškos sistemoms, kurios, kaip nustatyta, yra duomenų valdytojos, o ne vien paprastos duomenų tvarkytojos (žr. 2.3.1 skirsnį).

90 ESTT, C-131/12, *Google Spain SL, Google Inc. prieš Agencia Española de Protección de Datos (AEPD), Mario Costeja González* (DK), 2014 m. gegužės 13 d., 81–83 punktai.

Nagrinėdamas, ar *Google* turėjo pašalinti su pareiškėju susijusias nuorodas, ESTT nusprendė, kad tam tikromis sąlygomis asmenys turi teisę reikalauti, kad jų asmens duomenys būtų ištrinti iš internetinės paieškos sistemos paieškos rezultatų. Šia teise galima pasinaudoti tais atvejais, kai su asmeniu susijusi informacija yra netiksli, netinkama, nereikšminga arba perteklinė duomenų tvarkymo tikslais. ESTT pripažino, kad ši teisė nėra absoliuti; ją reikia suderinti su kitomis teisėmis, visų pirma plačiosios visuomenės interesu ir teise susipažinti su informacija. Kiekvieną prašymą ištrinti duomenis reikia įvertinti atskirai, kad būtų užtikrinta pusiausvyra tarp, viena vertus, duomenų subjekto pagrindinių teisių į asmens duomenų apsaugą ir privatų gyvenimą ir, kita vertus, visų interneto naudotojų teisėtų interesų. ESTT pateikė rekomendacijas dėl veiksnių, į kuriuos reikia atsižvelgti nustatant teisių pusiausvyrą. Nagrinėjamos informacijos pobūdis yra ypač svarbus veiksnys. Jeigu informacija yra neskelbtina atsižvelgiant į asmens privatų gyvenimą ir jeigu nėra viešojo intereso, kad informacija būtų prieinama, duomenų apsauga ir privatumas būtų viršesnis už plačiosios visuomenės teisę susipažinti su informacija. Priešingai, jeigu paaiškėja, kad duomenų subjektas yra visuomenės veikėjas arba kad informacija yra tokio pobūdžio, kad galima pateisinti galimybę plačiajai visuomenei leisti susipažinti su tokia informacija, tuomet pagrindinių teisių į duomenų apsaugą ir privatumą apribojimas yra pateisinamas.

Remdamasi sprendimu, 29 straipsnio darbo grupė priėmė ESTT sprendimo įgyvendinimo rekomendacijas. Rekomendacijose pateikiamas bendrų kriterijų, kuriuos turi naudoti priežiūros institucijos nagrinėdamos skundus, susijusius su asmenų prašymais ištrinti duomenis, sąrašas ir šie kriterijai turi padėti šioms institucijoms nustatyti šių teisių įgyvendinimo pusiausvyrą[91].

Kalbant apie teisės į duomenų apsaugą suderinimą su teise į saviraiškos laisvę, pažymėtina, kad EŽTT priėmė keletą svarbių sprendimų.

91 29 straipsnio darbo grupė (2014 m.), *ESTT sprendimo „Google Spain and Inc prieš Agencia Española de Protección de Datos (AEPD) ir Mario Costeja González“ (C-131/12) įgyvendinimo rekomendacijos*, WP 225, Briuselis, 2014 m. lapkričio 26 d.

Pavyzdys. Byloje *Axel Springer AG prieš Vokietiją*[92] EŽTT nusprendė, kad draudimu, kuriuo pareiškėjo įmonei apribotos galimybės skelbti straipsnį dėl gerai žinomo aktoriaus arešto ir nuteisimo, buvo pažeistas EŽTT 10 straipsnis. EŽTT pakartojo jo praktikoje suformuluotus kriterijus, į kuriuos reikia atsižvelgti nustatant teisės į saviraiškos laisvę ir teisės į privatų gyvenimą pusiausvyrą:

- ar paskelbtame straipsnyje aprašytas įvykis buvo visuotinės svarbos;
- ar atitinkamas asmuo buvo viešas, ir
- kaip buvo gauta informacija ir ar ji buvo patikima.

EŽTT nustatė, kad aktoriaus suėmimas ir nuteisimas buvo viešas teisminis faktas, taigi jis atitiko viešąjį interesą; aktorius buvo pakankamai gerai žinomas, kad jį būtų galima laikyti viešu asmeniu; informaciją pateikė prokuratūra ir jos tikslumo šalys neginčijo. Todėl įmonei nustatytų apribojimų paskelbimas nebuvo pagrįstai proporcingas teisėtam pareiškėjo privataus gyvenimo apsaugos tikslui. EŽTT padarė išvadą, kad buvo pažeistas EŽTK 10 straipsnis.

Pavyzdys. Byla *Coudec and Hachette Filipacchi Associés prieš Prancūziją*[93] buvo susijusi su Prancūzijos savaitiniame žurnale paskelbtu pokalbiu su N. Coste, kuri teigė, kad Monako princas Albertas yra jos sūnaus tėvas. Interviu taip pat buvo apibūdintas N. Coste ryšys su princu ir tai, kaip ji reagavo į vaiko gimimą, kartu buvo pateiktos princo su vaiku nuotraukos. Princas Albertas pareiškė ieškinį leidybos įmonei dėl jo teisės į privataus gyvenimo apsaugą pažeidimo. Prancūzijos teismai nusprendė, kad dėl šio straipsnio paskelbimo princas Albertas patyrė nepataisomą žalą, ir nurodė leidėjui atlyginti žalą ir paskelbti sprendimo duomenis žurnalo priekiniame viršelyje.

Žurnalų leidėjai iškėlė bylą EŽTT teigdami, kad Prancūzijos teismų sprendimais buvo nepagrįstai apribota jų teisė į saviraiškos laisvę. EŽTT turėjo rasti princo Alberto teisės į privatų gyvenimą, leidėjo saviraiškos teisės ir plačiosios visuomenės teisės būti informuotai pusiausvyrą. N. Coste teisė papasakoti savo istoriją visuomenei ir vaiko interesas, kad tėvo ir vaiko santykiai būtų oficialiai nustatyti, taip pat buvo svarbios aplinkybės.

92 EŽTT, *Axel Springer AG prieš Vokietiją* (DK), Nr. 39954/08, 2012 m. vasario 7 d., 90 ir 91 punktai.

93 EŽTT, *Coudec ir Hachette Filipacchi Associés prieš Prancūziją* (DK), Nr. 40454/07, 2015 m. lapkričio 10 d.

EŽTT nusprendė, kad interviu paskelbimas reiškė princo teisės į privatų gyvenimą apribojimą, ir toliau nagrinėjo, ar šis apribojimas buvo būtinas. Jis laikėsi nuomonės, kad paskelbtas interviu buvo susijęs su viešu asmeniu ir visuomenės interesu, nes Monako piliečiai buvo suinteresuoti sužinoti, kad princas turi vaiką, nes paveldimosios monarchijos ateitis „iš esmės yra susijusi su palikuonių buvimu“, todėl tai yra visuomenei rūpimas klausimas[94]. EŽTT taip pat pažymėjo, kad straipsnis sudarė sąlygas N. Coste ir jos vaikui įgyvendinti teisę į saviraiškos laisvę. Nacionaliniai teismai tinkamai neišnagrinėjo EŽTT praktikoje suformuotų principų ir kriterijų, taikomų nustatant teisės į privatų gyvenimą ir teisės į saviraiškos laisvę pusiausvyrą. Jis padarė išvadą, kad Prancūzija pažeidė EŽTK 10 straipsnį dėl saviraiškos laisvės.

EŽTT praktikoje vienas iš esminių kriterijų, susijusių su šių teisių pusiausvyra, yra tai, ar nagrinėjama saviraiškos forma padeda skatinti diskusijas viešojo intereso klausimais.

Pavyzdys. Byloje *Mosley prieš Jungtinę Karalystę*[95] nacionalinis savaitraštis paskelbė intymias pareiškėjo, kuris yra gerai žinomas asmuo, nuotraukas. Paskui pareiškėjas pareiškė civilinį ieškinį leidėjui ir prisiteisė žalos atlyginimą. Nepaisydamas priteistos piniginės kompensacijos, jis skundėsi, kad toliau kentėjo nuo jo teisės į privatumą pažeidimo, nes jam atsisakyta suteikti galimybę prieš paskelbiant atitinkamas nuotraukas kreiptis dėl uždraudimo, nes laikraščiui nebuvo nustatytas joks teisinis reikalavimas iš anksto pranešti apie paskelbimą.

EŽTT pažymėjo, kad nors tokia medžiaga paprastai skleidžiama pramogų, o ne švietimo tikslais, jai neabejotinai buvo taikoma EŽTK 10 straipsnio apsauga, o tai galėtų atitikti EŽTK 8 straipsnio reikalavimus, jei informacija būtų privataus ir intymaus pobūdžio ir nebūtų viešojo intereso ją skleisti. Vis dėlto reikia ypač atidžiai nagrinėti apribojimus, kurie galėtų būti taikomi kaip tam tikros cenzūros priemonės prieš paskelbiant medžiagą. Atsižvelgdamas į atgrasomąjį poveikį, kurį gali turėti reikalavimas pranešti iš anksto, abejones dėl jo veiksmingumo ir plačią veiksmų savo nuožiūra laisvę toje srityje, EŽTT padarė išvadą, kad 8 straipsnyje nebuvo teisiškai privalomo reikalavimo pranešti iš anksto. Todėl EŽTT padarė išvadą, kad EŽTK 8 straipsnis nebuvo pažeistas.

94 *Ten pat*, 104–116 punktai.

95 EŽTT, *Mosley prieš Jungtinę Karalystę*, Nr. 48009/08, 2011 m. gegužės 10 d., 129 ir 130 punktai.

Pavyzdys. Byloje *Bohlen prieš Vokietiją*[96] pareiškėjas, kuris yra gerai žinomas dainininkas ir meno kūrėjas, paskelbė autobiografinę knygą ir paskui, teismams priėmus atitinkamus sprendimus, buvo priverstas pašalinti tam tikras pasakojimo dalis. Ši istorija buvo plačiai aprašyta nacionalinėje žiniasklaidoje, o tabako įmonė, naudodama pareiškėjo vardą be jo sutikimo, pradėjo humoristinę reklaminę kampaniją, susijusią su šiuo įvykiu. Pareiškėjas nesėkmingai reikalavo, kad reklamos įmonė atlygintų žalą, teigdamas, kad buvo pažeistos jo teisės pagal EŽTK 8 straipsnį. EŽTT pakartojo kriterijus, kuriais grindžiama teisės į privatų gyvenimą ir teisės į saviraiškos laisvę pusiausvyra, ir nusprendė, kad 8 straipsnis nebuvo pažeistas. Pareiškėjas buvo visuomenės veikėjas, o reklamoje buvo kalbama ne apie jo privataus gyvenimo detales, o apie viešą renginį, apie kurį jau buvo paskelbta žiniasklaidoje ir kuris buvo viešų diskusijų dalis. Be to, reklama buvo humoristinio pobūdžio ir joje nebuvo jokių žalingų ar neigiamų aplinkybių, susijusių su pareiškėju.

Pavyzdys. Byloje *Biriuk prieš Lietuvą*[97] pareiškėja EŽTT įrodinėjo, kad Lietuva neįvykdė savo prievolės apsaugoti jos teisę į privatų gyvenimą, nes, nepaisant to, kad pagrindinis laikraštis rimtai pažeidė jos privatumą, bylą nagrinėjantys nacionaliniai teismai jai priteisė apgailėtinai mažą piniginę kompensaciją. Priteisdami neturtinę žalą, nacionaliniai teismai taikė nacionalinės teisės nuostatas dėl visuomenės informavimo, kuriose buvo nustatyta žemutinė neturtinės žalos, kurią žiniasklaidos priemonė sukėlė neteisėtai skleisdama visuomenei informaciją apie asmens privatų gyvenimą, kompensavimo riba. Šis atvejis kilo dėl to, kad didžiausias Lietuvos dienraštis pirmajame puslapyje paskelbė straipsnį, kuriame nurodyta, kad pareiškėja yra užsikrėtusi ŽIV. Straipsnyje taip pat buvo kritikuojamas pareiškėjo elgesys ir abejojama jos moralės normomis.

EŽTT priminė, kad asmens duomenų, bent jau medicininių duomenų, apsauga turi esminę reikšmę teisei į privatų gyvenimą pagal EŽTK. Asmens sveikatos duomenų konfidencialumas yra ypač svarbus, nes medicininių duomenų (šioje byloje tai buvo informacija apie tai, kad pareiškėja užsikrėtusi ŽIV) gali turėti ypač didelį poveikį asmens privačiam ir šeimos gyvenimui, jo darbui ir integracijai į visuomenę. EŽTT ypatingą dėmesį skyrė faktinei aplinkybei, kad, remiantis laikraštyje pateiktu pranešimu, ligoninės darbuotojai pateikė

96 EŽTT, *Bohlen prieš Vokietiją*, Nr. 53495/09, 2015 m. vasario 19 d., 45–60 punktai.

97 EŽTT, *Biriuk prieš Lietuvą*, Nr. 23373/03, 2008 m. lapkričio 25 d.

informaciją apie tai, kad pareiškėja užsikrėtusi ŽIV, ir taip akivaizdžiai pažeidė jiems taikomą profesinės paslapties išsaugojimo įpareigojimą. Todėl pareiškėjos teisė į privatų gyvenimą nebuvo teisėtai ribojama.

Straipsnį paskelbė spauda, o saviraiškos laisvė pagal EŽTK taip pat yra pagrindinė teisė. Tačiau nagrinėdamas, ar tokios rūšies informacijos apie pareiškėją paskelbimas galėjo būti pateisinamas viešojo intereso buvimu, EŽTT nustatė, kad paskelbiant informaciją iš esmės buvo siekiama parduoti daugiau laikraščių patenkinus skaitytojo smalsumą. Nemanytina, kad toks tikslas galėjo paskatinti visuomenės diskusijas viešojo intereso klausimais. Kadangi tai buvo „siaubingas piktnaudžiavimas spaudos laisve“, dėl didelių žalos atlyginimo apribojimų ir nedidelės neturtinės žalos sumos, numatytos pagal nacionalinę teisę, Lietuva neįvykdė savo pozityvios pareigos apsaugoti pareiškėjos teisę į privatų gyvenimą. EŽTT padarė išvadą, kad buvo pažeistas EŽTK 8 straipsnis.

Teisė į saviraiškos laisvę ir teisė į asmens duomenų apsaugą ne visada prieštarauja viena kitai. Tam tikrais atvejais veiksminga asmens duomenų apsauga padeda garantuoti saviraiškos laisvę.

Pavyzdys. Byloje *Tele2 Sverige* ESTT konstatavo, kad Chartijos 7 ir 8 straipsniuose nustatytų pagrindinių teisių apribojimas, nustatytas remiantis Direktyva 2006/24/EB (Duomenų saugojimo direktyva), buvo „plataus masto ir laikytinas itin rimtu. Be to, aplinkybė, kad duomenys saugomi ir vėliau naudojami apie tai neinformuojant abonento ar registruoto naudotojo, gali sudaryti atitinkamiems asmenims įspūdį, kaip savo išvados 52 ir 72 punktuose nurodė generalinis advokatas, kad jų privatus gyvenimas yra nuolat stebimas.“ ESTT taip pat nustatė, kad nediferencijuotas srauto ir vietos nustatymo duomenų naudojimas galėjo daryti poveikį elektroninių ryšių naudojimui ir tam, „kaip <...> naudotojai naudojasi <...> Chartijos 11 straipsnyje įtvirtinta saviraiškos laisve“[98]. Šiuo atžvilgiu nustatant reikalavimą, kad griežtos apsaugos priemonės duomenų saugojimui nebūtų taikomos nediferencijuotai, užtikrinama, kad duomenų apsaugos taisyklėmis galiausiai prisidedama prie saviraiškos laisvės įgyvendinimo.

98 ESTT, sujungtos bylos C-203/15 ir C-698/15, *Tele2 Sverige AB prieš Post- och telestyrelsen* ir *Secretary of State for the Home Department prieš Tom Watson ir kt.* (DK), 2016 m. gruodžio 21 d., 37 ir 101 punktai; ESTT, sujungtos bylos C-293/12 ir C-594/12, *Digital Rights Ireland Ltd prieš Minister for Communications, Marine and Natural Resources ir kt.* ir Kärntner Landesregierung ir kt. (DK), 2014 m. balandžio 8 d., 28 punktas.

Kalbant apie teisę gauti informaciją, kuri taip pat yra sudedamoji saviraiškos laisvės dalis, pažymėtina, kad vis labiau suprantama, kad demokratinės visuomenės veikimui svarbus valdžios skaidrumas. Skaidrumas yra bendrąjį interesą atitinkantis tikslas, kuriuo remiantis būtų galima pateisinti teisės į duomenų apsaugą apribojimą, jeigu jis yra būtinas ir proporcingas, kaip paaiškintas 1.2 skirsnyje. Per pastaruosius du dešimtmečius teisė susipažinti su valdžios institucijų turimais dokumentais pripažinta svarbia kiekvieno ES piliečio ir bet kurio fizinio ar juridinio asmens, gyvenančio ar turinčio registruotą buveinę valstybėje narėje, teise.

Pagal ET teisę galima remtis Rekomendacijoje dėl teisės susipažinti su oficialiais dokumentais nustatytais principais, kuriais vadovavosi Konvencijos dėl teisės susipažinti su oficialiais dokumentais (Konvencija Nr. 205) rengėjai[99].

Pagal ES teisę teisė susipažinti su dokumentais garantuojama Reglamente Nr. 1049/2001 dėl galimybės visuomenei susipažinti su Europos Parlamento, Tarybos ir Komisijos dokumentais (Galimybės susipažinti su dokumentais reglamentas)[100]. Chartijos 42 straipsnyje ir SESV 15 straipsnio 3 dalyje ši teisė susipažinti praplėsta, kad apimtų „Sąjungos institucijų, įstaigų ir organų bet kurios formos dokument[u]s“.

Ši teisė gali prieštarauti teisei į duomenų apsaugą, jeigu leidus susipažinti su dokumentu būtų atskleisti kitų asmenų asmens duomenys. Bendrojo duomenų apsaugos reglamento 86 straipsnyje aiškiai nustatyta, kad valdžios institucijų ir įstaigų turimuose oficialiuose dokumentuose esančius asmens duomenis atitinkama institucija arba įstaiga gali atskleisti laikydamasi Sąjungos[101] arba valstybės narės teisės akto, kad suderintų visuomenės galimybę susipažinti su oficialiais dokumentais su teise į duomenų apsaugą pagal reglamentą.

Todėl prašymus leisti susipažinti su valdžios institucijų turimais dokumentais arba informacija gali prireikti suderinti su asmenų, kurių duomenys pateikiami prašomuose dokumentuose, teise į duomenų apsaugą.

99 Europos Taryba, Ministrų Komitetas (2002 m.), Rekomendacija R (81) 19 ir Rekomendacija *Rec(2002)2* valstybėms narėms dėl teisės susipažinti su oficialiais dokumentais, 2002 m. vasario 21 d.; Europos Taryba, Konvencija dėl teisės susipažinti su oficialiais dokumentais, CETS Nr. 205, 2009 m. birželio 18 d. Konvencija dar neįsigaliojo.

100 2001 m. gegužės 30 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 1049/2001 dėl galimybės visuomenei susipažinti su Europos Parlamento, Tarybos ir Komisijos dokumentais, OL L 145, 2001.

101 Chartijos 42 straipsnis, SESV 15 straipsnio 3 dalis ir Reglamentas (EB) Nr. 1049/2009.

Pavyzdys. Byloje *Volker und Markus Schecke ir Hartmut Eifert prieš Land Hessen*[102] ESTT turėjo įvertinti ES žemės ūkio subsidijų paramos gavėjų vardų ir pavardžių ir jų gautų sumų paskelbimo proporcingumą, kurio reikalaujama pagal ES teisės aktus. Paskelbiant šią informaciją buvo siekiama didinti skaidrumą ir padėti visuomenei kontroliuoti, ar administracija tinkamai naudoja viešąsias lėšas. Keletas paramos gavėjų ginčijo šio paskelbimo proporcingumą.

ESTT atkreipė dėmesį į tai, kad teisė į duomenų apsaugą nėra absoliuti, ir teigė, kad paskelbus svetainėje duomenis apie dviejų ES žemės ūkio paramos fondų paramos gavėjų vardus, pavardes ir tikslias gautas sumas apskritai buvo ribojamas jų privatus gyvenimas, ypač jų teisė į asmens duomenų apsaugą.

ESTT nustatė, kad toks Chartijos 7 ir 8 straipsnių apribojimas buvo numatytas teisės akte ir atitiko ES pripažįstamo bendrojo intereso tikslą, t. y. padidinti Bendrijos lėšų panaudojimo skaidrumą. Tačiau ESTT nusprendė, kad ES žemės ūkio paramos iš šių dviejų fondų gavėjų, kurie yra fiziniai asmenys, vardų, pavardžių ir tikslių gautų sumų paskelbimas reiškė neproporcingą priemonę ir nebuvo pagrįstas atsižvelgiant į Chartijos 52 straipsnio 1 dalį. Jis pripažino, kad demokratinėje visuomenėje svarbu nuolat informuoti mokesčių mokėtojus apie viešųjų lėšų panaudojimą. Kadangi „[a]utomatiškai teikti pirmenybės skaidrumo tikslui, palyginti su teise į asmens duomenų apsaugą, negalima“[103], ES institucijos buvo įpareigotos rasti Sąjungos intereso, susijusio su skaidrumu, ir teisių į privatumą ir duomenų apsaugą įgyvendinimo apribojimų, su kuriais paramos gavėjai susidūrė dėl paskelbtos informacijos, pusiausvyrą.

ESTT laikėsi nuomonės, kad ES institucijos netinkamai nustatė šią pusiausvyrą, nes buvo galima numatyti priemones, kuriomis būtų daromas mažesnis neigiamas poveikis pagrindinėms asmenų teisėms, kartu veiksmingai prisidedant prie skaidrumo tikslo, kurio buvo siekiama paskelbiant informaciją. Pavyzdžiui, bendro informacijos paskelbimo, kuris daro poveikį visiems paramos gavėjams, nurodant jų vardą, pavardę ir tikslias kiekvieno iš jų gautas sumas, skirtumą būtų galima daryti, remiantis atitinkamais kriterijais, pavyzdžiui, laikotarpiais, kuriais šie asmenys gavo paramą, paramos dažnumu

102 ESTT, sujungtos bylos C-92/09 ir C-93/09, *Volker und Markus Schecke GbR ir Hartmut Eifert prieš Land Hessen* (DK), 2010 m. lapkričio 9 d., 47–52, 58, 66–67, 75, 86 ir 92 punktai.

103 *Ten pat*, 85 punktas.

arba jos suma ir pobūdžiu[104]. Todėl ES teisės aktą dėl informacijos, susijusios su Europos žemės ūkio fondų paramos gavėjais, paskelbimo ESTT paskelbė iš dalies negaliojančiu.

Pavyzdys. Byloje *Rechnungshof prieš Österreichischer Rundfunk ir kt.*[105] ESTT peržiūrėjo tam tikrų Austrijos teisės aktų suderinamumą su ES duomenų apsaugos teise. Pagal teisės aktą buvo reikalaujama, kad valstybinė įstaiga rinktų ir perduotų duomenis apie pajamas, kad paskelbtų įvairių viešųjų subjektų darbuotojų vardus, pavardes ir pajamas metinėje ataskaitoje, kuri pateikiama plačiajai visuomenei. Tam tikri asmenys atsisakė perduoti savo duomenis, remdamiesi duomenų apsaugos pagrindu.

Savo nuomonėje ESTT rėmėsi pagrindinių teisių apsauga kaip bendruoju ES teisės principu ir EŽTK 8 straipsniu, primindamas, kad tuo metu Chartija nebuvo privaloma. Jis nusprendė, kad duomenų apie asmens profesines pajamas rinkimas, visų pirma jų perdavimas tretiesiems asmenims, patenka į teisės į privatų gyvenimą taikymo sritį ir yra šios teisės pažeidimas. Apribojimą buvo galima pateisinti, jeigu jis būtų atitikęs teisės aktą, jeigu juo būtų siekiama teisėto tikslo ir jeigu jis būtų būtinas siekiant to tikslo demokratinėje visuomenėje. ESTT pažymėjo, kad Austrijos teisės aktu buvo siekiama teisėto tikslo, nes jo tikslas buvo užtikrinti, kad valstybės tarnautojų darbo užmokestis neviršytų pagrįstų ribų, t. y. aplinkybė, kuri, be kita ko, yra susijusi su šalies ekonomine gerove. Tačiau Austrijos interesas užtikrinti geriausią viešųjų lėšų panaudojimą turi būti suderintas su atitinkamų asmenų teisės į jų privatų gyvenimą apribojimo rimtumu.

Palikdamas nacionaliniam teismui patikrinti, ar duomenų apie fizinių asmenų pajamas paskelbimas buvo būtinas ir proporcingas atsižvelgiant į teisės aktais siekiamą tikslą, ESTT paprašė nacionalinio teismo įvertinti, ar tokį tikslą būtų galima vienodai veiksmingai pasiekti mažiau ribojančiomis priemonėmis. Kaip pavyzdį būtų galima pateikti asmens duomenų perdavimą tik stebėseną vykdančioms valdžios įstaigoms, o ne plačiajai visuomenei.

Kitose bylose tapo akivaizdu, kad, nustatant duomenų apsaugos ir galimybės susipažinti su dokumentais pusiausvyrą, kiekvienu atveju reikia atlikti išsamią analizę.

104 *Ten pat*, 89 punktas.

105 ESTT, sujungtos bylos C-465/00, C-138/01 ir C-139/01, *Rechnungshof prieš Österreichischer Rundfunk ir kt. ir Christa Neukomm ir Jospeh Lauermann prieš Österreichischer Rundfunk*, 2003 m. gegužės 20 d.

Nė viena iš šių teisių negali automatiškai būti viršesnė už kitą. ESTT turėjo galimybę dviejose bylose išaiškinti teisę susipažinti su dokumentais, kuriuose yra asmens duomenų.

Pavyzdys. Byloje *Europos Komisija prieš Bavarian Lager*[106] ESTT apibrėžė asmens duomenų apsaugos taikymo sritį atsižvelgiant į galimybę susipažinti su ES institucijų dokumentais, taip pat Reglamento (EB) Nr. 1049/2001 (Galimybės susipažinti su dokumentais reglamentas) ir Reglamento (EB) Nr. 45/2001 (ES institucijų duomenų apsaugos reglamentas) ryšį. 1992 m. įkurta įmonė *Bavarian Lager* į Jungtinę Karalystę importuoja Vokietijoje pagamintą ir į butelius išpilstytą alų, kuris iš esmės yra skirtas viešojo maitinimo įstaigoms ir barams. Tačiau įmonė susidūrė su tam tikrais sunkumais, nes Britanijos teisės aktai *de facto* buvo palankūs nacionaliniams gamintojams. Atsakydama į *Bavarian Lager* skundą, Europos Komisija prieš Jungtinę Karalystę pradėjo bylą dėl jos įsipareigojimų neįvykdymo, kurią išnagrinėjus Jungtinė Karalystė iš dalies pakeitė ginčijamas nuostatas ir suderino jas su ES teise. Tuomet *Bavarian Lager*, be kitų dokumentų, paprašė Europos Komisijos pateikti susitikimo, kuriame dalyvavo Komisijos, Jungtinės Karalystės institucijų ir *Confédération des Brasseurs du Marché Commun* (CBMC) atstovai, protokolą. Komisija sutiko atskleisti tam tikrus dokumentus, susijusius su susitikimu, tačiau pateiktoje kopijoje užtušavo penkių asmenų vardus ir pavardes; du asmenys aiškiai nesutiko atskleisti savo tapatybės, o Komisija negalėjo susisiekti su kitais trimis asmenimis. 2004 m. kovo 18 d. sprendimu Komisija atmetė naują *Bavarian Lager* prašymą gauti išsamų susitikimo protokolą ir visų pirma rėmėsi tų asmenų privataus gyvenimo apsauga, kuri garantuojama ES institucijų duomenų apsaugos reglamente.

Bavarian Lager netenkino ši pozicija ir ji pareiškė ieškinį pirmosios instancijos teisme. Teismas 2007 m. lapkričio 8 d. sprendimu panaikino Komisijos sprendimą (byla T-194/04, *The Bavarian Lager Co. Ltd prieš Europos Bendrijų Komisiją*) ir nustatė, kad paprasčiausias atitinkamų asmenų vardų ir pavardžių įrašymas į susitikime dalyvaujančių asmenų, kurie dalyvavo savo atstovaujamų įstaigų vardu, sąrašą nepakenkė privačiam gyvenimui ir nekėlė jokio pavojaus tų asmenų privačiam gyvenimui.

106 ESTT, C-28/08 P, *Europos Komisija prieš The Bavarian Lager Co. Ltd.* (DK), 2010 m. birželio 29 d.

Komisijai pateikus skundą, ESTT panaikino pirmosios instancijos teismo sprendimą. ESTT nusprendė, kad Galimybės susipažinti su dokumentais reglamente „nustatyta speciali tvarka ir sustiprinama asmens, kurio duomenys tam tikrais atvejais gali būti atskleisti visuomenei, apsauga“. Pasak ESTT, tais atvejais, kai prašymas yra pagrįstas Galimybės susipažinti su dokumentais reglamentu ir jame prašoma leisti susipažinti su dokumentais, kuriuose yra asmens duomenų, taikomos visos ES institucijų duomenų apsaugos reglamento nuostatos. Tuomet ESTT padarė išvadą, kad Komisija teisingai atmetė prašymą leisti susipažinti su visu 1996 m. spalio mėn. susitikimo protokolu. Atsižvelgiant į tai, kad penki minėtojo posėdžio dalyviai nedavė sutikimo, Komisija, pateikdama prašomo dokumento versiją, kurioje buvo užtušuotos minėtų asmenų pavardės, tinkamai laikėsi jai nustatyto atvirumo įsipareigojimo.

Be to, pasak ESTT, „[k]adangi *Bavarian Lager* nepateikė jokių aiškių ir pagrįstų įrodymų ir nenurodė kokio nors įtikinamo argumento, kurie patvirtintų šių asmens duomenų perdavimo būtinybę, Komisija negalėjo įvertinti skirtingų šalių interesų ir į juos atsižvelgti. Ji taip pat negalėjo patikrinti, ar nėra priežasties manyti, kad gali būti pažeisti teisėti duomenų subjekto interesai“, kaip to reikalaujama ES institucijų duomenų apsaugos reglamente.

Pavyzdys. Byloje *Client Earth ir PAN Europe prieš EFSA*[107] ESTT nagrinėjo, ar Europos maisto saugos tarnybos (EFSA) sprendimas atsisakyti leisti pareiškėjams be apribojimų susipažinti su visais dokumentais buvo būtinas siekiant apsaugoti asmenų, kurie buvo minimi dokumentuose, privatumą ir duomenų apsaugos teises. Tie dokumentai buvo susiję su EFSA darbo grupės bendradarbiaujant su išorės ekspertais parengtu rekomendacinės ataskaitos dėl augalų apsaugos produktų pateikimo rinkai projektu. Iš pradžių EFSA leido pareiškėjams iš dalies susipažinti su dokumentu, nesuteikdama galimybės susipažinti su kai kuriomis rekomendacinio dokumento projekto darbinėmis versijomis. Vėliau ji leido susipažinti su projektu, kuriame buvo pateiktos atskiros išorės ekspertų pastabos. Tačiau, remdamasi Reglamento (EB) Nr. 45/2001 dėl asmens duomenų tvarkymo ES institucijose ir įstaigose 8 straipsnio b punktu ir poreikiu apsaugoti išorės ekspertų privatumą, ji redagavo ekspertų vardus ir pavardes. Pirmojoje instancijoje ES Bendrasis Teismas patvirtino EFSA sprendimą.

107 ESTT, C-615/13 P, *ClientEarth, Pesticide Action Network Europe (PAN Europe) prieš Europos maisto saugos tarnybą (EFSA), Europos Komisiją*, 2015 m. liepos 16 d.

Gavęs pareiškėjų skundą, ESTT panaikino pirmojoje instancijoje priimtą sprendimą. Jis padarė išvadą, kad asmens duomenis toje byloje buvo būtina perduoti siekiant įvertinti kiekvieno išorės eksperto nepriklausomumą vykdant jų, kaip mokslininkų, užduotis ir užtikrinti, kad sprendimų priėmimo procesas EFSA išliktų skaidrus. Pasak ESTT, EFSA konkrečiai nenurodė, kaip išorės ekspertų, kurie pateikė konkrečių pastabų dėl rekomendacinio dokumento projekto, vardų ir pavardžių atskleidimas pakenktų ekspertų teisėtiems interesams. Bendrojo pobūdžio argumentas, susijęs su tikimybe, kad toks atskleidimas pažeis privatumą, nėra pakankamas, jeigu jis nepagrindžiamas su kiekvienu konkrečiu atveju susijusiais įrodymais.

Pagal šiuos ESTT sprendimus teisės į duomenų apsaugą apribojimas atsižvelgiant į galimybę susipažinti su dokumentais turi būti pagrįstas konkrečia ir pateisinama priežastimi. Teisė susipažinti su dokumentais automatiškai negali būti viršesnė už teisę į duomenų apsaugą[108].

Šis požiūris yra panašus į tą, kurio EŽTT laikosi dėl privatumo ir galimybės susipažinti su dokumentais, kaip matyti iš toliau pateiktų sprendimų. Byloje *Magyar Helsinki* priimtame sprendime EŽTT nurodė, kad 10 straipsniu asmeniui nebuvo suteikta galimybė susipažinti su valdžios institucijos turima informacija arba valdžios institucija nebuvo įpareigota perduoti tokios informacijos asmeniui. Tačiau tokia teisė arba pareiga galėjo atsirasti šiomis aplinkybėmis: pirma, kai informaciją įpareigojama atskleisti įsiteisėjusia teismo nutartimi; antra, kai galimybė susipažinti su informacija yra būtina, kad asmuo galėtų naudotis teise į saviraiškos laisvę, visų pirma teise gauti ir perduoti informaciją, ir kai jos nesuteikimas pažeistų tą teisę[109]. Tai, ar atsisakymas leisti susipažinti su informacija, atsižvelgiant į jo mastą, yra pareiškėjo saviraiškos laisvės apribojimas, reikia įvertinti kiekvienu konkrečiu atveju ir atsižvelgiant į jo konkrečias aplinkybes, įskaitant: i) prašymo pateikti informaciją tikslą; ii) prašomos informacijos pobūdį; iii) pareiškėjo funkcijas ir iv) ar informacija jau buvo prieinama.

Pavyzdys. Byloje *Magyar Helsinki Bizottság prieš Vengriją*[110] pareiškėjas, t. y. žmogaus teisių NVO, prašė, kad policija pateiktų informaciją, susijusią su *ex officio* gynybos advokato darbu, kad galėtų užbaigti tyrimą dėl valstybės samdomų gynėjų sistemos veikimo Vengrijoje. Policija atsisakė

108 Tačiau žr. išsamius svarstymus EDAPP (2011 m.), *Visuomenės galimybė susipažinti su dokumentais, kuriuose yra asmens duomenų, po* Bavarian Lager *sprendimo*, Briuselis, 2011 m. kovo 24 d.

109 EŽTT, *Magyar Helsinki Bizottság prieš Vengriją* (DK), Nr. 18030/11, 2016 m. lapkričio 8 d., 148 punktas.

110 *Ten pat*, 181, 187–200 punktai.

pateikti informaciją teigdama, kad tai buvo asmens duomenys, kurių nebuvo galima atskleisti. Taikydamas pirmiau minėtus kriterijus, EŽTT nusprendė, kad šiuo atveju buvo apribota pagal 10 straipsnį saugoma teisė. Tiksliau tariant, pareiškėjas norėjo įgyvendinti teisę perduoti informaciją, susijusią su viešuoju interesu, šiuo tikslu prašė leisti susipažinti su informacija ir informacija buvo būtina siekiant įgyvendinti pareiškėjo teisę į saviraiškos laisvę. Informacija apie valstybės samdomų gynėjų paskyrimą atitiko viešąjį interesą. Nebuvo jokios priežasties abejoti, kad atitinkamoje apklausoje buvo informacijos, kurią pareiškėjas įsipareigojo perduoti visuomenei ir kurią visuomenė turėjo teisę gauti. Todėl EŽTT sutiko, kad pareiškėjui buvo būtina pateikti prašymą leisti susipažinti su prašoma informacija tam, kad galėtų įvykdyti užduotį. Galiausiai informacija buvo parengta ir prieinama.

EŽTT padarė išvadą, kad atsisakymas leisti susipažinti su informacija toje byloje pakenkė pačiai laisvės gauti informaciją esmei. Prieidamas prie šios išvados, jis visų pirma nagrinėjo prašomos informacijos tikslą ir tai, ar ji padeda skatinti svarbias diskusijas viešojo intereso klausimais, prašomos informacijos pobūdį ir ar ji buvo susijusi su viešuoju interesu, ir byloje dalyvaujančio pareiškėjo visuomenėje atliekamu vaidmeniu.

Dėstydamas savo argumentus, EŽTT nurodė, kad NVO atliktas tyrimas buvo susijęs su teisingumo vykdymu ir teise į teisingą bylos nagrinėjimą, kuri pagal EŽTK turėjo esminę reikšmę. Kadangi prašoma informacija nebuvo susijusi su viešai neprieinamais duomenimis, atitinkamų duomenų subjektų (*ex officio* valstybės samdomų gynėjų) teisės į privatumą nebūtų buvusios pažeistos, jeigu policija pareiškėjui būtų leidusi susipažinti su informacija. Pareiškėjo prašoma informacija buvo statistinio pobūdžio ir susijusi su tuo, kiek kartų viešame baudžiamajame procese kaltinamiesiems *ex officio* buvo paskirti advokatai.

Atsižvelgdamas į tai, kad tyrimu buvo siekiama paskatinti svarbias diskusijas visuotinės svarbos klausimu, EŽTT laikėsi nuomonės, kad bet kokie NVO siūlomos paskelbti informacijos apribojimai turėjo būti atidžiai išnagrinėti. Prašoma informacija buvo susijusi su viešuoju interesu, nes viešasis interesas apima „klausimus, dėl kurių gali kilti didelių nesutarimų, kurie yra susiję su svarbiais socialiniais aspektais arba problema, apie kurią visuomenė būtų suinteresuota būti informuota“[111]. Todėl tai iš tikrųjų apimtų diskusijas

111 *Ten pat*, 156 punktas.

teisingumo vykdymo ir teisingo bylos nagrinėjimo klausimais, kurie buvo aptariami pareiškėjo tyrime. Nustatydamas įvairių teisių pusiausvyrą ir taikydamas proporcingumo principą, EŽTT nusprendė, kad buvo nepagrįstai pažeistos pareiškėjo teisės pagal EŽTK 10 straipsnį.

1.3.2. Profesinė paslaptis

Pagal nacionalinę teisę tam tikriems pranešimams gali būti taikoma pareiga saugoti profesinę paslaptį. Profesinė paslaptis gali būti suprantama kaip speciali etinė pareiga, kuria sukuriama teisinė prievolė, susijusi su tam tikromis profesijomis ir funkcijomis, ir kuri yra pagrįsta sąžiningumu ir pasitikėjimu. Šias funkcijas atliekantys asmenys ir institucijos privalo neatskleisti konfidencialios informacijos, kurią jie gavo atlikdami savo pareigas. Pareiga saugoti profesinę paslaptį visų pirma taikoma medicinos specialistams ir advokato ir kliento bendravimo konfidencialumui, be to, pagal daugumos jurisdikcijų taisykles pripažįstama pareiga saugoti profesinę paslaptį. Profesinė paslaptis nėra pagrindinė teisė, tačiau ji saugoma kaip viena iš teisės į privatų gyvenimą formų. Pavyzdžiui, ESTT nusprendė, kad tam tikrais atvejais „iš tikrųjų gali prireikti uždrausti atskleisti kai kurią konfidencialia pripažintą informaciją, siekiant apsaugoti <...> [EŽTK] 8 straipsnyje ir Chartijos 7 straipsnyje įtvirtintą įmonės pagrindinę teisę į privataus gyvenimo apsaugą“[112]. EŽTT taip pat buvo prašoma priimti sprendimą dėl to, ar profesinės paslapties apribojimai gali reikšti EŽTT 8 straipsnio pažeidimą, kaip parodyta paryškintuose pavyzdžiuose.

Pavyzdys. Byloje *Pruteanu prieš Rumuniją*[113] pareiškėjas veikė kaip komercinės įmonės advokatas, kuriam buvo uždrausta vykdyti banko sandorius, kai jam buvo pateikti kaltinimai dėl sukčiavimo. Bylos tyrimo metu Rumunijos teismai įgaliojo prokuratūrą tam tikrą laikotarpį perimti ir įrašyti įmonės partnerio pokalbius telefonu. Taip pat buvo daromi jo bendravimo su advokatu įrašai ir perimamas susirašinėjimas.

A. Pruteanu teigė, kad taip buvo apribota jo teisė į privatų gyvenimą ir susirašinėjimą. Savo sprendime EŽTT atkreipė dėmesį į advokato santykių su klientu statusą ir svarbą. Advokato pokalbių su klientu perėmimas neabejotinai pažeidė profesinę paslaptį, kuria buvo grindžiami šių dviejų asmenų

112 ESTT byla T-462/12 R, *Pilkington Group Ltd prieš Europos Komisiją*, Bendrojo Teismo pirmininko nutartis, 2013 m. kovo 11 d., 44 punktas.

113 EŽTT, *Pruteanu prieš Rumuniją*, Nr. 30181/05, 2015 m. vasario 3 d.

santykiai. Tokiu atveju advokatas taip pat galėjo skųstis dėl to, kad buvo apribota jo teisė į privatų gyvenimą ir susirašinėjimą. EŽTT nusprendė, kad buvo pažeistas EŽTK 8 straipsnis.

Pavyzdys. Byloje *Brito Ferrinho Bexiga Villa-Nova prieš Portugaliją*[114] pareiškėja, kuri buvo advokatė, remdamasi profesine paslaptimi ir banko paslaptimi, atsisakė mokesčių institucijoms atskleisti asmeninės banko sąskaitos išrašus. Prokuratūra pradėjo tyrimą dėl mokestinio sukčiavimo ir paprašė leidimo sustabdyti profesinio konfidencialumo principo galiojimą. Nacionaliniai teismai nurodė sustabdyti konfidencialumo ir banko paslapties taisyklių taikymą ir nusprendė, kad viešasis interesas turi būti viršesnis už pareiškėjos privačius interesus.

Pradėjęs bylą nagrinėti EŽTT nusprendė, kad galimybė susipažinti su pareiškėjos banko sąskaitos išrašais reiškė jos teisės į profesinio konfidencialumo gerbimą, kuri patenka į privataus gyvenimo sąvoką, apribojimą. Apribojimas turėjo teisinį pagrindą, nes buvo pagrįstas baudžiamojo proceso kodeksu ir juo buvo siekiama teisėto tikslo. Tačiau nagrinėdamas apribojimo būtinumą ir proporcingumą, EŽTT atkreipė dėmesį į tai, kad byla dėl konfidencialumo buvo nagrinėjama nedalyvaujant pareiškėjai ir be jos žinios. Todėl pareiškėja negalėjo pateikti savo argumentų. Be to, nors nacionalinėje teisėje buvo numatyta, kad tokiame procese turi būti konsultuojamasi su advokatų asociacija, tai nebuvo daroma. Galiausiai pareiškėja neturėjo galimybės veiksmingai ginčyti konfidencialumo ir jokios teisių gynimo priemonės, kuria remdamasi galėtų ginčyti priemonę. Dėl procedūrinių garantijų ir veiksmingos teisminės pareigos išlaikyti konfidencialumą sustabdymo priemonės kontrolės nebuvimo EŽTT padarė išvadą, kad buvo pažeistas EŽTK 8 straipsnis.

Profesinės paslapties ir duomenų apsaugos sąveika dažnai yra prieštaringa. Viena vertus, teisės aktuose nustatytos duomenų apsaugos taisyklės ir apsaugos priemonės padeda užtikrinti profesinę paslaptį. Pavyzdžiui, taisyklėmis, pagal kurias reikalaujama, kad duomenų valdytojai ir duomenų tvarkytojai įgyvendintų griežtas duomenų saugumo priemones, be kita ko, siekiama užkirsti kelią asmens duomenų, kuriems galioja profesinės paslapties išsaugojimo principas, konfidencialumo praradimui. Be to, pagal ES Bendrąjį duomenų apsaugos reglamentą leidžiama tvarkyti asmens sveikatos duomenis, priskiriamus prie specialių kategorijų asmens

114 EŽTT, *Brito Ferrinho Bexiga Villa-Nova prieš Portugaliją*, Nr. 69436/10, 2015 m. gruodžio 1 d.

duomenų, kuriems reikalinga griežtesnė apsauga, tačiau jiems taikomos tinkamos ir konkrečios duomenų subjektų teisių, visų pirma profesinės paslapties, apsaugos priemonės[115].

Kita vertus, duomenų valdytojams ir duomenų tvarkytojams nustatytomis profesinės paslapties saugojimo prievolėmis, susijusiomis su tam tikrais asmens duomenimis, gali būti ribojamos duomenų subjektų teisės, visų pirma teisė gauti informaciją. Nepaisant to, kad Bendrajame duomenų apsaugos reglamente pateikiamas išsamus sąrašas informacijos, kurią iš esmės reikia pateikti duomenų subjektui tais atvejais, kai asmens duomenys nebuvo iš jo gauti, šis atskleidimo reikalavimas netaikomas, kai asmens duomenys turi išlikti konfidencialūs dėl prievolės saugoti profesinę paslaptį, kuri nustatyta nacionalinėje arba ES teisėje[116].

Bendrajame duomenų apsaugos reglamente (BDAR) valstybėms narėms suteikiama galimybė priimant teisės aktą nustatyti konkrečias taisykles, kuriomis būtų užtikrinama prievolių saugoti profesinę paslaptį arba kitokių lygiaverčių paslapties išsaugojimo prievolių apsauga ir suderinama teisė į asmens duomenų apsaugą ir prievolė saugoti profesinę paslaptį[117].

BDAR nustatyta, kad valstybės narės gali priimti konkrečias taisykles dėl priežiūros institucijų įgaliojimų, susijusių su duomenų valdytojais arba duomenų tvarkytojais, kuriems taikoma prievolė saugoti profesinę paslaptį. Šios konkrečios taisyklės yra susijusios su įgaliojimais patekti į duomenų valdytojo arba duomenų tvarkytojo patalpas, patikrinti duomenų tvarkymo įrangą ir turimus asmens duomenis, jeigu tokie asmens duomenys buvo gauti vykdant veiklą, kuriai taikoma prievolė saugoti paslaptį. Todėl priežiūros institucijos, kurioms pavesta saugoti duomenis, privalo paisyti duomenų valdytojams ir duomenų tvarkytojams privalomų prievolių saugoti profesinę paslaptį. Be to, prievolė saugoti profesinę paslaptį taikoma ir patiems priežiūros institucijų nariams po to, kai jie nebedirba institucijose. Vykdydami savo užduotis priežiūros institucijų nariai arba darbuotojai gali sužinoti konfidencialią informaciją. Reglamento 54 straipsnio 2 dalyje aiškiai nustatyta, kad jie, atsižvelgdami į tokią konfidencialią informaciją, privalo saugoti profesinę paslaptį.

115 Bendrojo duomenų apsaugos reglamento 9 straipsnio 2 dalies h punktas ir 9 straipsnio 3 dalis.

116 *Ten pat*, 14 straipsnio 5 dalies d punktas.

117 *Ten pat*, 164 konstatuojamoji dalis ir 90 straipsnis.

Pagal BDAR reikalaujama, kad valstybės narės praneštų Komisijai apie taisykles, kurias jos priima siekdamos duomenų apsaugą ir reglamente nustatytus principus suderinti su prievole saugoti profesinę paslaptį.

1.3.3. Religijos ir tikėjimo laisvė

Religijos ir tikėjimo laisvė saugoma pagal EŽTK 9 straipsnį (minties, sąžinės ir religijos laisvė) ir ES pagrindinių teisių chartijos 10 straipsnį. Asmens duomenys, kuriais atskleidžiami religiniai arba filosofiniai įsitikinimai, laikomi „neskelbtinais duomenimis“ pagal ES ir ET teisę, o jų tvarkymui ir naudojimui taikoma griežtesnė apsauga.

Pavyzdys. Pareiškėjas byloje *Sinak Isik prieš Turkiją*[118] buvo alevitų religinės bendruomenės, kurios tikėjimui įtakos turėjo sufizmas ir priešislaminiai įsitikinimai ir kurią kai kurie mokslininkai laiko atskira religija, o kiti – islamo religijos dalimi, narys. Pareiškėjas skundėsi, kad prieš jo valią jo tapatybės kortelėje buvo langelis, kuriame pažymėta, kad jis išpažįsta „islamo“ religiją, o ne „alevizmą“. Nacionaliniai teismai, remdamiesi tuo, kad minėtuoju žodžiu buvo nurodoma islamo sekta, o ne atskira religija, atmetė jo prašymą pakeisti jo tapatybės kortelę, kad joje būtų nurodomas „alevizmas“. Tuomet pareiškėjas pateikė skundą EŽTT, kuriame nurodė, kad jis buvo įpareigotas atskleisti savo tikėjimą be savo sutikimo, nes tapatybės kortelėje buvo privaloma nurodyti asmens religiją ir kad taip buvo pažeidžiama jo teisė į religijos ir sąžinės laisvę, ypač atsižvelgiant į tai, kad jo tapatybės kortelėje pateikta nuoroda į „islamą“ buvo neteisinga.

EŽTT pakartojo, kad religijos laisvė apima laisvę išpažinti asmens religiją ne tik bendruomenėje su kitais, viešai ir to paties tikėjimo asmenų rate, bet taip pat pavieniui ir privačiai. Pagal tuo metu taikytus nacionalinės teisės aktus asmenys buvo įpareigoti turėti asmens tapatybės kortelę, t. y. dokumentą, kuris turėjo būti pateiktas bet kurios valdžios institucijos ar privačių įmonių prašymu, nurodant jų religiją. Taikant tokią prievolę nebuvo pripažįstama, kad asmens teisė išpažinti savo religiją taip pat apėmė atvirkštinę teisę, t. y. teisę nebūti įpareigotam atskleisti savo įsitikinimų. Nepaisant to, kad vyriausybė teigė, jog nacionalinės teisės aktai buvo iš dalies pakeisti taip, kad asmenys galėtų prašyti, kad jų tapatybės kortelėse esantis religijos langelis būtų paliktas tuščias, EŽTT manymu, vien tai, kad reikia prašyti išbraukti religiją, galėtų reikšti informacijos apie jų požiūrį į religiją atskleidimą. Be to, tais atvejais, kai tapatybės kortelėse yra religijos langelis ir jis paliekamas

118 EŽTT, *Sinan Işık prieš Turkiją*, Nr. 21924/05, 2010 m. vasario 2 d.

tuščias, taip sukuriama speciali konotacija, nes asmens tapatybės kortelės turėtojai, neturintys informacijos apie religiją, išsiskirtų iš tų asmenų, kurių kortelėje nurodomi jų įsitikinimai. EŽTT padarė išvadą, kad nacionaliniais teisės aktais buvo pažeistas EŽTK 9 straipsnis.

Tačiau bažnyčių ir religinių asociacijų ar bendruomenių veiklai vykdyti gali prireikti tvarkyti narių asmens duomenis, kad būtų galima palaikyti ryšius ir organizuoti veiklą kongregacijoje. Todėl bažnyčios ir religinės asociacijos dažnai įgyvendindavo taisykles, susijusias su asmens duomenų tvarkymu. Bendrojo duomenų apsaugos reglamento 91 straipsnyje nustatyta, kad jeigu tokios taisyklės yra išsamios, jos gali galioti toliau, jei bus suderintos su reglamento nuostatomis. Bažnyčias ir religines asociacijas, kurios turi tokias taisykles, privalo prižiūrėti nepriklausoma tam tikrais atvejais speciali priežiūros institucija, jeigu jos atitinka Bendrajame apsaugos reglamente nustatytus tokioms institucijoms keliamus reikalavimus[119].

Religinės organizacijos gali imtis asmens duomenų tvarkymo dėl kelių priežasčių, pavyzdžiui, siekdamos palaikyti ryšį su savo kongregacija arba perduoti informaciją apie religinius ar labdaros renginius, organizuoti iškilmes. Kai kuriose valstybėse bažnyčios turi tvarkyti savo narių registrus mokesčių tikslais, nes narystė religinėse įstaigose gali turėti įtakos asmenų mokėtiniems mokesčiams. Bet kuriuo atveju pagal Europos teisę religinius įsitikinimus atskleidžiantys duomenys yra neskelbtini duomenys, o bažnyčios turi būti atskaitingos už tokių duomenų nagrinėjimą ir tvarkymą, ypač dėl to, kad religinių organizacijų tvarkoma informacija dažnai susijusi su vaikais, pagyvenusiais asmenimis ar kitais pažeidžiamais visuomenės nariais.

1.3.4. Menų ir mokslo laisvė

Kita teisė, kurią reikia suderinti su teisėmis į privatų gyvenimą ir duomenų apsaugą, yra menų ir mokslo laisvė, kurios apsauga aiškiai užtikrinama ES pagrindinių teisių chartijos 13 straipsnyje. Ši teisė visų pirma kyla iš teisės į minties ir saviraiškos laisvę ir turi būti įgyvendinama atsižvelgiant į Chartijos 1 straipsnį (žmogaus orumas). EŽTT mano, kad menų ir mokslo laisvė saugoma pagal EŽTK 10 straipsnį[120]. Chartijos 13 straipsnyje garantuotai teisei taip pat gali būti taikomi Chartijos 52 straipsnio 1 dalyje nustatyti apribojimai, kurie taip pat gali būti aiškinami pagal EŽTK 10 straipsnio 2 dalį[121].

119 Bendrojo duomenų apsaugos reglamento 91 straipsnio 2 dalis.

120 EŽTT, *Müller ir kt. prieš Šveicariją*, Nr. 10737/84, 1988 m. gegužės 24 d.

121 Su Pagrindinių teisių chartija susiję išaiškinimai, OL C 303, 2007.

Pavyzdys. Byloje *Vereinigung bildender Künstler prieš Austriją*[122] Austrijos teismai uždraudė pareiškėjo asociacijai toliau eksponuoti paveikslą, kuriame buvo panaudotos įvairių visuomenės veikėjų, vaizduojamų įvairiomis lytinio akto pozomis, galvų nuotraukos. Austrijos parlamento narys, kurio nuotrauka buvo naudojama paveiksle, iškėlė bylą pareiškėjo asociacijai, siekdamas uždrausti paveikslo eksponavimą. Nacionalinis teismas nustatė draudimą. EŽTT pakartojo, kad EŽTK 10 straipsnis taikomas idėjų, kuriomis įžeidžiama, šokiruojama ar trikdoma valstybė ar bet kuris gyventojų sluoksnis, perdavimui. Tie, kurie kuria, atlieka, platina ar eksponuoja meno kūrinius, prisideda prie keitimosi idėjomis ir nuomonėmis, o valstybė privalo nederamai nepažeisti jų saviraiškos laisvės. Atsižvelgdamas į tai, kad parodoje buvo eksponuojami koliažai, kuriuose naudotos tik asmenų galvų nuotraukos, o kūnai buvo nutapyti nerealistiškai ir perdėm padidinti ir akivaizdu, kad tokia tapymo technika nebuvo siekiama atspindėti tikrovės ar sukurti kokių nors aliuzijų į ją, EŽTT toliau nurodė, jog „vargu, ar būtų galima teigti, kad piešiniu siekiama atkurti (atvaizduojamo asmens) privataus gyvenimo detales; tiesą sakant, piešinys buvo susijęs su jo, kaip politiko, visuomenine padėtimi“, ir kad „šiomis aplinkybėmis (atvaizduotas asmuo) turi tolerantiškiau reaguoti į kritiką“. Išnagrinėjęs įvairius susijusius interesus, EŽTT nustatė, kad neribotas draudimas toliau eksponuoti paveikslą būtų neproporcingas. EŽTT padarė išvadą, kad buvo pažeistas EŽTK 10 straipsnis.

Pagal Europos Sąjungos duomenų apsaugos teisę taip pat pripažįstama ypatinga mokslo vertė visuomenei. Pagal Bendrąjį duomenų apsaugos reglamentą ir atnaujintą 108-ąją konvenciją duomenis leidžiama saugoti ilgiau, jeigu jie bus tvarkomi tik mokslinių ar istorinių tyrimų tikslais. Be to, nepaisant pradinio konkrečios duomenų tvarkymo veiklos tikslo, paskesnis asmens duomenų naudojimas moksliniuose tyrimuose neturi būti laikomas nesuderinamu tikslu[123]. Tuo pat metu, siekiant apsaugoti duomenų subjektų teises ir laisves, būtina įgyvendinti tinkamas apsaugos priemones. ES arba valstybės narės teisėje gali būti nustatytos nuo duomenų subjektų teisių nukrypti leidžiančios nuostatos, pavyzdžiui, teisė susipažinti su duomenimis, juos ištaisyti, apriboti jų tvarkymą ir prieštarauti asmens duomenų tvarkymui mokslinių tyrimų, istoriniais arba statistiniais tikslais (taip pat žr. 6.1 skirsnį ir 9.4 skirsnį).

122 EŽTT, *Vereinigung bildender Künstler prieš Austriją*, Nr. 68354/01, 2007 m. sausio 25 d., 26 ir 34 punktai.

123 Bendrojo duomenų apsaugos reglamento 5 straipsnio 1 dalies b punktas ir atnaujintos 108-osios konvencijos 5 straipsnio 4 dalies b punktas.

1.3.5. Intelektinės nuosavybės apsauga

Teisė į nuosavybės apsaugą nustatyta EŽTK pirmojo protokolo 1 straipsnyje ir ES pagrindinių teisių Chartijos 17 straipsnio 1 dalyje. Vienas svarbus teisės į nuosavybę aspektas, kuris yra ypač svarbus duomenų apsaugai, yra intelektinės nuosavybės apsauga, kuri aiškiai nurodyta Chartijos 17 straipsnio 2 dalyje. Keliomis ES teisinės tvarkos direktyvomis siekiama veiksmingai apsaugoti intelektinę nuosavybę, visų pirma autorių teises. Intelektinė nuosavybė apima ne tik literatūros ir meno nuosavybę, bet ir patentą, prekių ženklą ir gretutines teises.

Kaip aiškiai nustatyta ESTT jurisprudencijoje, pagrindinę teisę į nuosavybės apsaugą būtina suderinti su kitų pagrindinių teisių apsauga, visų pirma teise į duomenų apsaugą[124]. Buvo atvejų, kai autorių teisių apsaugos institucijos reikalavo, kad prieigos prie interneto paslaugų teikėjai atskleistų dalijimosi interneto rinkmenomis platformų naudotojų tapatybę. Tokiose platformose interneto naudotojai gali nemokamai atsisiųsti muzikos kūrinius, nepaisant to, kad jiems taikoma autorių teisių apsauga.

Pavyzdys. Byla *Promusicae prieš Telefónica de España*[125] buvo susijusi su Ispanijos prieigos prie interneto paslaugų teikėjo *Telefónica* atsisakymo atskleisti ne pelno muzikos ir audiovizualinių įrašų gamintojų ir leidėjų organizacijai *Promusicae* tam tikrų asmenų, kuriems ji teikė prieigos prie interneto paslaugas, asmens duomenis. *Promusicae* prašė atskleisti informaciją, kad galėtų pradėti civilinę bylą prieš šiuos asmenis, kurie, jos teigimu, naudojosi rinkmenų mainų programa, suteikiančia prieigą prie fonogramų, kurių naudojimo teises turėjo *Promusicae* nariai.

Ispanijos teismas perdavė klausimą ESTT klausdamas, ar tokie asmens duomenys turi būti perduoti pagal Bendrijos teisę, atsižvelgiant į nagrinėjamą civilinę bylą, siekiant užtikrinti veiksmingą autorių teisių apsaugą. Jis rėmėsi direktyvomis 2000/31/EB, 2001/29/EB ir 2004/48/EB, skaitydamas jas kartu su Chartijos 17 ir 47 straipsniais. ESTT padarė išvadą, kad šiomis trimis direktyvomis, taip pat E. privatumo direktyva (Direktyva 2002/58/EB) valstybėms narėms nedraudžiama nustatyti pareigos atskleisti asmens duomenis civilinėse bylose siekiant užtikrinti veiksmingą autorių teisių apsaugą.

124 EŽTT, C-275/06, *Productores de Música de España (Promusicae) prieš Telefónica de España SAU* (DK), 2008 m. sausio 29 d., 62–68 punktai.

125 *Ten pat*, 54 ir 60 punktai.

Todėl ESTT atkreipė dėmesį į tai, kad byloje buvo keliamas klausimas dėl poreikio suderinti įvairių pagrindinių teisių, t. y. teisės į privatų gyvenimą, apsaugos reikalavimus su teisėmis į nuosavybės apsaugą ir veiksmingą teisių gynimą.

Jis padarė išvadą, kad „perkeldamos minėtas direktyvas, valstybės narės privalo užtikrinti, kad bus vadovaujamasi tokiu jų aiškinimu, kuris leistų užtikrinti teisingą pusiausvyrą tarp įvairių Bendrijos teisės sistemos saugomų pagrindinių teisių. Be to, įgyvendindamos šias direktyvas perkeliančias priemones valstybių narių valdžios institucijos ir teismai privalo ne tik aiškinti savo nacionalinę teisę taip, kad ji atitiktų Bendrijos teisę, bet ir užtikrinti, kad nebūtų vadovaujamasi tokiu jų aiškinimu, kuris pažeistų minėtas pagrindines teises arba kitus bendruosius Bendrijos teisės principus, kaip antai proporcingumo principas“[126].

Pavyzdys. Byla *Bonnier Audio AB ir kt. prieš Perfect Communication Sweden AB*[127] buvo susijusi su intelektinės nuosavybės teisių ir asmens duomenų apsaugos teisių pusiausvyra. Pareiškėjai – penkios leidybos įmonės, turinčios autorių teises į 27 garso knygas, – iškėlė bylą Švedijos teisme, teigdamos, kad šios autorių teisės buvo pažeistos naudojant FTP serverį (rinkmenų perdavimo protokolą, kuris sudaro sąlygas dalytis rinkmenomis ir perduoti duomenis internetu). Pareiškėjai prašė, kad interneto paslaugų teikėjas atskleistų asmens, kuris naudoja IP adresą, iš kurio buvo išsiųstos rinkmenos, vardą, pavardę ir adresą. Interneto paslaugų teikėjas „ePhone“ nesutiko su pareiškėju ir teigė, kad jis pažeidė Direktyvą 2006/24/EB (Duomenų saugojimo direktyva, kuri pripažinta negaliojančia 2014 m.).

Švedijos teismas perdavė klausimą ESTT, klausdamas, ar Direktyva 2006/24/EB draudžiama taikyti Direktyvos 2004/48/EB (Intelektinės nuosavybės teisių gynimo direktyva) 8 straipsniu pagrįstą nacionalinę nuostatą, pagal kurią leidžiama nustatyti draudimą, reikalaujantį interneto paslaugų teikėją perduoti autorių teisių turėtojams informaciją apie abonentus, kurių IP adresai tariamai buvo naudojami darant pažeidimus. Klausimas buvo grindžiamas prielaida, kad pareiškėjas pateikė aiškių tam tikros autorių teisės pažeidimo įrodymų ir kad priemonė yra proporcinga.

126 *Ten pat*, 65 ir 68 punktai; taip pat žr. ESTT, C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) prieš Netlog NV*, 2012 m. vasario 16 d.

127 ESTT, C-461/10, *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB prieš Perfect Communication Sweden AB*, 2012 m. balandžio 19 d.

ESTT nurodė, kad Direktyvoje 2006/24/EB buvo reglamentuojamas tik elektroninių ryšių paslaugų teikėjo sukurtų duomenų tvarkymas ir saugojimas siekiant sunkių nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas vykdymo tikslais ir perduoti juos nacionalinėms institucijoms. Todėl nacionalinė nuostata, kuria į nacionalinę teisę perkeliama Intelektinės nuosavybės teisių gynimo direktyva, nepatenka į Direktyvos 2006/24/EB taikymo sritį, todėl ji nėra draudžiama pagal tą direktyvą[128].

Kalbant apie atitinkamo vardo, pavardės ir adreso perdavimą, kurio prašė pareiškėjai, pažymėtina, kad ESTT nusprendė, jog toks veiksmas reiškia asmens duomenų tvarkymą ir patenka į Direktyvos 2002/58/EB (E. privatumo direktyva) taikymo sritį. Jis taip pat pažymėjo, kad tuos duomenis buvo reikalaujama perduoti civilinėje byloje autorių teisių turėtojo naudai, siekiant užtikrinti veiksmingą autorių teisių apsaugą, todėl, atsižvelgiant į pagrindinį duomenų perdavimo tikslą, toks perdavimas patenka į Direktyvos 2004/48/EB taikymo sritį[129].

ESTT padarė išvadą, kad direktyvas 2002/58/EB ir 2004/48/EB būtina aiškinti kaip nedraudžiančias priimti tokių nacionalinės teisės aktų, kurie, pavyzdžiui, nagrinėjami pagrindinėje byloje, jeigu tokiu teisės aktu nacionaliniam teismui, kuriame iškelta byla, leidžiama priimti nutartį dėl asmens duomenų atskleidimo, siekiant įvertinti nagrinėjamus prieštaraujančius interesus, remiantis kiekvienos bylos faktinėmis aplinkybėmis, ir tinkamai atsižvelgiant į proporcingumo principo reikalavimus.

1.3.6. Duomenų apsauga ir ekonominiai interesai

Skaitmeniniame arba didžiųjų duomenų amžiuje duomenys apibūdinami kaip ekonomikos „naujoji nafta“, padedanti skatinti inovacijas ir kūrybiškumą[130]. Dauguma įmonių sukūrė patikimus verslo modelius, susijusius su duomenų tvarkymu, ir toks tvarkymas dažnai apima asmens duomenis. Tam tikros įmonės gali manyti, kad konkrečios asmens duomenų apsaugos taisyklės praktiškai gali sukelti pernelyg sudėtingas prievoles, kurios galėtų turėti įtakos jų ekonomikos interesams. Todėl kyla

128 *Ten pat*, 40–41 punktai.

129 *Ten pat*, 52–54 punktai. Taip pat žr. ESTT, C-275/06, *Productores de Música de España (Promusicae) prieš Telefónica de España SAU* (DK), 2008 m. sausio 29 d., 58 punktas.

130 Žr., pvz., *Financial Times* (2016 m.), *Data is the new oil… who's going to own it?*, 2016 m. lapkričio 16 d.

klausimas, ar duomenų valdytojų ir duomenų tvarkytojų arba plačiosios visuomenės interesais gali būti pateisinamas teisės į duomenų apsaugą apribojimas.

Pavyzdys. Byloje *Google Spain*[131] ESTT nusprendė, kad tam tikromis aplinkybėmis asmenys turi teisę prašyti, kad paieškos sistemos pašalintų paieškos rezultatus iš savo paieškos rodyklės. Dėstydamas savo argumentus, ESTT atkreipė dėmesį į tai, kad naudojant paieškos sistemas ir į sąrašą įtrauktus paieškos rezultatus, galima sudaryti išsamų asmens profilį. Ši informacija gali būti susijusi su svarbiu asmens privataus gyvenimo aspektu ir be paieškos sistemos jos nebūtų galima lengvai rasti ar tarpusavyje susieti. Taigi tai gali būti rimtas duomenų subjektų pagrindinių teisių į privatumą ir asmens duomenų apsaugą apribojimas.

Paskui ESTT nagrinėjo, ar apribojimą buvo galima pateisinti. Dėl paieškos sistemos įmonės ekonominio intereso tvarkyti duomenis ESTT nurodė, kad „vien paieškos [sistemos] eksploatuotojo ekonominio intereso tvarkyti tokius duomenis nepakanka tam, kad būtų galima <...> pateisinti [apribojimą]“ ir kad „paprastai“ Chartijos 7 ir 8 straipsniuose nustatytos pagrindinės teisės yra viršesnės už tokį plačiosios visuomenės ekonominį interesą rasti tą informaciją atlikus paiešką pagal duomenų subjekto vardą ir pavardę[132].

Vienas iš pagrindinių Europos duomenų apsaugos teisės aspektų yra suteikti asmenims didesnę savo asmens duomenų kontrolę. Ypač skaitmeniniame amžiuje trūksta pusiausvyros tarp verslo subjektų, kurie tvarko didžiuosius asmens duomenis ir turi galimybę su jais susipažinti, įgaliojimų ir asmenų, kuriems priklauso šie asmens duomenys, įgaliojimų kontroliuoti savo informaciją. Nustatydamas duomenų apsaugos ir ekonominių interesų, pavyzdžiui, trečiųjų šalių interesų, susijusių su uždarosiomis akcinėmis bendrovėmis ir akcinėmis bendrovėmis, pusiausvyrą, ESTT kiekvieną atvejį vertina atskirai, kaip matyti iš sprendimo *Manni*.

131 ESTT, C-131/12, *Google Spain SL, Google Inc prieš Agencia Española de Protección de Datos (AEPD), Mario Costeja González* (DK), 2014 m. gegužės 13 d.

132 *Ten pat*, 81 ir 97 punktai.

Pavyzdys. Byla *Manni*[133] buvo susijusi su asmens duomenų įtraukimu į viešą prekybos registrą. S. Manni prašė Lečės prekybos rūmų ištrinti jo asmens duomenis iš to registro po to, kai išsiaiškino, kad potencialūs klientai ieškojo informacijos registre ir matė, kad jis buvo įmonės, kurios bankrotas buvo paskelbtas daugiau nei prieš dešimt metų, administratorius. Ši informacija pakenkė potencialiems jo klientams ir galėjo turėti neigiamą poveikį jo komerciniams interesams.

ESTT buvo prašoma nustatyti, ar toje byloje pagal ES teisę buvo pripažįstama teisė reikalauti ištrinti duomenis. Prieidamas prie šios išvados, jis derino ES duomenų apsaugos taisykles ir S. Manni komercinį interesą pašalinti informaciją apie jo ankstesnės įmonės bankrotą su viešuoju interesu susipažinti su informacija. ESTT tinkamai atsižvelgė į faktą, kad pareiga atskleisti viešam registrui informaciją apie įmones buvo nustatyta įstatyme, visų pirma ES direktyvoje, siekiant sudaryti sąlygas trečiosioms šalims lengviau susipažinti su informacija apie įmonę. Atskleidimas buvo svarbus siekiant apsaugoti trečiųjų šalių, kurios gali norėti užsiimti verslu su konkrečia įmone, interesus, nes vienintelės apsaugos priemonės, kurias akcinės bendrovės ir uždarosios akcinės bendrovės siūlo trečiosioms šalims, yra jų turtas. Todėl „atskleidimas tretiesiems asmenims turi suteikti galimybę susipažinti su bendrovės pagrindiniais dokumentais ir sužinoti kai kuriuos su ja susijusius duomenis, ypač duomenis apie asmenis, kurie yra įgalioti prisiimti įsipareigojimų bendrovės vardu“[134].

Atsižvelgdamas į teisėto tikslo, kurio siekia registras, svarbą, ESTT nusprendė, kad S. Manni neturėjo teisės ištrinti savo asmens duomenis, nes poreikis apsaugoti trečiųjų šalių interesus, susijusius su akcinėmis bendrovėmis ir uždarosiomis akcinėmis bendrovėmis, ir užtikrinti teisinį tikrumą, sąžiningą prekybą, taigi ir tinkamą vidaus rinkos veikimą, buvo viršesnis už jo teises pagal duomenų apsaugos teisės aktus. Tai ypač pasakytina apie tai, kad asmenys, kurie nusprendžia dalyvauti prekyboje per akcinę bendrovę arba uždarąją akcinę bendrovę, žino, kad privalo atskleisti informaciją, susijusią su jų tapatybe ir funkcijomis.

133 ESTT, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce prieš Salvatore Manni*, 2017 m. kovo 9 d.

134 *Ten pat*, 49 punktas.

Nors ir nustatęs, kad šiuo atveju nėra pagrindo reikalauti ištrinti duomenis, ESTT pripažino, kad egzistuoja teisė prieštarauti duomenų tvarkymui, pažymėdamas: „vis dėlto negalima atmesti galimybės, kad gali susiklostyti konkrečios situacijos, kai remiantis privalomais ir teisėtais pagrindais, susijusiais su konkrečia duomenų subjekto padėtimi, galimybė susipažinti su įmonių registre esančiais su tuo asmeniu susijusiais asmens duomenimis pasibaigus pakankamai ilgam laikotarpiui <...> bus apribota taip, kad susipažinti su šiais duomenimis bus leista tik tretiesiems asmenims, įrodžiusiems, kad turi konkretų interesą tai padaryti“[135].

ESTT nurodė, kad būtent nacionaliniai teismai kiekvienoje byloje, atsižvelgdami į visas su atitinkamu asmeniu susijusias aplinkybes, turi įvertinti teisėtų ir privalomų pagrindų, kuriais remiantis išimtiniais atvejais būtų pateisinama trečiųjų šalių galimybė susipažinti su įmonių registruose esančiais asmens duomenimis, buvimą arba nebuvimą. Tačiau jis paaiškino, kad S. Manni byloje vien faktas, kad jo asmens duomenų, esančių registre, atskleidimas tariamai turėjo poveikį jo klientūrai, negalėjo būti laikomas tokiu teisėtu ir privalomu pagrindu. Potencialūs S. Manni klientai turi teisėtą interesą gauti informaciją, susijusią su jo ankstesnės įmonės bankrotu.

S. Manni ir kitų į registrą įtrauktų asmenų pagrindinių teisių į privatų gyvenimą ir asmens duomenų apsaugą, garantuojamą pagal Chartijos 7 ir 8 straipsnius, apribojimas atitiko bendrojo intereso tikslą ir buvo būtinas bei proporcingas.

Todėl byloje *Manni* ESTT nusprendė, kad teisės į duomenų apsaugą ir privatumą nebuvo viršesnės už trečiųjų šalių interesą susipažinti su įmonių registre esančia informacija apie akcines bendroves ir uždarąsias akcines bendroves.

135 *Ten pat*, 60 punktas.

2

Duomenų apsaugos terminija

ES	Reglamentuojami klausimai	ET
Asmens duomenys		
Bendrojo duomenų apsaugos reglamento 4 straipsnio 1 punktas Bendrojo duomenų apsaugos reglamento 4 straipsnio 5 punktas ir 5 straipsnio 1 dalies e punktas Bendrojo duomenų apsaugos reglamento 9 straipsnis ESTT, sujungtos bylos C-92/09 ir C-93/09, *Volker und Markus Schecke GbR ir Hartmut Eifert prieš Land Hessen* (DK), 2010 m. ESTT, C-275/06, *Productores de Música de España (Promusicae) prieš Telefónica de España SAU* (DK), 2008 m. ESTT, C-70/10, *Scarlet Extended SA prieš Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 2011 m. ESTT, C-582/14, *Patrick Breyer prieš Bundesrepublik Deutschland*, 2016 m. ESTT, sujungtos bylos C-141/12 ir C-372/12, *YS prieš Minister voor Immigratie, Integratie en Asiel* ir *Minister voor Immigratie, Integratie en Asiel prieš M ir S*, 2014 m.	**Duomenų apsaugos teisinė apibrėžtis**	Atnaujintos 108-osios konvencijos 2 straipsnio a punktas EŽTT, *Bernh Larsen Holding AS ir kiti prieš Norvegiją*, Nr. 24117/08, 2013 m. EŽTT, *Uzun prieš Vokietiją*, Nr. 35623/05, 2010 m. EŽTT, *Amann prieš Šveicariją* (DK), Nr. 27798/95, 2000 m.

ES	Reglamentuojami klausimai	ET
ESTT, *Criminal proceedings against Bodil Lindqvist*, C-101/01, 2003 m.	**Specialios asmens duomenų kategorijos (neskelbtini duomenys)**	Atnaujintos 108-osios konvencijos 6 straipsnio 1 dalis
ESTT, C-434/16, *Peter Nowak prieš Data Protection Commissioner*, 2017 m.	**Anoniminti asmens duomenys ir asmens duomenys, kuriems suteikti pseudonimai**	Atnaujintos 108-osios konvencijos 5 straipsnio 4 dalies e punktas Atnaujintos 108-osios konvencijos aiškinamosios ataskaitos 50 punktas
Duomenų tvarkymas		
Bendrojo duomenų apsaugos reglamento 4 straipsnio 2 punktas ESTT, C-212/13, *František Ryneš prieš Úřad pro ochranu osobních údajů*, 2014 m. ESTT, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce prieš Salvatore Manni*, 2017 m. ESTT, C-101/01, *Criminal proceedings against Bodil Lindqvist*, 2003 m. ESTT, C-131/12, *Google Spain SL, Google Inc. prieš Agencia Española de Protección de Datos (AEPD), Mario Costeja González* (DK), 2014 m.	**Apibrėžtys**	Atnaujintos 108-osios konvencijos 2 straipsnio b ir c punktai
Duomenų naudotojai		
Bendrojo duomenų apsaugos reglamento 4 straipsnio 7 punktas ESTT, C-212/13, *František Ryneš prieš Úřad pro ochranu osobních údajů*, 2014 m. ESTT, C-1318/12, *Google Spain SL, Google Inc.prieš Agencia Española de Protección de Datos (AEPD), Mario Costeja González* (DK), 2014 m.	**Duomenų valdytojas**	Atnaujintos 108-osios konvencijos 2 dalies d punktas Rekomendacijos dėl profiliavimo1 straipsnio g punktas*
Bendrojo duomenų apsaugos reglamento 4 straipsnio 8 punktas	**Duomenų tvarkytojas**	Atnaujintos 108-osios konvencijos 2 straipsnio f punktas Rekomendacijos dėl profiliavimo 1 straipsnio h punktas

ES	Reglamentuojami klausimai	ET
Bendrojo duomenų apsaugos reglamento 4 straipsnio 9 punktas	Gavėjas	Atnaujintos 108-osios konvencijos 2 dalies e punktas
Bendrojo duomenų apsaugos reglamento 4 straipsnio 10 punktas	Trečioji šalis	
Sutikimas		
Bendrojo duomenų apsaugos reglamento 4 straipsnio 11 punktas ir 7 straipsnis ESTT, C-543/09, *Deutsche Telekom AG prieš Bundesrepublik Deutschland*, 2011 m. ESTT, C-536/15, *Tele2 (Netherlands) BV ir kt. prieš Autoriteit Consument en Markt (AMC)*, 2017 m.	Galiojančio sutikimo apibrėžtis ir reikalavimai	Atnaujintos 108-osios konvencijos 5 straipsnio 2 dalis Rekomendacijos dėl medicininių duomenų 6 straipsnis ir įvairios paskesnės rekomendacijos EŽTT, *Elberte prieš Latviją*, Nr. 61243/08, 2015 m.

Pastaba. Europos Tarybos Ministrų Kabinetas (2010), Ministrų Komiteto rekomendacija CM/Rec(2010)13 valstybėms narėms dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu profiliavimo kontekste (Rekomendacija dėl profiliavimo), 2010 m. lapkričio 23 d.*

2.1. Asmens duomenys

Pagrindiniai faktai

- Asmens duomenys – tai duomenys, susiję su asmeniu, kurio tapatybė yra nustatyta arba gali būti nustatyta, t. y. duomenų subjektu.
- Siekdamas išsiaiškinti, ar galima nustatyti fizinio asmens tapatybę, duomenų valdytojas arba kitas asmuo turėtų atsižvelgti į visas pagrįstas priemones, kurios gali būti naudojamos, pavyzdžiui, išskyrimą, siekiant tiesiogiai arba netiesiogiai nustatyti fizinio asmens tapatybę.
- Autentifikavimas – tai įrodymas, kad tam tikras asmuo turi tam tikrą tapatybę ir (arba) yra įgaliotas vykdyti tam tikrą veiklą.
- Esama specialių duomenų kategorijų, vadinamųjų neskelbtinų duomenų, kurie išvardyti atnaujintoje 108-ojoje konvencijoje ir ES duomenų apsaugos teisėje, kuriems būtina taikyti griežtesnę apsaugą, todėl jiems taikomos specialios teisinės taisyklės.
- Duomenys yra anoniminami, jeigu jie nebesusiję su asmeniu, kurio tapatybė nustatyta arba gali būti nustatyta.

- Pseudonimų suteikimas – tai priemonė, kurią naudojant duomenų negalima priskirti duomenų subjektui neturint papildomos informacijos, kuri laikoma atskirai. „Raktą“, kuris sudaro sąlygas pakartotinai nustatyti duomenų subjektų tapatybę, privaloma laikyti atskirai ir saugiai. Duomenys, kuriems buvo suteikti pseudonimai, išlieka asmens duomenimis. ES teisėje sąvoka „pseudoniminiai duomenys“ nevartojama.
- Anonimintai informacijai duomenų apsaugos principai ir taisyklės netaikomi. Tačiau jie taikomi duomenims, kuriems buvo suteikti pseudonimai.

2.1.1. Pagrindiniai asmens duomenų koncepcijos aspektai

Pagal ES teisę ir **ET teisę** „asmens duomenys“ apibrėžiami kaip informacija, susijusi su fiziniu asmeniu, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti[136]. Tai informacija apie asmenį, kurio tapatybė yra visiškai aiški arba ją galima nustatyti remiantis papildoma informacija. Siekdamas išsiaiškinti, ar asmens tapatybę galima nustatyti, duomenų valdytojas arba kitas asmuo privalo atsižvelgti į visas pagrįstas priemones, kurios gali būti naudojamos asmens tapatybei tiesiogiai arba netiesiogiai nustatyti, pavyzdžiui, tai išskyrimas, suteikiantis galimybę vertinti vieną asmenį atskirai nuo kito[137].

Jeigu tvarkomi tokio asmens duomenys, šis asmuo vadinamas „duomenų subjektu“.

Duomenų subjektas

Pagal ES teisę fiziniai asmenys yra vieninteliai subjektai, kuriems taikomos duomenų apsaugos taisyklės[138], be to, pagal Europos duomenų apsaugos teisę apsauga suteikiama tik gyviems žmonėms[139]. Bendrajame duomenų apsaugos reglamente (BDAR) asmens duomenys apibrėžiami kaip bet kuri informacija, susijusi su fiziniu asmeniu, kurio tapatybė nustatyta arba gali būti nustatyta.

ET teisėje, visų pirma atnaujintoje 108-ojoje konvencijoje, taip pat pateikiama nuoroda į asmenų apsaugą tvarkant jų asmens duomenis. Šiuo atveju asmens duomenys taip pat reiškia bet kokią informaciją, susijusią su asmeniu, kurio tapatybė

136 Bendrojo duomenų apsaugos reglamento 4 straipsnio 1 punktas; atnaujintos 108-osios konvencijos 2 straipsnio a punktas.

137 Bendrojo duomenų apsaugos reglamento 26 konstatuojamoji dalis.

138 *Ten pat*, 1 straipsnis.

139 *Ten pat*, 27 konstatuojamoji dalis. Taip pat žr. 29 straipsnio darbo grupės (2007 m.) *Nuomonę Nr. 4/2007 dėl asmens duomenų sąvokos*, WP 136, 2007 m. birželio 20 d., p. 22.

nustatyta arba gali būti nustatyta. Šis fizinis asmuo, kuris BDAR ir atnaujintoje 108-ojoje konvencijoje atitinkamai vadinamas anglų k. terminais *natural person* arba *individual*, duomenų apsaugos teisėje vadinamas duomenų subjektu.

Tam tikra apsauga suteikiama ir juridiniams asmenims. EŽTT jurisprudencijoje yra atvejų, kai sprendimai buvo priimti dėl juridinių asmenų prašymų, susijusių su tariamais jų teisės į apsaugą nuo jų duomenų naudojimo pagal ETŽK 8 straipsnį pažeidimais. EŽTK 8 straipsnis taikomas tiek teisei į privatų ir šeimos gyvenimą, tiek teisei į būsto neliečiamybę ir susirašinėjimo slaptumą. Todėl EŽTT bylas gali nagrinėti atsižvelgdamas veikiau į pastarąją teisę, o ne į teisę į privatų gyvenimą.

Pavyzdys. Byla *Bernh Larsen Holding AS ir kiti prieš Norvegiją*[140] buvo susijusi su trijų Norvegijos bendrovių skundu dėl mokesčių institucijos sprendimo, kuriuo jos įpareigotos pateikti mokesčių auditoriams visų duomenų, kuriuos jos laikė bendrai naudojamame kompiuterio serveryje, kopiją.

EŽTT nustatė, kad bendrovėms pareiškėjoms nustačius tokią prievolę buvo apribotos jų teisės į „būsto neliečiamybę“ ir „susirašinėjimo slaptumą“ pagal EŽTK 8 straipsnį. Tačiau EŽTT nustatė, kad mokesčių institucijos taikė veiksmingas ir tinkamas apsaugos nuo piktnaudžiavimo priemones: bendrovės pareiškėjos apie tai buvo informuotos gerokai anksčiau; jos dalyvavo atliekant patikrinimus vietoje ir galėjo pateikti pastabas, o užbaigus mokestinį patikrinimą dokumentai turėjo būti sunaikinti. Tokiomis aplinkybėmis reikėjo nustatyti tinkamą, viena vertus, bendrovių pareiškėjų teisės į būsto neliečiamybę ir susirašinėjimo slaptumą ir jų intereso užtikrinti jose dirbančių asmenų privatumą, ir, kita vertus, viešojo intereso užtikrinti veiksmingą mokestinį patikrinimą pusiausvyrą. Todėl EŽTT nusprendė, kad 8 straipsnis nebuvo pažeistas.

Pagal atnaujintą 108-ąją konvenciją duomenų apsauga visų pirma taikoma fiziniams asmenims; tačiau susitariančiosios šalys duomenų apsaugą gali savo nacionalinėje teisėje taikyti ir juridiniams asmenims, pavyzdžiui, įmonėms ir asociacijoms. Atnaujintos Konvencijos aiškinamojoje ataskaitoje teigiama, kad pagal nacionalinę teisę gali būti apsaugoti teisėti juridinių asmenų interesai, išplečiant Konvencijos

140 EŽTT, *Bernh Larsen Holding AS ir kiti prieš Norvegiją*, Nr. 24117/08, 2013 m. kovo 14 d. Tačiau taip pat žr. *Liberty ir kiti prieš Jungtinę Karalystę*, Nr. 58243/00, 2008 m. liepos 1 d.

taikymo sritį ir įtraukiant tokius subjektus[141]. **ES duomenų apsaugos teisėje** neaptariamas su juridiniais asmenimis susijusių duomenų tvarkymas, visų pirma tai pasakytina apie įmones, kurios yra įsisteigusios kaip juridiniai asmenys, įskaitant juridinio asmens pavadinimą ir formą ir jo kontaktinius duomenis[142]. Tačiau E. privatumo direktyva siekiama apsaugoti ryšių konfidencialumą ir teisėtus juridinių asmenų interesus, susijusius su didėjančiais automatinio duomenų apie abonentus ir naudotojus saugojimo ir tvarkymo pajėgumais[143]. E. privatumo reglamente apsauga taip pat praplečiama juridiniams asmenims.

Pavyzdys. Byloje *Volker und Markus Schecke ir Hartmut Eifert prieš Land Hessen*[144] ESTT dėl žemės ūkio paramos gavėjų asmens duomenų paskelbimo konstatavo, kad „juridinis asmuo gali remtis Chartijos 7 ir 8 straipsniuose numatyta apsauga, tik jei iš jo oficialaus pavadinimo galima nustatyti vieno ar kelių fizinių asmenų tapatybę. <...> [T]eisė į privat[ų] gyvenim[ą] tvarkant asmens duomenis siejama su visa informacija apie fizinį asmenį, kurio tapatybė nustatyta arba gali būti nustatyta <...>“[145].

Derindamas, viena vertus, ES interesą užtikrinti pagalbos skyrimo skaidrumą ir, kita vertus, asmenų, kurie gavo paramą, pagrindines teises į privatumą ir duomenų apsaugą, ESTT nusprendė, kad šių pagrindinių teisių apribojimas buvo neproporcingas. Jis manė, kad skaidrumo tikslas galėjo būti veiksmingai pasiektas priemonėmis, mažiau ribojančiomis atitinkamų asmenų teises. Tačiau nagrinėdamas informacijos apie paramą gavusius juridinius asmenis skelbimo proporcingumą ESTT padarė kitokią išvadą ir nusprendė, kad toks skelbimas neviršija proporcingumo principo ribų. ESTT pareiškė, kad „[t]eisės į asmens duomenų apsaugą apribojimas skirtingai veikia juridinius subjektus ir fizinius asmenis“[146]. Juridiniams asmenims buvo nustatytos griežtesnės pareigos skelbti su jais susijusią informaciją. ESTT manymu, dėl reikalavimo, kad nacionalinės institucijos prieš skelbdamos duomenis išnagrinėtų, ar kiekvieno paramą gaunančio juridinio asmens duomenys sudaro sąlygas nustatyti bet kokius susijusius fizinius asmenis, toms institucijoms tektų nepagrįsta

141 Atnaujintos 108-osios konvencijos aiškinamosios ataskaitos 30 punktas.

142 Bendrojo duomenų apsaugos reglamento 14 konstatuojamoji dalis.

143 E. privatumo direktyvos 7 konstatuojamoji dalis ir 1 straipsnio 2 dalis.

144 ESTT, sujungtos bylos C-92/09 ir C-93/09, *Volker und Markus Schecke GbR ir Hartmut Eifert prieš Land Hessen* (DK), 2010 m. lapkričio 9 d., 53 punktas.

145 *Ten pat*, 52–53 punktai.

146 *Ten pat*, 87 punktas.

administracinė našta. Todėl teisės aktais, kuriais reikalaujama bendrai skelbti duomenis apie juridinius asmenis, buvo užtikrinta tinkama konkuruojančių interesų pusiausvyra.

Duomenų pobūdis

Asmens duomenys gali būti bet kokios rūšies informacija, jeigu ji yra susijusi su asmeniu, kurio tapatybė nustatyta arba gali būti nustatyta.

Pavyzdys. Vadovo atliktas darbuotojo darbo rezultatų vertinimas, saugomas darbuotojo asmens byloje, yra darbuotojo asmens duomenys. Taip yra net tuo atveju, kai tokiame vertinime iš dalies arba visiškai perteikiama vadovo asmeninė nuomonė, pavyzdžiui, „darbuotojas nėra pasirengęs dirbti“, o ne konkretūs faktai, pavyzdžiui, „per pastaruosius šešis mėnesius darbuotojas penkias savaites nedirbo“.

Asmens duomenys apima informaciją apie asmens privatų gyvenimą, įskaitant informaciją apie profesinę veiklą, taip pat informaciją apie jo visuomeninį gyvenimą.

Byloje *Amann*[147] EŽTT sąvoką „asmens duomenys“ aiškino kaip neapsiribojančią tik su asmens privataus gyvenimo sritimi susijusiais klausimais. Ši sąvokos „asmens duomenys“ reikšmė taip pat yra svarbi BDAR.

Pavyzdys. Byloje *Volker und Markus Schecke ir Hartmut Eifert prieš Land Hessen*[148] ESTT pareiškė, kad „šiuo atžvilgiu nesvarbu, ar paskelbti duomenys yra susiję su profesionalaus pobūdžio veikla <...>. Europos Žmogaus Teisių Teismas, atsižvelgdamas į Konvencijos [EŽTK] 8 straipsnio aiškinimą, šiuo klausimu nusprendė, kad sąvoka „privatus gyvenimas“ neturi būti aiškinama ribojamai ir kad nėra jokios rimtos priežasties, kuria remiantis būtų galima pateisinti profesinio <...> pobūdžio veiklos nepriskyrimą privataus gyvenimo sąvokai“.

147 Žr. EŽTT, *Amann prieš Šveicariją*, Nr. 27798/95, 2000 m. vasario 16 d., 65 punktas.

148 ESTT, sujungtos bylos C-92/09 ir C-93/09, *Volker und Markus Schecke GbR ir Hartmut Eifert prieš Land Hessen* (DK), 2010 m. lapkričio 9 d.

Pavyzdys. Sujungtose bylose *YS prieš Minister voor Immigratie, Integratie en Asiel* ir *Minister voor Immigratie, Integratie en Asiel prieš M ir S*[149] ESTT pareiškė, kad sprendimo dėl Imigracijos ir natūralizacijos tarnybos projekte pateikta teisinė analizė, kurioje buvo aptariami prašymai išduoti leidimą gyventi, pati savaime nereiškia asmens duomenų, net jeigu joje ir būtų tam tikrų asmens duomenų.

EŽTT jurisprudencijoje, susijusioje su EŽTK 8 straipsniu, patvirtinama, kad gali būti sudėtinga visiškai atskirti privataus ir profesinio gyvenimo klausimus[150].

Pavyzdys. Byloje *Bărbulescu prieš Rumuniją*[151] pareiškėjas buvo atleistas iš darbo dėl darbdavio interneto naudojimo darbo valandomis, pažeidžiant vidaus taisykles. Darbdavys stebėjo jo ryšius ir nacionaliniame teisme nagrinėjant bylą pateikė įrašus, kuriuose buvo matomos išimtinai privataus pobūdžio žinutės. Prieidamas prie išvados, kad turi būti taikomas 8 straipsnis, EŽTT neatsakė į klausimą, ar, atsižvelgiant į darbdavio ribojamąsias nuostatas, pareiškėjas pagrįstai galėjo tikėtis privatumo, tačiau bet kuriuo atveju nusprendė, kad dėl darbdavio nurodymų darbo vietoje negali visiškai nevykti privatus socialinis gyvenimas. Iš esmės susitariančiosioms valstybėms turėjo būti suteikta plati veiksmų laisvė vertinant poreikį nustatyti teisinę sistemą, reglamentuojančią sąlygas, kuriomis darbdavys galėtų reguliuoti savo darbuotojų neprofesinius elektroninius ar kitokios formos ryšius darbo vietoje. Vis dėlto nacionalinės institucijos turėjo užtikrinti, kad darbdavio nustatytos susirašinėjimo ir kitų ryšių stebėsenos priemonės, nepaisant jų masto ir trukmės, taip pat apimtų tinkamas ir pakankamas apsaugos nuo piktnaudžiavimo priemones. Proporcingumas ir procedūrinės garantijos prieš savivalę buvo esminės ir EŽTT nustatė įvairius šiomis aplinkybėmis svarbius veiksnius. Tokie veiksniai apėmė, pavyzdžiui, darbdavio vykdomos darbuotojų stebėsenos mastą ir darbuotojų privatumo apribojimo laipsnį, pasekmes darbuotojui ir tai, ar buvo numatytos tinkamos apsaugos priemonės. Be to, nacionalinės institucijos turėjo užtikrinti, kad darbuotojas, kurio ryšiai buvo stebimi, turėtų galimybę pasinaudoti teisių gynimo priemone teisminėje institucijoje, kuri turi jurisdikciją bent jau iš esmės nustatyti, kaip buvo laikomasi

149 ESTT, sujungtos bylos C-141/12 ir C-372/12, *YS prieš Minister voor Immigratie, Integratie en Asiel* ir *Minister voor Immigratie, Integratie en Asiel prieš M ir S*, 2014 m. liepos 17 d., 39 punktas.

150 Žr., pvz., EŽTT, *Rotaru prieš Rumuniją* (DK), Nr. 28341/95, 2000 m. gegužės 4 d., 43 punktas; EŽTT, *Niemietz prieš Vokietiją*, Nr. 13710/88, 1992 m. gruodžio 16 d., 29 punktas.

151 EŽTT, *Bărbulescu prieš Rumuniją* (DK), Nr. 61496/08, 2017 m. rugsėjo 5 d., 121 punktas.

šių išdėstytų kriterijų ir ar ginčijamos priemonės buvo teisėtos. Šioje byloje EŽTT nustatė, kad 8 straipsnis buvo pažeistas, nes nacionalinės institucijos neužtikrino tinkamos pareiškėjo teisės į jo privatų gyvenimą ir susirašinėjimo slaptumą apsaugos, taigi nesugebėjo nustatyti tinkamos aptariamų interesų pusiausvyros.

Pagal ES teisę ir **ET teisę** informacija apima asmens duomenis, jeigu:

- remiantis šia informacija nustatoma arba gali būti nustatyta asmens tapatybė, arba

- asmuo, nors jo tapatybė ir nenustatyta, remiantis šia informacija, gali būti išskirtas taip, kad duomenų subjekto tapatybę galima išsiaiškinti atliekant papildomą paiešką.

Abiejų rūšių informacija yra saugoma lygiai taip pat, kaip pagal Europos duomenų apsaugos teisę. Galimybė tiesiogiai arba netiesiogiai nustatyti asmenų tapatybę turi būti nuolat vertinama, „turint omenyje duomenų tvarkymo metu turimas technologijas bei technologinę plėtrą“[152]. EŽTT ne kartą nurodė, kad „asmens duomenų“ sąvoka pagal EŽTK yra tokia pati kaip ir 108-ojoje konvencijoje, visų pirma atsižvelgiant į sąlygą, susijusią su asmenimis, kurių tapatybė nustatyta arba kurių tapatybę galima nustatyti[153].

BDAR nustatyta, kad fizinio asmens tapatybę galima nustatyti, kai jo „tapatybę tiesiogiai arba netiesiogiai galima nustatyti, visų pirma pagal identifikatorių, kaip antai vardą ir pavardę, asmens identifikavimo numerį, buvimo vietos duomenis ir interneto identifikatorių arba pagal vieną ar kelis to <...> asmens fizinės, fiziologinės, genetinės, psichinės, ekonominės, kultūrinės ar socialinės tapatybės požymius“[154]. Taigi tapatybei nustatyti reikia informacijos, kuri apibūdintų asmenį taip, kad jį būtų galima atskirti nuo visų kitų asmenų ir atpažinti kaip asmenį. Asmens vardas ir pavardė yra pagrindinis tokios apibūdinamosios informacijos pavyzdys, kuria remiantis galima tiesiogiai nustatyti asmens tapatybę. Tam tikrais atvejais kiti požymiai gali turėti panašų poveikį kaip vardas ir pavardė, todėl asmens tapatybę galima nustatyti netiesiogiai. Telefono numeris, socialinio draudimo numeris ir transporto priemonės registracijos numeris yra visi informacijos, kuria remiantis

152 Bendrojo duomenų apsaugos reglamento 26 konstatuojamoji dalis.

153 Žr. EŽTT, *Amann prieš Šveicariją* (DK), Nr. 27798/95, 2000 m. vasario 16 .d, 65 punktas.

154 Bendrojo duomenų apsaugos reglamento 4 straipsnio 1 punktas.

galima nustatyti asmens tapatybę, pavyzdžiai. Taip pat galima naudoti požymius, pavyzdžiui, kompiuterizuotas rinkmenas, slapukus ir interneto srauto stebėjimo priemones, kad būtų galima nustatyti asmenų elgseną ir įpročius. Kaip paaiškinta 29 straipsnio darbo grupės nuomonėje, „[n]et ir nesiteiraujant asmens vardo, pavardės ir adreso jį įmanoma priskirti kokiai nors kategorijai pagal socialinius ir ekonominius, psichologinius, filosofinius ar kitus kriterijus bei priskirti jam tam tikrus sprendimus, nes dėl asmens kontaktinės priemonės (kompiuterio) nėra būtina atskleisti asmens tapatybės siaurąja prasme“[155]. Asmens duomenų apibrėžtis pagal ET ir ES yra pakankamai plati, kad apimtų visas galimybes (taigi ir visus tapatybės nustatymo laipsnius) nustatyti tapatybę.

Pavyzdys. Sprendime *Promusicae prieš Telefónica de España*[156] ESTT pareiškė, kad „nebuvo ginčyta, kad *Promusicae* prašomas pagrindinėje byloje aptariamų tam tikrų [atitinkamos internetinės dalijimosi rinkmenomis platformos] naudotojų vardų bei pavardžių ir fizinio adreso nurodymas reiškia padaryti asmens duomenis, t. y. informaciją, susijusią su fiziniu asmeniu, kurio tapatybė yra nustatyta arba gali būti nustatyta, kaip numatyta Direktyvos 95/46/EB 2 straipsnio a punkte [dabartinis BDAR 4 straipsnio 1 punktas] pateikiamame apibrėžime, prieinamus. Toks duomenų, kuriuos, *Promusicae* teigimu, saugo *Telefónica*, o to ši neginčija, pateikimas yra asmens duomenų tvarkymas“[157].

Pavyzdys. Byla *Scarlet Extended SA prieš Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*[158] buvo susijusi su tuo, kad interneto paslaugų teikėjas *Scarlet* atsisakė įdiegti elektroninių ryšių filtravimo sistemą, kurioje naudojama dalijimosi rinkmenomis programinė įranga, siekiant užkirsti kelią dalijimuisi rinkmenomis, kuris pažeidžia autorių teises, saugomas SABAM – valdymo įmonės, atstovaujančios autoriams, kompozitoriams ir redaktoriams. ESTT nusprendė, kad naudotojų IP adresai „yra saugomų asmens duomenų dalis, nes leidžia tiksliai nustatyti tokius vartotojus“.

155 29 straipsnio duomenų apsaugos darbo grupė, *Nuomonė Nr. 4/2007 dėl asmens duomenų sąvokos*, WP 136, 2007 m. birželio 20 d., p. 15.

156 ESTT, C-275/06, *Productores de Música de España (Promusicae) prieš Telefónica de España SAU* (DK), 2008 m. sausio 29 d., 45 punktas.

157 Ankstesnės Direktyvos 95/46/EB 2 straipsnio b punktas, dabar – Bendrojo duomenų apsaugos reglamento 4 straipsnio 2 dalis.

158 ESTT, C-70/10, *Scarlet Extended SA prieš Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 2011 m. lapkričio 24 d., 51 punktas.

Kadangi dauguma vardų nėra unikalūs, asmens tapatybei nustatyti gali prireikti papildomų požymių, siekiant užtikrinti, kad asmuo nebūtų supainiotas su kitu asmeniu. Kartais, siekiant nustatyti asmens, su kuriuo yra susijusi informacija, tapatybę, gali prireikti derinti tiesioginius ir netiesioginius požymius. Dažnai naudojama gimimo data ir vieta. Be to, siekiant geriau atskirti piliečius, kai kuriose šalyse nustatyti personalizuoti numeriai. Perduoti mokesčių duomenys[159], duomenys apie prašymą išduoti leidimą gyventi pateikiantį asmenį, esantys administraciniame dokumente[160], ir dokumentai, susiję su bankininkystės ir patikėtinio santykiais[161], gali būti asmens duomenys. Technologijų amžiuje biometriniai duomenys, pavyzdžiui, pirštų atspaudai, skaitmeninės nuotraukos arba rainelės skenavimas, vietos nustatymo duomenys ir internetiniai požymiai, vis dažniau naudojami nustatant asmenų tapatybę.

Tačiau tam, kad būtų taikoma Europos duomenų apsaugos teisė, nėra jokio poreikio nustatyti faktinę duomenų subjekto tapatybę; pakanka, kad būtų galima nustatyti atitinkamo asmens tapatybę. Laikoma, kad asmens tapatybę galima nustatyti, jeigu yra pakankamai prieinamos informacijos, kuria remiantis galima tiesiogiai arba netiesiogiai nustatyti asmens tapatybę[162]. Pagal BDAR 26 konstatuojamąją dalį lyginamasis kriterijus yra tai, ar tikėtina, kad numatomiems informacijos naudotojams bus prieinamos ir administruojamos pagrįstos tapatybės nustatymo priemonės (žr. 2.3.2 skirsnį).

Pavyzdys. Vietos institucija nusprendžia rinkti duomenis apie vietos gatvėse greitį viršijančius automobilius. Ji fotografuoja automobilius, automatiškai įrašo laiką ir vietą, kad pateiktų duomenis kompetentingai institucijai, kuri skirtų baudą greitį viršijusiems asmenims. Duomenų subjektas pateikia skundą, kuriame teigia, kad duomenų apsaugos teisėje nėra teisinio pagrindo, kuriuo remdamasi vietos institucija galėtų rinkti tokius duomenis. Vietos institucija teigia, kad ji nerenka asmens duomenų. Pasak jos, valstybinio numerio ženklai yra anoniminiai. Vietos institucija neturi teisinių įgaliojimų susipažinti su bendrais transporto priemonės registracijos duomenimis, kad išsiaiškintų automobilio savininko arba vairuotojo tapatybę.

159 ESTT, C-201/14, *Smaranda Bara ir kt. prieš Casa Națională de Asigurări de Sănătate ir kt,* 2015 m. spalio 1 d.

160 ESTT, sujungtos bylos C-141/12 ir C-372/12, *YS prieš Minister voor Immigratie, Integratie en Asiel* ir *Minister voor Immigratie, Integratie en Asiel prieš M ir S*, 2014 m. liepos 17 d.

161 EŽTT, *M. N. ir kiti prieš San Mariną*, Nr. 28005/12, 2015 m. liepos 7 d.

162 Bendrojo duomenų apsaugos reglamento 4 straipsnio 1 punktas.

Šis argumentas neatitinka BDAR 26 konstatuojamosios dalies. Akivaizdu, kad duomenys renkami siekiant nustatyti greitį viršijusių asmenų tapatybę ir juos nubausti, todėl galima daryti prielaidą, kad asmenų tapatybę bus bandoma nustatyti. Nors vietos institucijos neturi tiesiogiai joms prieinamų tapatybės nustatymo priemonių, jos perduoda duomenis kompetentingai institucijai, policijai, kuri turi tokias priemones. 26 konstatuojamojoje dalyje taip pat aiškiai aprašomas atvejis, kai numatoma, kad asmens tapatybę gali bandyti nustatyti ne tik tiesioginis duomenų naudotojas, bet ir kiti duomenų gavėjai. Atsižvelgiant į 26 konstatuojamąją dalį, vietos institucijos veiksmai prilygsta duomenų apie asmenis, kurių tapatybę galima nustatyti, rinkimui, todėl tokiai veiklai reikalingas teisinis pagrindas pagal duomenų apsaugos teisę.

„Įsitikinant, ar tam tikros priemonės, pagrįstai tikėtina, galėtų būti naudojamos siekiant nustatyti fizinio asmens tapatybę, reikėtų atsižvelgti į visus objektyvius veiksnius, pavyzdžiui, sąnaudas ir laiko trukmę, kurių prireiktų tapatybei nustatyti, turint omenyje duomenų tvarkymo metu turimas technologijas bei technologinę plėtrą.“[163]

Pavyzdys. Byloje *Breyer prieš Bundesrepublik Deutschland*[164] ESTT nagrinėjo galimybės netiesiogiai nustatyti duomenų subjektų tapatybę sąvoką. Byla buvo susijusi su dinaminiais IP adresais, kurie pasikeičia kaskart, kai prie interneto prisijungiama iš naujo. Vokietijos federalinių institucijų administruojamos interneto svetainės užregistravo ir saugojo dinamiškus IP adresus, kad užkirstų kelią kibernetiniams išpuoliams ir prireikus inicijuotų baudžiamąjį procesą. Tik interneto paslaugų teikėjas, kuriuo naudojosi P. Breyer, turėjo papildomos informacijos, reikalingos jo tapatybei nustatyti.

ESTT laikėsi nuomonės, kad dinaminis IP adresas, kurį internetinių žiniasklaidos paslaugų teikėjas registruoja, kai asmuo prisijungia prie interneto svetainės, prie kurios teikėjas suteikė visuomenei prieigą, yra asmens duomenys, kai tik trečioji šalis – šiuo atveju interneto paslaugų teikėjas – turi papildomų duomenų, reikalingų asmens tapatybei nustatyti[165]. Jis nusprendė, kad „nereikalaujama, jog visa informacija, pagal kurią galima nustatyti duomenų subjekto tapatybę, būtų laikoma vieno asmens rankose“, kad informacija

163 *Ten pat*, 26 konstatuojamoji dalis.

164 ESTT, C-582/14, *Patrick Breyer prieš Bundesrepublik Deutschland*, 2016 m. spalio 19 d., 47–48 punktai.

165 Ankstesnės 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyvos 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo 2 straipsnio a punktas.

būtų laikoma asmens duomenimis. Interneto paslaugų teikėjo užregistruoto dinaminio IP adreso naudotojai tam tikrais atvejais gali būti nustatyti, pavyzdžiui, vykstant baudžiamajam procesui kibernetinių išpuolių atveju, padedant kitiems asmenims[166]. Pasak ESTT, kai paslaugų teikėjas „turi teisines priemones, leidžiančias nustatyti duomenų subjekto tapatybę pagal papildomus duomenis, kuriuos interneto paslaugų teikėjas turi apie tą asmenį“, tai yra „priemonė, kuri gali būti pagrįstai naudojama duomenų subjekto tapatybei nustatyti“. Todėl tokie duomenys laikomi asmens duomenimis.

Pagal ET teisę galimybė nustatyti tapatybę suprantama panašiai. Atnaujintos 108-osios konvencijos aiškinamojoje ataskaitoje pateikiamas panašus aprašymas: sąvoka „tapatybė gali būti nustatyta“ reiškia ne tik paties asmens civilinį ar teisinį statusą, bet ir tai, kas gali leisti vieną asmenį „individualizuoti“ arba išskirti iš kitų asmenų, todėl su juo gali būti elgiamasi skirtingai. Šis „individualizavimas“ galėtų būti atliekamas, pavyzdžiui, nurodant, kad asmuo yra „jis“ arba „ji“, arba nurodant prietaisą arba prietaisų derinį (kompiuteris, mobilusis telefonas, filmavimo kamera, žaidimų prietaisai ir pan.), susietą su identifikavimo numeriu, pseudonimu, biometriniais ar genetiniais duomenimis, vietos nustatymo duomenimis arba kitu identifikatoriumi[167]. Laikoma, kad asmens tapatybės negalima nustatyti, jeigu tam reikia nepagrįstai daug laiko, pastangų arba išteklių. Taip, pavyzdžiui, yra tuo atveju, kai duomenų subjekto tapatybei nustatyti reikėtų pernelyg sudėtingų, ilgų ir brangių operacijų. Kiekvienu konkrečiu atveju, atsižvelgiant į tokius veiksnius kaip duomenų tvarkymo tikslas, tapatybės nustatymo sąnaudos ir nauda, duomenų valdytojo tipas ir naudojama technologija, būtina įvertinti laiko, pastangų arba išteklių nepagrįstumą[168].

Kalbant apie formą, kuria asmens duomenys saugomi arba naudojami, svarbu pažymėti, kad nesvarbu, ar taikoma duomenų apsaugos teisė. Rašytiniuose arba žodiniuose pranešimuose gali būti asmens duomenų, taip pat vaizdų[169], įskaitant

166 ESTT, C-70/10, *Scarlet Extended SA prieš Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 2011 m. lapkričio 24 d., 47–48 punktai.

167 Atnaujintos 108-osios konvencijos aiškinamosios ataskaitos 18 punktas.

168 *Ten pat*, 17 punktas.

169 EŽTT, *Von Hannover prieš Vokietiją*, Nr. 59320/00, 2004 m. birželio 24 d.; EŽTT, *Sciacca prieš Italiją*, Nr. 50774/99, 2005 m. sausio 11 d.; ESTT, C-212/13, *František Ryneš prieš Úřad pro ochranu osobních údajů*, 2014 m. gruodžio 11 d.

apsauginės vaizdo stebėjimo sistemos (AVSS) įrašus[170] arba garsą[171]. Elektroninėmis priemonėmis įrašyta informacija ir popieriuje esanti informacija taip pat gali būti asmens duomenys. Net ir žmogaus audinio ląstelių mėginiai, kuriuose yra asmens DNR informacija, gali būti šaltinis, iš kurio išgaunami biometriniai duomenys[172], jeigu duomenys yra susiję su asmeniui būdingomis arba įgytomis savybėmis, jeigu juose pateikiama unikali informacija apie asmens sveikatą arba fiziologiją ir duomenys gaunami išanalizavus to asmens biologinį mėginį[173].

Anoniminimas

Remiantis BDAR ir atnaujintoje 108-ojoje konvencijoje nustatytu saugojimo apribojimo principu (jis išsamiau aptartas 3 skyriuje), duomenys turi būti laikomi „tokia forma, kad duomenų subjektų tapatybę būtų galima nustatyti ne ilgiau, nei tai yra būtina tais tikslais, kuriais asmens duomenys yra tvarkomi“[174]. Todėl duomenys turėtų būti ištrinti arba anoniminti, jei duomenų valdytojas norėjo juos saugoti, kai jų nebereikėjo ir jie nebeatitiko pradinio tikslo.

Duomenų anoniminimo procesas reiškia, kad iš asmens duomenų rinkinio pašalinama visa su tapatybės nustatymu susijusi informacija, kad nebebūtų galima nustatyti duomenų subjekto tapatybės[175]. Savo Nuomonėje Nr. 05/2014 29 straipsnio darbo grupė analizuoja įvairių anoniminimo metodų veiksmingumą ir ribas[176]. Ji pripažįsta galimą tokių metodų vertę, tačiau pabrėžia, kad tam tikri metodai nebūtinai visais atvejais veikia. Siekiant rasti optimalų sprendimą konkrečioje situacijoje, dėl tinkamo anoniminimo proceso turėtų būti sprendžiama kiekvienu konkrečiu atveju. Nepaisant naudojamo metodo, turi būti negrįžtamai užkirstas kelias tapatybės nustatymui. Tai reiškia, kad, norint anoniminti duomenis, informacijoje negali

170 EŽTT, *Peck prieš Jungtinę Karalystę*, Nr. 44647/98, 2003 m. sausio 28 d.; EŽTT, *Köpke prieš Vokietiją* (dec.), Nr. 420/07, 2010 m. spalio 5 d.; EDAPP (2010 m.), *EDAPP rekomendacijos dėl stebėjimo vaizdo kameromis*, 2010 m. kovo 17 d.

171 EŽTT, *P. G. ir J. H. prieš Jungtinę Karalystę*, Nr. 44787/98, 2001 m. rugsėjo 25 d., 59–60 punktai; EŽTT, *Wisse prieš Prancūziją*, Nr. 71611/01, 2005 m. gruodžio 20 d. (versija prancūzų kalba).

172 Žr. 29 straipsnio darbo grupės (2007 m.) *Nuomonę Nr. 4/2007 dėl asmens duomenų sąvokos*, WP 136, 2007 m. birželio 20 d., p. 9; Europos Taryba, Ministrų komiteto rekomendacija *Rec(2006)4* valstybėms narėms dėl mokslinių tyrimų žmogaus biologinių medžiagų srityje, 2006 m. kovo 15 d.

173 Bendrojo duomenų apsaugos reglamento 4 straipsnio 13 punktas.

174 *Ten pat*, 5 straipsnio 1 dalies e punktas; atnaujintos 108-osios konvencijos 5 straipsnio 4 dalies e punktas.

175 Bendrojo duomenų apsaugos reglamento 26 konstatuojamoji dalis.

176 29 straipsnio darbo grupė (2014 m.), *Nuomonė Nr. 05/2014 dėl nuasmeninimo metodų*, WP 216, 2014 m. balandžio 10 d.

būti palikta jokių elementų, kurie, dedant pagrįstas pastangas, galėtų padėti iš naujo nustatyti atitinkamo (-ų) asmens (-ų) tapatybę[177]. Pakartotinio tapatybės nustatymo riziką galima įvertinti atsižvelgiant į „laiką, pastangas ir išteklius, reikalingus atsižvelgiant į duomenų pobūdį, jų naudojimo aplinkybes, prieinamas pakartotinio tapatybės nustatymo technologijas ir susijusias išlaidas“[178].

Sėkmingai anoniminus duomenis, jie nebelaikomi asmens duomenimis ir duomenų apsaugos teisės aktai nebetaikomi.

BDAR nustatyta, kad asmuo arba organizacija, kontroliuojanti asmens duomenų tvarkymą, negali būti įpareigota saugoti, gauti ar tvarkyti papildomą informaciją, kad nustatytų duomenų subjekto tapatybę vien tam, kad būtų laikomasi reglamento. Tačiau šiai taisyklei taikoma svarbi išimtis – jeigu duomenų subjektas, siekdamas įgyvendinti savo teisę susipažinti su duomenimis, juos ištaisyti, ištrinti arba apriboti jų tvarkymą ir teisę į duomenų perkeliamumą, duomenų valdytojui pateikia papildomos informacijos, kuri sudaro sąlygas nustatyti jo tapatybę, tuomet šie duomenys, kurie anksčiau buvo anoniminti, vėl tampa asmens duomenimis[179].

Pseudonimų suteikimas

Asmens duomenyse yra požymių, pavyzdžiui, vardas, pavardė, gimimo data, lytis, adresas ar kiti duomenys, pagal kuriuos būtų galima nustatyti asmens tapatybę. Pseudonimų suteikimo asmens duomenims procesas reiškia, kad šie požymiai pakeičiami pseudonimu.

ES teisėje sąvoka „pseudonimų suteikimas“ apibrėžiama kaip „asmens duomenų tvarkymas taip, kad asmens duomenys nebegalėtų būti priskirti konkrečiam duomenų subjektui nesinaudojant papildoma informacija, jeigu tokia papildoma informacija yra saugoma atskirai ir jos atžvilgiu taikomos techninės bei organizacinės priemonės siekiant užtikrinti asmens duomenų nepriskyrimą fiziniam asmeniui, kurio tapatybė yra nustatyta arba kurio tapatybę galima nustatyti“[180]. Priešingai nei anoniminti duomenys, duomenys, kuriems suteikti pseudonimai, vis tiek yra asmens duomenys, todėl jiems taikomi duomenų apsaugos teisės aktai. Nors dėl

177 Bendrojo duomenų apsaugos reglamento 26 konstatuojamoji dalis.

178 Europos Taryba, 108-osios konvencijos (2017 m.) komitetas, *Rekomendacijos dėl asmenų apsaugos tvarkant asmens duomenis didžiųjų duomenų eroje*, 2017 m sausio 23 d., 6.2 punktas.

179 Bendrojo duomenų apsaugos reglamento 11 straipsnis.

180 *Ten pat*, 4 straipsnio 5 punktas.

pseudonimų suteikimo gali sumažėti duomenų subjektams kylanti saugumo rizika, tokiai veiklai BDAR vis tiek galioja.

BDAR pripažįstami įvairūs pseudonimų suteikimo panaudojimo būdai, kurie yra tinkama techninė priemonė duomenų apsaugai stiprinti, ir konkrečiai paminimi kaip duomenų tvarkymo struktūros ir saugumo užtikrinimo priemonė[181]. Pseudonimų suteikimas taip pat yra tinkama apsaugos priemonė, kuri galėtų būti naudojama tvarkant asmens duomenis kitais tikslais, nei jie buvo iš pradžių surinkti[182].

Pseudonimų suteikimas nėra aiškiai paminėtas **ET** atnaujintos 108-osios konvencijos teisinėje apibrėžtyje. Tačiau atnaujintos 108-osios konvencijos aiškinamojoje ataskaitoje aiškiai nurodyta, kad „pseudonimo arba bet kokio skaitmeninio identifikatoriaus ir (arba) skaitmeninės tapatybės naudojimas nelemia duomenų anoniminimo, nes duomenų subjektą vis dar galima nustatyti arba individualizuoti“[183]. Vienas iš būdų suteikti pseudonimus duomenims – duomenų šifravimas. Kai duomenims suteikiami pseudonimai, sąsaja su tapatybe nustatoma naudojant pseudonimą ir iššifravimo raktą. Be tokio rakto sunku nustatyti duomenis, kuriems suteikti pseudonimai. Tačiau asmenys, turintys teisę naudoti iššifravimo raktą, gali lengvai iš naujo nustatyti tapatybę. Ypač svarbu užtikrinti, kad šifravimo raktais nesinaudotų leidimo neturintys asmenys. Todėl „[p]seudoniminiai duomenys <...> turi būti laikomi asmens duomenimis <...>“, kuriems taikoma atnaujinta [108-oji] konvencija[184].

Tapatumo patvirtinimas

Tai yra procedūra, per kurią asmuo gali įrodyti, kad turi tam tikrą tapatybę ir (arba) yra įgaliotas atlikti tam tikrus veiksmus, pavyzdžiui, įeiti į saugomą zoną arba pasiimti pinigų iš banko sąskaitos. Tapatumo nustatymas gali būti užtikrintas lyginant biometrinius duomenis, pavyzdžiui, pase esančią nuotrauką ar pirštų atspaudus, su asmens, prisistačiusio, pavyzdžiui, imigracijos kontrolės metu, duomenimis[185]; arba paprašius pateikti informaciją, kurią turėtų žinoti tik tam tikros tapatybės arba atitinkamus įgaliojimus turintis asmuo, pavyzdžiui, asmeninį identifikavimo numerį (PIN) arba slaptažodį; arba pareikalavus pateikti tam tikrą atpažinimo ženklą, kurį turėtų turėti tik tam tikros tapatybės arba atitinkamus įgaliojimus turintis asmuo,

181 *Ten pat*, 25 straipsnio 1 punktas.

182 *Ten pat*, 6 straipsnio 4 punktas.

183 Atnaujintos 108-osios konvencijos aiškinamosios ataskaitos 18 punktas.

184 *Ten pat*.

185 *Ten pat*, 56–57 punktai.

pavyzdžiui, specialią lustinę kortelę arba banko seifo raktą. Be slaptažodžių arba lustinių kortelių, elektroniniai parašai, kurie kartais naudojami kartu su PIN kodais, yra priemonė, kurią naudojant visų pirma galima nustatyti elektroninius pranešimus siunčiančio asmens tapatybę ir patvirtinti jo tapatumą.

2.1.2. Specialios asmens duomenų kategorijos

Pagal ES teisę ir **ET teisę** esama specialių kategorijų asmens duomenų, kurių tvarkymas, atsižvelgiant į jų pobūdį, gali kelti pavojų duomenų subjektams, todėl jiems reikalinga griežtesnė apsauga. Tokiems duomenims taikomas draudimo principas ir yra nedaug sąlygų, kuriomis toks duomenų tvarkymas yra teisėtas.

Atsižvelgiant į atnaujintos 108-osios konvencijos (6 straipsnis) ir BDAR (9 straipsnis) sistemą, neskelbtinais duomenimis laikomi šių kategorijų duomenys:

- asmens duomenys, kuriais atskleidžiama rasinė arba etninė kilmė;
- asmens duomenys, kuriais atskleidžiamos politinės pažiūros, religiniai arba kitokie įsitikinimai, įskaitant filosofinius įsitikinimus;
- asmens duomenys, kuriais atskleidžiama narystė profesinėje sąjungoje;
- genetiniai ir biometriniai duomenys, kurie tvarkomi siekiant nustatyti asmens tapatybę;
- asmens duomenys, susiję su sveikata, seksualiniu gyvenimu arba lytine orientacija.

Pavyzdys. Byla *Bodil Lindqvist*[186] buvo susijusi su nuorodomis į įvairius asmenis interneto puslapyje pateikiant jų vardą ar pavardę arba kitomis priemonėmis, pavyzdžiui, jų telefono numeriu ar informacija apie jų pomėgius. ESTT konstatavo, kad „paminėjimas, kad asmuo susižeidė koją ir yra dalinėse laikinojo nedarbingumo atostogose, yra asmens duomenys apie sveikatą“[187].

186 ESTT, C-101/01, *Baudžiamoji byla prieš Bodil Lindqvist*, 2003 m. lapkričio 6 d., 51 punktas.

187 Ankstesnės Direktyvos 95/46/EB 8 straipsnio 1 dalis, dabartinė Bendrojo duomenų apsaugos reglamento 9 straipsnio 1 dalis.

Asmens duomenys, susiję su apkaltinamaisiais nuosprendžiais ir nusikalstamomis veikomis

Atnaujinta 108-oji konvencija apima asmens duomenis, susijusius su nusikalstamomis veikomis, baudžiamosiomis bylomis ir apkaltinamaisiais nuosprendžiais, ir yra susijusi su saugumo priemonėmis, kurios pateikiamos specialių kategorijų asmens duomenų sąraše[188]. Pagal BDAR sistemą su apkaltinamaisiais nuosprendžiais ir nusikalstamomis veikomis arba atitinkamomis saugumo priemonėmis susiję asmens duomenys iš esmės nėra minimi specialių kategorijų duomenų sąraše, tačiau jie aptariami atskirame straipsnyje. BDAR 10 straipsnyje nustatyta, kad tokie duomenys gali būti tvarkomi tik „prižiūrint valdžios institucijai arba kai duomenų tvarkymas leidžiamas Sąjungos arba valstybės narės teise, kurioje nustatytos tinkamos duomenų subjektų teisių ir laisvių apsaugos priemonės“. Kita vertus, išsamūs registrai, kuriuose kaupiama informacija apie apkaltinamuosius nuosprendžius, gali būti tvarkomi tik kontroliuojant konkrečioms valdžios institucijoms[189]. ES asmens duomenų tvarkymas teisėsaugos srityje reglamentuojamas konkrečiame teisės akte, t. y. Direktyvoje (ES) 2016/680[190]. Direktyvoje nustatytos konkrečios duomenų apsaugos taisyklės, kurių kompetentingos institucijos privalo laikytis tvarkydamos asmens duomenis, visų pirma siekdamos nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas (žr. 8.2.1 skirsnį).

2.2. Duomenų tvarkymas

Pagrindiniai faktai

- „Duomenų tvarkymas“ yra susijęs bet kokia asmens duomenų tvarkymo operacija.
- Sąvoka „tvarkymas“ apima automatizuotą ir neautomatizuotą tvarkymą.
- Pagal ES teisę „tvarkymas“ taip pat reiškia tvarkymą rankiniu būdu struktūrizuotose bylų sistemose.
- Pagal ET teisę „tvarkymas“ pagal nacionalinę teisę gali apimti ir rankinį tvarkymą.

188 Atnaujintos 108-osios konvencijos 6 straipsnio 1 dalis.

189 Bendrojo duomenų apsaugos reglamento 10 straipsnis.

190 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, ir kuria panaikinamas Tarybos pamatinis sprendimas 2008/977/JHA, OL L 119, 2016.

2.2.1. Duomenų tvarkymo koncepcija

Asmens duomenų tvarkymo koncepcija išsamiai apibūdinta **tiek ES, tiek ir ET teisėje**: asmens „duomenų tvarkymas – bet kokia <...> operacija <...>, kaip antai [asmens duomenų] rinkimas, įrašymas, rūšiavimas, sisteminimas, saugojimas, adaptavimas ar keitimas, išgava, susipažinimas, naudojimas, atskleidimas persiunčiant, platinant ar kitu būdu sudarant galimybę jais naudotis, taip pat sugretinimas ar sujungimas su kitais duomenimis, apribojimas, ištrynimas arba sunaikinimas“[191]. Atnaujintoje 108-ojoje konvencijoje prie šios apibrėžties pridedamas asmens duomenų išsaugojimas[192].

Pavyzdys. Byloje *František Ryneš*[193] F. Ryneš vidaus AVSS stebėjimo sistemoje, kurią buvo sumontavęs, kad apsaugotų savo turtą, užfiksavo dviejų asmenų, kurie išdaužė jo namų langus, atvaizdus. ESTT nustatė, kad stebėjimas vaizdo kameromis, kai įrašomi ir saugomi asmens duomenys, yra automatinis duomenų tvarkymas, kuriam taikoma ES duomenų apsaugos teisė.

Pavyzdys. Byloje *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce prieš Salvatore Manni*[194] S. Manni prašė pašalinti jo asmens duomenis iš reitingavimo įmonės registro, kuriame jis buvo susietas su nekilnojamojo turto įmonės likvidavimu, nes tai turėjo neigiamos įtakos jo reputacijai. ESTT nusprendė, kad „įtraukdama minėtą informaciją į registrą, saugodama ją ir prireikus trečiųjų asmenų prašymu pateikdama jiems šią informaciją registrą tvarkanti institucija atlieka „asmens duomenų tvarkymą“ ir yra šių duomenų „valdytoja“.

Pavyzdys. Darbdaviai renka ir tvarko savo darbuotojų duomenis, įskaitant informaciją apie darbo užmokestį. Darbo sutartys yra teisinis pagrindas teisėtai tai daryti.

191 Bendrojo duomenų apsaugos reglamento 4 straipsnio 2 punktas. Taip pat žr. atnaujintos 108-osios konvencijos 2 straipsnio b punktą.

192 Atnaujintos 108-osios konvencijos 2 straipsnio b punktas.

193 ESTT, C-212/13, *František Ryneš prieš Úřad pro ochranu osobních údajů*, 2014 m. gruodžio 11 d., 25 punktas.

194 ESTT, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce prieš Salvatore Manni*, 2017 m. kovo 9 d., 35 punktas.

Darbdaviai duomenis apie savo darbuotojų darbo užmokestį turi pateikti mokesčių institucijoms. Šis duomenų perdavimas taip pat bus „duomenų tvarkymas“, kaip ši sąvoka suprantama atnaujintoje 108-ojoje konvencijoje ir BDAR. Tačiau tokio atskleidimo teisinis pagrindas nėra darbo sutartys. Turi būti nustatytas papildomas duomenų tvarkymo operacijų, po kurių darbdavys perduoda darbo užmokesčio duomenis mokesčių institucijoms, teisinis pagrindas. Šį teisinį pagrindą paprastai galima rasti nacionalinių mokesčių įstatymų nuostatose. Jei tokių nuostatų nebūtų ir jeigu nebūtų jokio kito teisėto duomenų tvarkymo pagrindo, šis asmens duomenų perdavimas būtų laikomas neteisėtu duomenų tvarkymu.

2.2.2. Automatizuotas duomenų tvarkymas

Duomenų apsauga pagal atnaujintą 108-ąją konvenciją ir BDAR visapusiškai taikoma automatizuotam duomenų tvarkymui.

Pagal **ES teisę** automatizuotas asmens duomenų tvarkymas apima „visiškai arba iš dalies automatizuotomis priemonėmis“ atliekamas operacijas[195]. Atnaujintoje 108-ojoje konvencijoje pateikiama panaši apibrėžtis[196]. Praktiškai tai reiškia, kad bet kokiam asmens duomenų tvarkymui naudojant automatizuotas priemones pasitelkiant, pavyzdžiui, asmeninį kompiuterį, nešiojamąjį prietaisą arba maršruto parinktuvą, taikomos ES ir ET duomenų apsaugos taisyklės.

Pavyzdys. Byla *Bodil Lindqvist*[197] buvo susijusi su nuorodomis į įvairius asmenis interneto puslapyje pateikiant jų vardą ar pavardę arba kitus duomenis, pavyzdžiui, jų telefono numerį ar informaciją apie pomėgius. ESTT nusprendė, kad „veiksmai, kuriais interneto puslapyje paminimi įvairūs asmenys, kurių tapatybė atskleidžiama arba nurodant pavardę, arba kitus duomenis, pavyzdžiui, telefono numerį ar su darbo sąlygomis ir pomėgiais susijusią informaciją, yra atlikti „visiškai ar iš dalies automatiniais būdais tvarkant asmens duomenis“, kaip tai suprantama pagal Direktyvos 95/46/EB 3 straipsnio 1 dalį[198].

195 Bendrojo duomenų apsaugos reglamento 2 straipsnio 1 dalis ir 4 straipsnio 2 punktas.

196 Atnaujintos 108-osios konvencijos 2 straipsnio b ir c punktai; atnaujintos 108-osios konvencijos aiškinamosios ataskaitos 21 punktas.

197 ESTT, C-101/01, *Criminal proceedings against Bodil Lindqvist*, 2003 m. lapkričio 6 d., 27 punktas.

198 Bendrojo duomenų apsaugos reglamento 2 straipsnio 1 punktas.

Pavyzdys. Byloje *Google Spain SL, Google Inc. prieš Agencia Española de Protección de Datos (AEPD), Mario Costeja González*[199] M. C. González prašė pašalinti arba pakeisti *Google* paieškos sistemoje ryšį tarp jo vardo ir pavardės ir dviejų laikraščio puslapių, kuriuose skelbiamas nekilnojamojo turto aukcionas socialinio draudimo skoloms išieškoti. ESTT pareiškė, kad „automatiškai, nuolat ir sistemiškai naršydamas po internetą, kad surastų per jį paskelbtą informaciją, paieškos variklio eksploatuotojas „renka" tokius duomenis, kuriuos „atgamina [paima]", „užrašo" ir po to panaudodamas indeksavimo programas „surūšiuoja", „išsaugo" savo serveriuose ir prireikus „atskleidžia" arba „padaro prieinamus" savo naudotojams jų paieškos rezultatų sąrašų pavidalu"[200]. ESTT padarė išvadą, kad tokie veiksmai reiškė „duomenų tvarkymą", „nesvarbu, kad tas pačias operacijas paieškos variklio eksploatuotojas taip pat taiko kitų rūšių informacijai ir neskiria šios kitų rūšių informacijos nuo asmens duomenų".

2.2.3. Neautomatizuotas duomenų tvarkymas

Duomenų apsaugą taip pat reikia užtikrinti tvarkant duomenis rankiniu būdu.

Pagal ES teisę užtikrinama duomenų apsauga jokiais būdais nėra taikoma tik automatizuotam duomenų tvarkymui. Atitinkamai pagal ES teisę duomenų apsauga galioja asmens duomenų tvarkymui rankinėje bylų sistemoje, t. y. specialiai susistemintoje popierinėje byloje[201]. Susisteminta bylų sistema yra tokia sistema, kurioje į kategorijas skirstomi asmens duomenų rinkiniai, su kuriais galima susipažinti remiantis tam tikrais kriterijais. Pavyzdžiui, jeigu darbdavys tvarko popierinę bylą pavadinimu „darbuotojų atostogos", kurioje abėcėline tvarka pateikiami visi duomenys apie atostogas, kurias praėjusiais metais buvo paėmę darbuotojai, byla bus laikoma rankine bylų sistema, kuriai taikomos ES duomenų apsaugos taisyklės. Šiuo atveju duomenų apsauga praplečiama dėl to, kad:

- popierinės bylos gali būti susistemintos taip, kad informaciją būtų galima rasti greitai ir lengvai;

199 ESTT, C-131/12, *Google Spain SL, Google Inc. prieš Agencia Española de Protección de Datos (AEPD), Mario Costeja González* (DK), 2014 m. gegužės 13 d.

200 *Ten pat*, 28 punktas.

201 Bendrojo duomenų apsaugos reglamento 2 straipsnio 1 punktas.

- asmens duomenis saugant susistemintose popierinės bylose galima lengvai apeiti įstatyme nustatytus apribojimus, kurie taikomi automatizuotam duomenų tvarkymui[202].

ET teisėje pateiktoje automatizuoto duomenų tvarkymo apibrėžtyje pripažįstama, kad tarp automatizuotų operacijų gali būti reikalingi tam tikri rankinio asmens duomenų tvarkymo etapai[203]. Atnaujintos 108-osios konvencijos 2 straipsnio c punkte nustatyta, kad „jeigu automatizuotas tvarkymas nenaudojamas, duomenų tvarkymas – tai operacija ar operacijos, atliekamos su asmens duomenimis pagal struktūrizuotą tokių duomenų rinkinį, kuris yra prieinamas arba kurį galima gauti pagal konkrečius kriterijus“.

2.3. Asmens duomenų naudotojai

Pagrindiniai faktai

- Asmuo, kuris nustato kitų asmenų asmens duomenų tvarkymo priemones ir tikslus, yra „duomenų valdytojas“ pagal duomenų apsaugos teisę; jeigu šį sprendimą kartu priima keletas asmenų, jie gali būti „bendrais duomenų valdytojais“.
- „Duomenų valdytojas“ – tai fizinis arba juridinis asmuo, kuris duomenų valdytojo vardu tvarko asmens duomenis.
- Jeigu duomenų tvarkytojas pats nustato duomenų tvarkymo priemones ir tikslus, jis tampa duomenų valdytoju.
- „Gavėjas“ – tai bet kuris asmuo, kuriam atskleidžiami duomenys.
- „Trečioji šalis“ – tai fizinis arba juridinis asmuo, kuris nėra duomenų subjektas, duomenų valdytojas, duomenų tvarkytojas, ir asmenys, kuriems leidžiama tvarkyti asmens duomenis remiantis tiesioginiu duomenų valdytojo arba duomenų tvarkytojo įgaliojimu.
- Sutikimas, kaip asmens duomenų tvarkymo pagrindas, turi būti duotas laisva valia, pagrįstas informacija, konkretus ir vienareikšmiškai išreikštas aiškiu patvirtinamuoju veiksmu, kuriuo pritariama duomenų tvarkymui.
- Specialių kategorijų duomenims tvarkyti sutikimo pagrindu reikalingas aiškus sutikimas.

202 Bendrojo duomenų apsaugos reglamento 15 konstatuojamoji dalis.

203 Atnaujintos 108-osios konvencijos 2 straipsnio b ir c punktai.

2.3.1. Duomenų valdytojai ir duomenų tvarkytojai

Svarbiausia pasekmė, kuri atsiranda duomenų valdytojui arba duomenų tvarkytojui, yra teisinė pareiga laikytis atitinkamų prievolių pagal duomenų apsaugos teisę. Privačiajame sektoriuje tai paprastai yra fizinis arba juridinis asmuo; viešajame sektoriuje tai paprastai yra institucija. Tarp duomenų valdytojo ir duomenų tvarkytojo yra esminis skirtumas: duomenų valdytojas – tai fizinis arba juridinis asmuo, kuris nustato duomenų tvarkymo tikslus ir priemones, o duomenų tvarkytojas – tai fizinis arba juridinis asmuo, kuris duomenis tvarko duomenų valdytojo vardu ir vadovaudamasis griežtais nurodymais. Iš esmės būtent duomenų valdytojas privalo vykdyti duomenų tvarkymo kontrolę ir jis atsako už šią kontrolę, įskaitant teisinę atsakomybę. Tačiau įgyvendinus duomenų apsaugos taisyklių reformą, dabar duomenų tvarkytojai privalo laikytis daugybės reikalavimų, kurie taikomi ir duomenų valdytojams. Pavyzdžiui, pagal BDAR duomenų tvarkytojai privalo registruoti visų kategorijų duomenų tvarkymo veiklą, kad įrodytų, jog laikosi reglamente nustatytų prievolių[204]. Taip pat reikalaujama, kad duomenų tvarkytojai įgyvendintų tinkamas technines ir organizacines priemones ir taip užtikrintų saugų duomenų tvarkymą[205], tam tikrose situacijose paskirtų duomenų apsaugos pareigūną[206] ir praneštų duomenų valdytojui apie duomenų saugumo pažeidimus[207].

Tai, ar asmuo gali nuspręsti ir nustatyti duomenų tvarkymo tikslą ir priemones, priklauso nuo faktinių bylos aspektų ar aplinkybių. Remiantis BDAR pateikta duomenų valdytojo apibrėžtimi, duomenų valdytojais gali būti fiziniai asmenys, juridiniai asmenys ar bet kurios kitos įstaigos. Tačiau 29 straipsnio darbo grupė pažymėjo, kad, siekiant asmenims suteikti stabilesnį subjektą, kad jie galėtų naudotis savo teisėmis, „duomenų valdytoju visų pirma reikėtų laikyti bendrovę arba subjektą, o ne konkretų toje bendrovėje arba subjekte dirbantį asmenį“[208]. Pavyzdžiui, bendrovė, kuri specialistams parduoda sveikatos priežiūros priemones, yra duomenų valdytoja, kuri sudaro ir tvarko visų specialistų platinimo tam tikroje vietovėje sąrašą, o ne komercijos direktorius, kuris faktiškai naudoja ir tvarko sąrašą.

204 Bendrojo duomenų apsaugos reglamento 30 straipsnio 2 dalis.

205 *Ten pat*, 32 straipsnis.

206 *Ten pat*, 37 straipsnis.

207 *Ten pat*, 33 straipsnio 2 punktas.

208 29 straipsnio darbo grupė (2010 m.), *Nuomonė Nr. 1/2010 dėl sąvokų „duomenų valdytojas“ ir „duomenų tvarkytojas“*, WP 169, Briuselis, 2010 m. vasario 16 d.

Pavyzdys. Kai įmonės *Sunshine* rinkodaros padalinys planuoja tvarkyti duomenis rinkos tyrimui, už tokį duomenų tvarkymą atsakingu duomenų valdytoju bus laikoma ši bendrovė, o ne rinkodaros skyriaus darbuotojai. Rinkodaros skyrius negali būti duomenų valdytojas, nes jis neturi atskiro subjektiškumo.

Pagal ES ir ET teisę fiziniai asmenys gali būti duomenų valdytojai. Tačiau tais atvejais, kai tvarkomi kitų asmenų duomenys, susiję tik su asmenine ar namų ūkio veikla, privatūs asmenys nepatenka į BDAR ir atnaujintos 108-osios konvencijos taikymo sritį ir jie nelaikomi duomenų valdytojais[209]. Asmeniui, kuris laiko savo susirašinėjimą, asmeninį dienoraštį, kuriame aprašomi įvykiai, susiję su jo draugais ir kolegomis, ir šeimos narių įrašus apie sveikatą, gali būti netaikomos duomenų apsaugos taisyklės, nes ši veikla gali būti išimtinai asmeninė arba namų ūkio veikla. BDAR taip pat nustatyta, kad asmeninė arba namų ūkio veikla taip pat galėtų apimti veiklą socialiniuose tinkluose ir internetinę veiklą, jeigu ji vykdoma tokios veiklos kontekste[210]. Priešingai, duomenų apsaugos taisyklės taikomos visa apimtimi duomenų valdytojams ir duomenų tvarkytojams, kurie suteikia priemones tvarkyti asmens duomenis vykdant asmeninę arba namų ūkio veiklą (pavyzdžiui, socialinių tinklų platformos)[211].

Dėl piliečių prieigos prie interneto ir galimybės naudotis e. prekybos platformomis, socialiniais tinklais ir tinklaraščio svetainėmis siekiant dalytis savo asmenine informacija ir informacija apie kitus asmenis tampa vis sunkiau atskirti asmeninį duomenų tvarkymą nuo neasmeninio duomenų tvarkymo[212]. Tai, ar veikla yra išimtinai asmeninio arba namų ūkio pobūdžio, priklauso nuo aplinkybių[213]. Veikla, kuri turi profesinių arba komercinių aspektų, negali patekti į namų ūkio išimties taikymo sritį[214]. Todėl jeigu iš duomenų tvarkymo masto ir dažnumo galima daryti išvadą, kad tai yra profesionali veikla arba visą darbo dieną vykdoma veikla, privatus asmuo galėtų būti laikomas duomenų valdytoju. Be profesionalaus ar komercinio duomenų tvarkymo

209 Bendrojo duomenų apsaugos reglamento 18 konstatuojamoji dalis ir 2 straipsnio 2 dalies c punktas; atnaujintos 108-osios konvencijos 3 straipsnio 2 dalis.

210 Bendrojo duomenų apsaugos reglamento 18 konstatuojamoji dalis.

211 *Ten pat*, 18 konstatuojamoji dalis; atnaujintos 108-osios konvencijos aiškinamosios ataskaitos 29 punktas.

212 Žr. 29 straipsnio darbo grupės pareiškimą diskusijose dėl duomenų apsaugos reformos paketo (2013 m.), *2 priedas. Pasiūlymai ir pakeitimai dėl asmeninei ir namų ūkio veiklai taikomos išimties*, 2013 m. vasario 27 d.

213 Atnaujintos 108-osios konvencijos aiškinamosios ataskaitos 28 punktas.

214 Žr. Bendrojo duomenų apsaugos reglamento 18 konstatuojamąją dalį ir atnaujintos 108-osios konvencijos aiškinamosios ataskaitos 27 punktą.

pobūdžio, kitas veiksnys, į kurį būtina atsižvelgti, yra tai, ar su asmens duomenimis gali susipažinti didelis skaičius asmenų, kurie akivaizdžiai nepatenka į asmens privatumo sferą. Su Duomenų apsaugos direktyva susijusioje teismų praktikoje nustatyta, kad duomenų apsaugos teisė bus taikoma tais atvejais, kai privatus asmuo, naudodamasis internetu, viešoje svetainėje skelbia duomenis apie kitus asmenis. ESTT dar nepriėmė sprendimo dėl panašių faktinių aplinkybių pagal BDAR, kuriame būtų pateikta daugiau gairių klausimais, kurie galėtų būti laikomi nepatenkančiais į duomenų apsaugos teisės aktuose nustatytą „namų ūkio išimtį", pavyzdžiui, socialinių tinklų naudojimas asmeniniais tikslais.

Pavyzdys. Byla *Bodil Lindqvist*[215] buvo susijusi su nuorodomis į įvairius asmenis interneto puslapyje pateikiant jų vardą ar pavardę arba kitomis priemonėmis, pavyzdžiui, jų telefono numeriu ar informacija apie jų pomėgius. ESTT pritarė, kad „veiksmai, kuriais interneto puslapyje paminimi įvairūs asmenys, kurių tapatybė atskleidžiama arba nurodant pavardę, arba kitus duomenis <...>, yra atlikti „visiškai ar iš dalies automatiniais būdais tvarkant asmens duomenis", kaip tai suprantama pagal Duomenų apsaugos direktyvos 3 straipsnio 1 dalį[216].

Toks asmens duomenų tvarkymas nepatenka į išimtinai asmeninės ar vidaus veiklos, kuriai negalioja ES duomenų apsaugos taisyklės, taikymo sritį, nes šią išimtį „<...> reikia aiškinti kaip numatančią tik tokią veiklą, kuria privatūs asmenys užsiima neperžengdami privataus ar šeimos gyvenimo ribų, o taip akivaizdžiai nėra tvarkant asmens duomenis, kai jie paskelbiami internete ir tampa prieinami neapibrėžtam asmenų skaičiui"[217].

Pasak ESTT, privačiai įrengtų saugumo kamerų vaizdo įrašams tam tikromis aplinkybėmis taip pat gali būti taikomi ES duomenų apsaugos teisės aktai.

215 ESTT, C-101/01, *Baudžiamoji byla prieš Bodil Lindqvist*, 2003 m. lapkričio 6 d.

216 *Ten pat*, 27 punktas; ankstesnės Direktyvos 95/46/EB 3 straipsnio 1 dalis, dabartinė Bendrojo duomenų apsaugos reglamento 2 straipsnio 1 dalis.

217 ESTT, C-101/01, *Baudžiamoji byla prieš Bodil Lindqvist*, 2003 m. lapkričio 6 d., 47 punktas.

Pavyzdys. Byloje *František Ryneš*[218] F. Ryneš vidaus AVSS stebėjimo sistemoje, kurią buvo sumontavęs, kad apsaugotų savo turtą, užfiksavo dviejų asmenų, kurie išdaužė jo namų langus, atvaizdus. Tada įrašas buvo perduotas policijai ir juo buvo remiamasi nagrinėjant baudžiamąją bylą.

ESTT konstatavo, kad „<...> vaizdo stebėjimas apima, net jei tik iš dalies, viešąją erdvę ir todėl yra nukreiptas į tokiu būdu duomenis tvarkančio asmens privačios sferos išorę, jis negali būti laikomas išimtinai „asmenine ar namų ūkio veikla“[219].

Duomenų valdytojas

Pagal ES teisę duomenų valdytojas apibrėžiamas kaip subjektas, kuris „vienas ar drauge su kitais nustato duomenų tvarkymo tikslus ir priemones“[220]. Duomenų valdytojo sprendime nustatomos duomenų tvarkymo priežastys ir būdai.

Pagal ET teisę atnaujintoje 108-ojoje konvencijoje duomenų valdytojas apibrėžiamas kaip „fizinis ar juridinis asmuo, valdžios institucija, tarnyba, agentūra ar bet kuris kitas organas, kuris vienas ar kartu su kitais asmenimis turi įgaliojimus priimti sprendimus dėl duomenų tvarkymo“[221]. Tokie įgaliojimai priimti sprendimus yra susiję su duomenų tvarkymo tikslais ir priemonėmis, taip pat tvarkytinų duomenų kategorijomis ir galimybe susipažinti su duomenimis[222]. Tai, ar šie įgaliojimai atsiranda dėl teisinio įgaliojimo, ar dėl faktinių aplinkybių, turi būti sprendžiama kiekvienu konkrečiu atveju[223].

Pavyzdys. Bylą *Google Spain*[224] iškėlė Ispanijos pilietis, kuris norėjo, kad senas laikraščio straipsnis apie jo finansinę istoriją būtų pašalintas iš *Google*.

218 ESTT, C-212/13, *František Ryneš prieš Úřad pro ochranu osobních údajů*, 2014 m. gruodžio 11 d., 33 punktas.

219 Ankstesnės Direktyvos 95/46/EB 3 straipsnio 2 dalies antra įtrauka, dabartinis Bendrojo duomenų apsaugos reglamento 2 straipsnio 2 dalies c punktas.

220 Bendrojo duomenų apsaugos reglamento 4 straipsnio 7 punktas.

221 Atnaujintos 108-osios konvencijos 2 straipsnio d punktas.

222 Atnaujintos 108-osios konvencijos aiškinamosios ataskaitos 22 punktas.

223 *Ten pat*.

224 ESTT, C-131/12, *Google Spain SL, Google Inc. prieš Agencia Española de Protección de Datos (AEPD), Mario Costeja González* (DK), 2014 m. gegužės 13 d.

ESTT buvo klausiama, ar *Google*, kaip paieškos sistemos eksploatuotojas, buvo duomenų „valdytojas“, kaip tai suprantama pagal Duomenų apsaugos direktyvos 2 straipsnio d punktą[225]. ESTT nagrinėjo plačią apibrėžtį „duomenų valdytojas“, kad būtų užtikrinta „veiksminga ir visapusiška duomenų subjektų apsauga“[226]. ESTT nustatė, kad paieškos sistemos eksploatuotojas nustatė veiklos tikslus ir priemones ir kad jis padarė į interneto puslapius svetainių leidėjų atsiųstus duomenis prieinamus bet kuriam interneto naudotojui, kuris atlieka paiešką naudodamas duomenų subjekto vardą ir pavardę[227]. Todėl ESTT nustatė, kad *Google* galėjo būti laikomas „duomenų valdytoju“[228].

Jeigu duomenų valdytojas arba duomenų tvarkytojas yra įsisteigęs už ES ribų, ta įmonė turi raštu paskirti atstovą ES[229]. BDAR pažymima, kad atstovas turi būti įsisteigęs „vienoje iš tų valstybių narių, kuriose yra duomenų subjektai ir kurių asmens duomenys yra tvarkomi prekių ar paslaugų siūlymo jiems tikslais arba kurių elgesys yra stebimas“[230]. Jeigu atstovas nepaskiriamas, pačiam duomenų valdytojui ar duomenų tvarkytojui vis tiek galima pareikšti ieškinį[231].

Bendras duomenų valdymas

BDAR nustatyta, kad jeigu du ar daugiau duomenų valdytojų kartu nustato duomenų tvarkymo tikslą ir priemones, jie laikomi bendrais duomenų valdytojais. Tai reiškia, kad jie drauge nusprendžia tvarkyti duomenis bendram tikslui[232]. Atnaujintos 108-osios konvencijos aiškinamojoje ataskaitoje nustatyta, kad pagal **ET sistemą** taip pat gali būti keletas duomenų valdytojų arba bendri duomenų valdytojai[233].

225 Bendrojo duomenų apsaugos reglamento 4 straipsnio 7 punktas; ESTT, C-131/12, *Google Spain SL, Google Inc. prieš Agencia Española de Protección de Datos (AEPD), Mario Costeja González* (DK), 2014 m. gegužės 13 d., 21 punktas.

226 ESTT, C-131/12, *Google Spain SL, Google Inc. prieš Agencia Española de Protección de Datos (AEPD), Mario Costeja González* (DK), 2014 m. gegužės 13 d., 34 punktas.

227 *Ten pat*, 35–40 punktai.

228 *Ten pat*, 41 punktas.

229 Bendrojo duomenų apsaugos reglamento 27 straipsnio 1 punktas.

230 *Ten pat*, 27 straipsnio 3 punktas.

231 *Ten pat*, 27 straipsnio 5 punktas.

232 *Ten pat*, 4 straipsnio 7 punktas ir 26 straipsnis.

233 Atnaujintos 108-osios konvencijos 2 straipsnio d punktas; atnaujintos 108-osios konvencijos aiškinamosios ataskaitos 22 punktas.

29 straipsnio darbo grupė atkreipia dėmesį į tai, kad bendras duomenų valdymas gali būti vykdomas įvairiomis formomis ir kad skirtingų duomenų valdytojų dalyvavimas vykdant valdymo veiklą gali būti nevienodas[234]. Dėl tokio lankstaus požiūrio gali būti prisitaikoma prie vis sudėtingesnių duomenų tvarkymo realijų[235]. Todėl bendri duomenų valdytojai konkrečioje sutartyje privalo nustatyti savo atitinkamą atsakomybę už prievolių pagal reglamentą laikymąsi[236].

Bendrai valdant duomenis atsiranda bendra atsakomybė už duomenų tvarkymo veiklą[237]. Pagal **ES teisę** tai reiškia, kad kiekvienas duomenų valdytojas arba duomenų tvarkytojas gali būti laikomas visiškai atsakingu už visą bendrai valdant duomenis padarytą žalą, taip užtikrinant, kad duomenų subjektui būtų veiksmingai sumokėta kompensacija[238].

Pavyzdys. Kelių kredito įstaigų bendrai valdoma duomenų bazė, kurioje pateikiami duomenys apie įsipareigojimų nevykdančius klientus, yra įprastas bendro duomenų valdymo pavyzdys. Kai kuris nors asmuo kreipiasi į banką, priklausantį bendrų duomenų valdytojų grupei, ir prašo suteikti kreditą, toks bankas patikrina duomenų bazėje esančią informaciją ir priima pagrįstą sprendimą dėl pareiškėjo kreditingumo.

Teisinėse nuostatose aiškiai nenustatyta, ar bendram duomenų valdymui reikia bendro tikslo, kuris būtų vienodas kiekvienam iš duomenų valdytojų, ar pakanka, jeigu tikslai sutampa tik iš dalies. Dabar Europos lygmeniu nėra prieinamos atitinkamos teismų praktikos. Savo 2010 m. nuomonėje dėl duomenų valdytojų ir duomenų tvarkytojų 29 straipsnio darbo grupė nurodo, kad bendri duomenų valdytojai gali turėti bendrus visus duomenų tvarkymo tikslus arba tik kai kurie tikslai arba priemonės, arba jų dalis gali būti bendri[239]. Pirmuoju atveju skirtingų subjektų santykiai būtų labai glaudūs, o antruoju – santykiai būtų ne tokie tvirti.

234 29 straipsnio darbo grupė (2010 m.), *Nuomonė Nr. 1/2010 dėl sąvokų „duomenų valdytojas“ ir „duomenų tvarkytojas“*, WP 169, Briuselis, 2010 m. vasario 16 d., p. 19.

235 *Ten pat*.

236 Bendrojo duomenų apsaugos reglamento 79 konstatuojamoji dalis.

237 *Ten pat*, 21 punktas.

238 *Ten pat*, 82 straipsnio 4 punktas.

239 29 straipsnio darbo grupė (2010 m.), *Nuomonė Nr. 1/2010 dėl sąvokų „duomenų valdytojas“ ir „duomenų tvarkytojas“*, WP 169, Briuselis, 2010 m. vasario 16 d., p. 19.

29 straipsnio darbo grupė pritaria platesniam koncepcijos „bendras duomenų valdymas“ aiškinimui siekiant sudaryti sąlygas lankstesniam požiūriui, kuris apimtų vis sudėtingesnę dabartinę duomenų tvarkymo tikrovę[240]. Byla, kurioje dalyvavo Pasaulinė tarpbankinių finansinių telekomunikacijų organizacija (SWIFT), patvirtina darbo grupės poziciją.

Pavyzdys. Vadinamojoje SWIFT byloje Europos bankų institucijos, iš pradžių kaip duomenų tvarkytojos, naudojo SWIFT, kad galėtų perduoti duomenis vykdydamos bankų sandorius. SWIFT atskleidė tokius bankų sandorių duomenis, kurie buvo saugomi Jungtinėse Amerikos Valstijose (JAV) esančiame kompiuteriniame serveryje, JAV iždo departamentui, nors SWIFT besinaudojantys Europos bankai nedavė aiškaus nurodymo organizacijai atskleisti tokius duomenis. 29 straipsnio darbo grupė, vertindama šios padėties teisėtumą, padarė išvadą, kad SWIFT naudojančios Europos bankininkystės institucijos ir pati SWIFT turi būti laikomos bendrais duomenų valdytojais, kurie atsako Europos klientams už jų duomenų atskleidimą JAV valdžios institucijoms[241].

Duomenų tvarkytojas

ES teisėje duomenų tvarkytojas apibrėžiamas kaip subjektas, kuris asmens duomenis tvarko duomenų valdytojo vardu[242]. Duomenų tvarkytojui patikėta veikla gali būti susijusi su konkrečia užduotimi ar aplinkybėmis arba gali būti gana bendro ir plataus pobūdžio.

Pagal ET teisę sąvoka „duomenų tvarkytojas“ suprantama taip pat, kaip ir pagal ES teisę[243].

Duomenų tvarkytojai ne tik tvarko duomenis kitiems, bet ir patys yra duomenų valdytojai, kiek tai susiję su jų pačių atliekamu duomenų tvarkymu, pavyzdžiui, savo darbuotojų administravimu, pardavimu ir apskaita.

240 *Ten pat*.

241 29 straipsnio darbo grupė (2006 m.), *Nuomonė Nr. 10/2006 dėl Pasaulinės tarpbankinių finansinių telekomunikacijų organizacijos (SWIFT) atliekamo asmens duomenų tvarkymo*, WP 128, Briuselis, 2006 m. lapkričio 22 d.

242 Bendrojo duomenų apsaugos reglamento 4 straipsnio 8 punktas.

243 Atnaujintos 108-osios konvencijos 2 straipsnio f punktas.

Pavyzdys. Įmonė *Everready* specializuojasi duomenų tvarkymo administruojant kitų įmonių žmogiškuosius išteklius srityje. Vykdydama šią funkciją, įmonė *Everready* yra duomenų tvarkytoja. Tačiau jeigu įmonė *Everready* tvarko savo pačios darbuotojų duomenis, tai yra duomenų valdytojo vykdomos duomenų tvarkymo operacijos, kuriomis siekiama įvykdyti darbdavio pareigas.

Duomenų tvarkytojo ir duomenų valdytojo santykiai

Kaip matėme, duomenų valdytojas apibrėžiamas kaip subjektas, kuris nustato duomenų tvarkymo tikslus ir priemones. BDAR aiškiai nustatyta, kad duomenų tvarkytojas asmens duomenis gali tvarkyti tik vadovaudamasis duomenų valdytojo nurodymais, išskyrus atvejus, kai pagal ES arba valstybės narės teisę reikalaujama, kad tai darytų duomenų tvarkytojas[244]. Duomenų valdytojo ir duomenų tvarkytojo sutartis yra esminis jų tarpusavio santykių aspektas, be to, tai yra teisinis reikalavimas[245].

Pavyzdys. Įmonės *Sunshine* direktorius nusprendžia, kad įmonė *Cloudy* – debesijos duomenų saugojimo specialistė – turėtų tvarkyti įmonės *Sunshine* klientų duomenis. Įmonė *Sunshine* išlieka duomenų valdytoja, o įmonė *Cloudy* yra tik duomenų tvarkytoja, nes pagal sutartį įmonė *Cloudy* gali naudoti įmonės *Sunshine* klientų duomenis tik įmonės *Sunshine* nustatytais tikslais.

Jei duomenų tvarkytojui suteikiami įgaliojimai nustatyti duomenų tvarkymo būdus, duomenų valdytojas vis dėlto turi turėti galimybę tinkamai kontroliuoti duomenų tvarkytojo sprendimus dėl duomenų tvarkymo būdų. Bendra atsakomybė vis tiek priklauso duomenų valdytojui, kuris privalo prižiūrėti duomenų tvarkytojus ir užtikrinti, kad jų sprendimai atitiktų duomenų apsaugos teisę ir jų pačių nurodymus.

Be to, jeigu duomenų tvarkytojas nesilaikytų duomenų valdytojo nustatytų duomenų tvarkymo sąlygų, jis taptų duomenų valdytoju bent tais atvejais, kai pažeidžia duomenų valdytojo nurodymus. Tokiomis aplinkybėmis duomenų tvarkytojas greičiausiai bus laikomas duomenų valdytoju, kuris veikia neteisėtai. Todėl pradinis duomenų valdytojas turės paaiškinti, kaip duomenų tvarkytojas galėjo pažeisti jam

244 Bendrojo duomenų apsaugos reglamento 29 straipsnis.

245 *Ten pat*, 28 straipsnio 3 punktas.

suteiktus įgaliojimus[246]. Iš tiesų 29 straipsnio darbo grupė tokiais atvejais linkusi daryti prielaidą dėl bendro duomenų valdymo, nes taip geriausiai apsaugomi duomenų subjektų interesai[247].

Klausimų dėl atsakomybės padalijimo gali kilti ir tais atvejais, kai duomenų valdytojas yra maža įmonė, o duomenų tvarkytojas yra didelė kolektyvinė bendrovė, kuri gali diktuoti paslaugų teikimo sąlygas. Tokiomis aplinkybėmis 29 straipsnio darbo grupė laikosi nuomonės, kad atsakomybės standartas neturėtų būti mažinamas dėl ekonominės pusiausvyros nebuvimo ir kad turi būti išlaikytas sąvokos „duomenų valdytojas" supratimas[248].

Siekiant aiškumo ir skaidrumo, išsami informacija apie duomenų valdytojo ir duomenų tvarkytojo santykius turi būti pateikiama rašytinėje sutartyje[249]. Sutartyje visų pirma privaloma aptarti duomenų tvarkymo dalyką, pobūdį, tikslą ir trukmę, asmens duomenų rūšį ir duomenų subjektų kategorijas. Joje taip pat turėtų būti nustatytos duomenų valdytojo ir duomenų tvarkytojo pareigos ir teisės, pavyzdžiui, konfidencialumo ir saugumo reikalavimai. Tokios sutarties nebuvimas yra duomenų valdytojo pareigos pateikti rašytinius tarpusavio atsakomybės dokumentus pažeidimas ir už tai gali būti taikomos sankcijos. Kai žala padaroma dėl veikimo nepaisant duomenų valdytojo teisėtų nurodymų arba juos pažeidžiant, atsakomybėn gali būti traukiamas ne tik duomenų valdytojas, bet ir duomenų tvarkytojas[250]. Duomenų tvarkytojas privalo saugoti visų kategorijų duomenų tvarkymo veiklos, kurią jis vykdo duomenų valdytojo vardu, įrašus[251]. Šie įrašai turi būti pateikti priežiūros institucijai jos prašymu, nes ir duomenų valdytojas, ir duomenų tvarkytojas, vykdydami savo užduotis, turi bendradarbiauti su ta institucija[252]. Duomenų valdytojai ir duomenų tvarkytojai taip pat turi galimybę laikytis patvirtinto elgesio kodekso arba sertifikavimo mechanizmo, kad įrodytų savo atitiktį BDAR reikalavimams[253].

246 *Ten pat*, 82 straipsnio 2 punktas.

247 29 straipsnio darbo grupė (2010 m.), *Nuomonė Nr. 1/2010 dėl sąvokų „duomenų valdytojas" ir „duomenų tvarkytojas"*, WP 169, Briuselis, 2010 m. vasario 16 d., p. 25; 29 straipsnio darbo grupė (2006 m.), *Nuomonė Nr. 10/2006 dėl Pasaulinės tarpbankinių finansinių telekomunikacijų organizacijos (SWIFT) atliekamo asmens duomenų tvarkymo,* WP 128, Briuselis, 2006 m. lapkričio 22 d.

248 29 straipsnio darbo grupė (2010 m.), *Nuomonė Nr. 1/2010 dėl sąvokų „duomenų valdytojas" ir „duomenų tvarkytojas"*, WP 169, Briuselis, 2010 m. vasario 16 d., p. 26.

249 Bendrojo duomenų apsaugos reglamento 28 straipsnio 3 ir 9 dalys.

250 *Ten pat*, 82 straipsnio 2 dalis.

251 *Ten pat*, 30 straipsnio 2 dalis.

252 *Ten pat*, 30 straipsnio 4 dalis ir 31 straipsnis.

253 *Ten pat*, 28 straipsnio 5 dalis ir 42 straipsnio 4 dalis.

Duomenų tvarkytojai gali norėti perduoti tam tikras užduotis kitiems duomenų tvarkytojams. Tai yra teisiškai leistina, jeigu tarp duomenų valdytojo ir duomenų tvarkytojo nustatomos atitinkamos sutartinės sąlygos, įskaitant tai, ar kiekvienu atveju duomenų valdytojo leidimas yra būtinas, ar pakanka tik informuoti. BDAR nustatyta, kad pirminis duomenų tvarkytojas išlieka visiškai atsakingas duomenų valdytojui, jei pagalbinis duomenų tvarkytojas nevykdo savo duomenų apsaugos prievolių[254].

Pagal ET teisę visapusiškai taikomas pirmiau pateiktas sąvokų „duomenų valdytojas" ir „duomenų tvarkytojas" išaiškinimas[255].

2.3.2. Gavėjai ir trečiosios šalys

Duomenų apsaugos direktyvoje nustatytą skirtumą tarp šių dviejų kategorijų asmenų arba subjektų iš esmės lemia jų santykiai su duomenų valdytoju, taigi ir jų galimybė susipažinti su duomenų valdytojo turimais asmens duomenimis.

Trečioji šalis – tai kitas nei duomenų valdytojas ir duomenų tvarkytojas subjektas. Pagal BDAR 4 straipsnio 10 punktą trečioji šalis – „fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuri nėra duomenų subjektas, duomenų valdytojas, duomenų tvarkytojas, arba asmenys, kuriems tiesioginiu duomenų valdytojo ar duomenų tvarkytojo įgaliojimu leidžiama tvarkyti asmens duomenis". Tai reiškia, kad organizacijai, kuri nėra duomenų valdytoja, net jei ji priklauso tai pačiai grupei arba patronuojančiajai įmonei, dirbantys asmenys priklausys (arba priklauso) „trečiosios šalies" kategorijai. Kita vertus, banko filialai, kurie tvarko kliento sąskaitas tiesiogiai vadovaujant jų buveinei, nebūtų „trečiosios šalys"[256].

Sąvoka „gavėjas" yra platesnė nei sąvoka „trečioji šalis". Pagal BDAR 4 straipsnio 9 punktą, gavėjas – „fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuriai atskleidžiami asmens duomenys, nesvarbu, ar tai trečioji šalis ar ne". Šis gavėjas gali būti duomenų valdytojui arba duomenų tvarkytojui nepriklausantis asmuo, – tokiu atveju tai būtų trečioji šalis, – arba duomenų valdytojo arba duomenų tvarkytojo vidaus subjektas, pavyzdžiui, darbuotojas arba kitas tos pačios įmonės arba institucijos skyrius.

254 *Ten pat*, 28 straipsnio 4 dalis.

255 Žr., pvz., atnaujintos 108-osios konvencijos 2 straipsnio b ir f punktus; Rekomendacijos dėl profiliavimo 1 straipsnį.

256 29 straipsnio darbo grupė (2010 m.), *Nuomonė Nr. 1/2010 dėl sąvokų „duomenų valdytojas" ir „duomenų tvarkytojas"*, WP 169, Briuselis, 2010 m. vasario 16 d., p. 31.

Skirtumas tarp gavėjų ir trečiųjų šalių yra svarbus tik dėl teisėto duomenų atskleidimo sąlygų. Duomenų valdytojo arba duomenų tvarkytojo darbuotojai gali būti asmens duomenų gavėjai be papildomų teisinių reikalavimų, jeigu jie dalyvauja duomenų valdytojo arba duomenų tvarkytojo vykdomose duomenų tvarkymo operacijose. Trečioji šalis, kuri veikia atskirai nuo duomenų valdytojo ar duomenų tvarkytojo, nėra įgaliota naudoti duomenų valdytojo tvarkomų asmens duomenų, nebent konkrečiu atveju galioja konkretūs teisiniai pagrindai.

Pavyzdys. Duomenų valdytojo darbuotojas, kuris asmens duomenis naudoja vykdydamas jam darbdavio pavestas užduotis, yra duomenų gavėjas, bet ne trečioji šalis, nes jis duomenis naudoja duomenų valdytojo vardu ir vadovaudamasis duomenų valdytojo nurodymais. Pavyzdžiui, jeigu darbdavys, atsižvelgdamas į būsimą darbo rezultatų vertinimą, atskleidžia savo darbuotojų asmens duomenis savo žmogiškųjų išteklių departamentui, žmogiškųjų išteklių grupė bus asmens duomenų gavėja, nes duomenys jai buvo atskleisti duomenų valdytojui tvarkant duomenis.

Tačiau jeigu organizacija savo darbuotojų duomenis teikia mokymo įmonei, kuri juos naudoja tam, kad pritaikytų mokymo programą prie darbuotojų poreikių, mokymo įmonė yra trečioji šalis. Taip yra todėl, kad mokymo įmonė neturi konkretaus teisėto pagrindo arba įgaliojimo (kuris „žmogiškųjų išteklių“ atveju atsiranda iš darbo santykių su duomenų valdytoju) tvarkyti šiuos asmens duomenis. Kitaip tariant, dirbdama su duomenų valdytoju, ji negavo informacijos.

2.4. Sutikimas

Pagrindiniai faktai

- Sutikimas, kaip asmens duomenų tvarkymo pagrindas, turi būti duotas laisva valia, pagrįstas informacija, konkretus ir vienareikšmiškai išreikštas aiškiu patvirtinamuoju veiksmu, kuriuo pritariama duomenų tvarkymui.
- Specialių kategorijų duomenims tvarkyti reikalingas aiškus sutikimas.

Sutikimas yra vienas iš šešių teisėtų asmens duomenų tvarkymo pagrindų; tai bus išsamiai paaiškinta 4 skyriuje. Sutikimas – tai „laisva valia duotas, konkretus ir nedviprasmiškas tinkamai informuoto duomenų subjekto valios išreiškimas“[257].

ES teisėje nustatyta keletas galiojančio sutikimo elementų, kuriais siekiama užtikrinti, kad duomenų subjektai tikrai sutiktų, kad jų duomenys būtų naudojami konkrečiu būdu[258]:

- Sutikimas turi būti duodamas aiškiu patvirtinamuoju veiksmu, kuriuo savanoriškai, konkrečiai, turint pakankamai informacijos ir aiškiai nurodoma, kad duomenų subjektas sutinka, kad jo asmens duomenys būtų tvarkomi. Tai gali būti veiksmas arba pareiškimas.

- Duomenų subjektui turi būti suteikta teisė bet kuriuo metu atšaukti sutikimą.

- Teikiant rašytinį pareiškimą, kuris apima ir kitus klausimus, pavyzdžiui, „įteikimo sąlygas“, prašymai duoti sutikimą turi būti pateikiami aiškia ir paprasta kalba, suprantama ir lengvai prieinama forma, aiškiai atskiriant sutikimą nuo kitų klausimų; jei šios deklaracijos dalis pažeidžia BDAR, ji nėra privaloma.

Sutikimas pagal duomenų apsaugos teisę galios, tik jeigu bus įgyvendinti visi šie reikalavimai. Būtent duomenų valdytojas privalo įrodyti, kad duomenų subjektas sutiko, kad jo duomenys būtų tvarkomi[259]. Galiojančio sutikimo aspektai išsamiau bus aptarti 4.1.1 skyriuje dėl teisėtų asmens duomenų tvarkymo pagrindų.

108-ojoje konvencijoje sutikimo apibrėžtis nepateikiama; šis klausimas turi būti aptartas nacionalinėje teisėje. Tačiau **pagal ET teisę** galiojančio sutikimo elementai atitinka pirmiau paaiškintus elementus[260].

Civilinėje teisėje nustatyti papildomi galiojančio sutikimo reikalavimai, pavyzdžiui, veiksnumas, paprastai taikomi ir duomenų apsaugos srityje, nes tokie reikalavimai yra pagrindinės teisinės sąlygos. Veiksnumo neturinčių asmenų negaliojantis sutikimas reikš, kad nėra teisinio pagrindo tvarkyti tokių asmenų duomenis. Kalbant

257 Bendrojo duomenų apsaugos reglamento 4 straipsnio 11 punktas. Taip pat žr. atnaujintos 108-osios konvencijos 5 straipsnio 2 dalį.

258 Bendrojo duomenų apsaugos reglamento 7 straipsnis.

259 *Ten pat*, 7 straipsnio 1 dalis.

260 Atnaujintos 108-osios konvencijos 5 straipsnio 2 dalis; atnaujintos 108-osios konvencijos aiškinamosios ataskaitos 42–45 punktai.

apie nepilnamečių veiksnumą sudaryti sutartis, BDAR nustatyta, kad jo taisyklės dėl minimalaus amžiaus, nuo kurio galima gauti galiojantį sutikimą, nedaro poveikio valstybių narių bendrajai sutarčių teisei[261].

Sutikimas turi būti duodamas aiškiai, kad neliktų abejonių dėl duomenų subjekto ketinimo[262]. Sutikimas turi būti aiškus, kai jis susijęs su neskelbtinų duomenų tvarkymu, ir gali būti duodamas žodžiu arba raštu[263]. Sutikimą galima duoti elektroninėmis priemonėmis[264]. Pagal **ES** ir **ET teisę** asmuo sutikimą tvarkyti jo asmens duomenis privalo duoti padarydamas pareiškimą arba atlikdamas aiškų patvirtinamąjį veiksmą[265]. Todėl sutikimu negali būti laikomas tylėjimas, iš anksto pažymėti langeliai, iš anksto užpildytos formos arba neveikimas[266].

261 Bendrojo duomenų apsaugos reglamento 8 straipsnio 3 dalis.

262 *Ten pat*, 6 straipsnio 1 dalies a punktas ir 9 straipsnio 2 dalies a punktas.

263 *Ten pat*, 32 konstatuojamoji dalis.

264 *Ten pat*.

265 *Ten pat*, 4 straipsnio 11 punktas; atnaujintos108-osios konvencijos aiškinamosios ataskaitos 42 punktas.

266 Bendrojo duomenų apsaugos reglamento 32 konstatuojamoji dalis ir atnaujintos 108-osios konvencijos aiškinamosios ataskaitos 42 punktas.

3

Pagrindiniai Europos duomenų apsaugos teisės principai

ES	Reglamentuojami klausimai	ET
Bendrojo duomenų apsaugos reglamento 5 straipsnio 1 dalies a punktas	**Teisėtumo principas**	Atnaujintos 108-osios konvencijos 5 straipsnio 3 dalis
Bendrojo duomenų apsaugos reglamento 5 straipsnio 1 dalies a punktas	**Sąžiningumo principas**	Atnaujintos 108-osios konvencijos 5 straipsnio 4 dalies a punktas EŽTT, *K. H. ir kiti prieš Slovakiją*, Nr. 32881/04, 2009 m.
Bendrojo duomenų apsaugos reglamento 5 straipsnio 1 dalies a punktas ESTT, C-201/14, *Smaranda Bara ir kt. prieš Casa Națională de Asigurări de Sănătate ir kt.*, 2015 m.	**Skaidrumo principas**	Atnaujintos 108-osios konvencijos 5 straipsnio 4 dalies a punktas ir 8 straipsnis EŽTT, *Haralambie prieš Rumuniją*, Nr. 21737/03, 2009 m.
Bendrojo duomenų apsaugos reglamento 5 straipsnio 1 dalies b punktas	**Tikslų apribojimo principas**	Atnaujintos 108-osios konvencijos 5 straipsnio 4 dalies b punktas
Bendrojo duomenų apsaugos reglamento 5 straipsnio 1 dalies c punktas ESTT, sujungtos bylos C-293/12 ir C-594/12, *Digital Rights Ireland* ir Kärntner Landesregierung ir kt. (DK), 2014 m.	**Duomenų kiekio mažinimo principas**	Atnaujintos 108-osios konvencijos 5 straipsnio 4 dalies c punktas

ES	Reglamentuojami klausimai	ET
Bendrojo duomenų apsaugos reglamento 5 straipsnio 1 dalies d punktas ESTT, C-553/07, *College van burgemeester en wethouders van Rotterdam prieš M. E. E. Rijkeboer*, 2009 m.	**Duomenų tikslumo principas**	Atnaujintos 108-osios konvencijos 5 straipsnio 4 dalies d punktas
Bendrojo duomenų apsaugos reglamento 5 straipsnio 1 dalies e punktas ESTT, sujungtos bylos C-293/12 ir C-594/12, *Digital Rights Ireland* ir Kärntner Landesregierung ir kt., (DK), 2014 m.	**Saugojimo trukmės apribojimo principas**	Atnaujintos 108-osios konvencijos 5 straipsnio 4 dalies e punktas EŽTT, *S. ir Marper prieš Jungtinę Karalystę* (DK), Nr. 30562/04 ir 30566/04, 2008 m.
Bendrojo duomenų apsaugos reglamento 5 straipsnio 1 dalies f punktas ir 32 straipsnis	**Duomenų saugumo (vientisumo ir konfidencialumo) principas**	Atnaujintos 108-osios konvencijos 7 straipsnis
Bendrojo duomenų apsaugos reglamento 5 straipsnio 2 dalis	**Atskaitomybės principas**	Atnaujintos 108-osios konvencijos 10 straipsnis

Bendrojo duomenų apsaugos reglamento 5 straipsnyje nustatyti asmens duomenų tvarkymą reglamentuojantys principai. Šie principai apima:

- teisėtumą, sąžiningumą ir skaidrumą;
- tikslų apribojimą;
- duomenų kiekio mažinimą;
- duomenų tikslumą;
- saugojimo trukmės apribojimą;
- vientisumą ir konfidencialumą.

Principai naudojami kaip atskaitos taškas kituose reglamento straipsniuose nustatant išsamesnes nuostatas. Jie taip pat numatyti atnaujintos 108-osios konvencijos 5, 7, 8 ir 10 straipsniuose. Visi vėlesni ET arba ES lygmeniu priimami duomenų apsaugos teisės aktai turi atitikti šiuos principus, be to, į juos būtina atsižvelgti aiškinant tokius teisės aktus. Pagal ES teisę duomenų tvarkymo principus apriboti galima tik

tiek, kiek tokie apribojimai atitinka 12–22 straipsniuose nustatytas teises ir pareigas, ir tokiais apribojimais turi būti paisoma pagrindinių teisių ir laisvių esmės. Bet kokios šių pagrindinių principų išimtys ir apribojimai gali būti numatyti ES arba nacionaliniu lygmeniu[267]; jie turi būti numatyti įstatymu, jais turi būti siekiama teisėto tikslo ir jie turi būti būtini bei proporcingi demokratinėje visuomenėje[268]. Turi būti įvykdytos visos trys sąlygos.

3.1. Duomenų tvarkymo teisėtumo, sąžiningumo ir skaidrumo principai

Pagrindiniai faktai

- Teisėtumo, sąžiningumo ir skaidrumo principai taikomi visai asmens duomenų tvarkymo veiklai.
- BDAR nustatyta, kad pagal teisėtumo principą reikalaujama, kad duomenys būtų tvarkomi pagal vieną iš šių sąlygų:
  - duomenų subjekto sutikimas;
  - būtinybė sudaryti sutartį;
  - teisinė prievolė;
  - būtinybė apsaugoti duomenų subjekto arba kito asmens gyvybinius interesus;
  - būtinybė atlikti užduotį viešojo intereso labui;
  - duomenų valdytojo arba trečiosios šalies teisėtų interesų būtinybė, jeigu už šiuos interesus nėra viršesni duomenų subjekto interesai ir teisės.
- Asmens duomenys turėtų būti tvarkomi sąžiningai.
  - Duomenų subjektą privaloma informuoti apie riziką, siekiant užtikrinti, kad duomenų tvarkymas nesukeltų nenumatytų neigiamų pasekmių.

267 Atnaujintos 108-osios konvencijos 5 straipsnio 1 dalies c punktas; Bendrojo duomenų apsaugos reglamento 23 straipsnio 1 dalis.

268 Bendrojo duomenų apsaugos reglamento 23 straipsnio 1 punktas.

- Asmens duomenys turėtų būti tvarkomi skaidriai.
  - Duomenų valdytojai prieš pradėdami tvarkyti duomenų subjektų duomenis privalo informuoti juos, be kita ko, apie duomenų tvarkymo tikslą ir duomenų valdytojo tapatybę ir adresą.
  - Informaciją apie duomenų tvarkymo operacijas privaloma pateikti aiškia ir paprasta kalba, kad duomenų subjektai galėtų lengvai suprasti taisykles, riziką, apsaugos priemones ir susijusias teises.
  - Duomenų subjektai turi teisę susipažinti su savo duomenimis visais atvejais, kai duomenys yra tvarkomi.

3.1.1. Duomenų tvarkymo teisėtumas

Pagal **ES ir ET duomenų apsaugos įstatymus** reikalaujama asmens duomenis tvarkyti teisėtai[269]. Teisėtas duomenų tvarkymas reiškia, kad duomenų subjektas turi duoti sutikimą arba turi galioti kitas duomenų apsaugos teisės aktuose nustatytas teisėtas pagrindas[270]. BDAR 6 straipsnio 1 dalyje be sutikimo nustatyti penki teisėti duomenų tvarkymo pagrindai, t. y. tvarkyti duomenis būtina siekiant įvykdyti sutartį, atlikti užduotį, vykdant viešosios valdžios funkcijas, įvykdyti teisinę prievolę, siekiant teisėtų duomenų valdytojo arba trečiosios šalies interesų arba jeigu tai būtina norint apsaugoti duomenų subjekto gyvybinius interesus. Šie pagrindai išsamiau bus aptarti 4.1 skirsnyje.

3.1.2. Tvarkymo sąžiningumas

Be teisėto duomenų tvarkymo, pagal ES ir ET duomenų apsaugos įstatymus reikalaujama asmens duomenis tvarkyti sąžiningai[271]. Pagal sąžiningo duomenų tvarkymo principą visų pirma reglamentuojami duomenų valdytojo ir duomenų subjekto santykiai.

Duomenų valdytojai turėtų pranešti duomenų subjektams ir plačiajai visuomenei, kad jie tvarkys duomenis teisėtai ir skaidriai, ir privalo sugebėti įrodyti, kad duomenų tvarkymo operacijos atitinka BDAR. Duomenų tvarkymo operacijų negalima atlikti

269 Atnaujintos 108-osios konvencijos 5 straipsnio 3 dalis; Bendrojo duomenų apsaugos reglamento 5 straipsnio 1 dalies a punktas.

270 Europos Sąjungos pagrindinių teisių chartijos 8 straipsnio 2 dalis; Bendrojo duomenų apsaugos reglamento 40 konstatuojamoji dalis ir 6–9 straipsniai; atnaujintos108-osios konvencijos 5 straipsnio 2 dalis; atnaujintos 108-osios konvencijos aiškinamosios ataskaitos 41 punktas.

271 Bendrojo duomenų apsaugos reglamento 5 straipsnio 1 dalies a punktas; atnaujintos 108-osios konvencijos 5 straipsnio 4 dalies a punktas.

slaptai ir duomenų subjektai turėtų žinoti apie galimą riziką. Be to, duomenų valdytojai, kiek įmanoma, privalo veikti taip, kad greitai įgyvendintų duomenų subjekto pageidavimus, ypač tais atvejais, kai jo sutikimas yra duomenų tvarkymo teisinis pagrindas.

Pavyzdys. Byloje *K. H. ir kiti prieš Slovakiją*[272] pareiškėjos – romų etninės kilmės moterys – nėštumo ir gimdymo metu buvo gydomos dviejose rytinėje Slovakijos dalyje esančiose ligoninėse. Paskui nė viena iš jų negalėjo vėl pastoti, nepaisant pakartotinių bandymų. Nacionaliniai teismai liepė ligoninėms leisti pareiškėjoms ir jų atstovams susipažinti su medicinos dokumentais ir daryti jų išrašus ranka, tačiau nepatenkino jų prašymo daryti dokumentų fotokopijas, tariamai siekdamas užkirsti kelią piktnaudžiavimui jais. Valstybių „pozityviosios prievolės" pagal EŽTK 8 straipsnį reiškė prievolę leisti duomenų subjektui daryti savo duomenų bylų kopijas. Būtent valstybė turėjo nustatyti asmens duomenų bylų kopijų darymo tvarką arba, kai tinkama, nurodyti pagrįstas priežastis, dėl kurių atsisakoma tai daryti. Pareiškėjų atveju nacionaliniai teismai draudimą pareiškėjoms daryti savo medicinos dokumentų kopijas iš esmės grindė poreikiu užtikrinti, kad nebūtų piktnaudžiaujama atitinkama informacija. Tačiau EŽTT nebuvo aišku, kaip pareiškėjos, kurioms bet kuriuo atveju buvo leista susipažinti su visais jų medicinos dokumentais, galėjo piktnaudžiauti su jomis susijusia informacija. Be to, tokiam netinkamam naudojimui buvo galima užkirsti kelią ir kitomis priemonėmis, o ne vien draudžiant pareiškėjoms daryti bylų kopijas. Valstybė neįrodė, kad yra pakankamai įtikinamų priežasčių neleisti pareiškėjoms veiksmingai susipažinti su informacija apie savo sveikatą. EŽTT padarė išvadą, kad buvo pažeistas EŽTK 8 straipsnis.

Kalbant apie interneto paslaugas, pažymėtina, kad dėl duomenų tvarkymo sistemų ypatumų duomenų subjektams turi būti įmanoma iš tikrųjų suprasti, kas daroma su jų duomenimis. Bet kuriuo atveju sąžiningumo principas apima ne tik prievolę užtikrinti skaidrumą; jis taip pat galėtų būti siejamas su etiniu asmens duomenų tvarkymu.

272 EŽTT, *K. H. ir kiti prieš Slovakiją*, Nr. 32881/04, 2009 m. balandžio 28 d.

Pavyzdys. Universiteto mokslinių tyrimų departamentas atlieka eksperimentą, kuriame analizuojami 50 subjektų nuotaikų pokyčiai. Subjektai privalo kiekvieną valandą tam tikru laiku užregistruoti savo mintis elektroninėje rinkmenoje. 50 asmenų davė sutikimą dalyvauti šiame konkrečiame projekte ir kad universitetas šiuo konkrečiu būdu naudotų duomenis. Mokslinių tyrimų departamentas netrukus išsiaiškina, kad minčių registravimas elektroniniu būdu būtų labai naudingas kitam projektui, susijusiam su psichikos sveikata, kurį koordinuotų kita grupė. Net jeigu universitetas, kaip duomenų valdytojas, galėjo tuos pačius duomenis naudoti kitos grupės darbui nesiimdamas papildomų veiksmų, kad užtikrintų tų duomenų tvarkymo teisėtumą, atsižvelgiant į tai, kad tikslai yra suderinami, universitetas, vadovaudamasis savo mokslinių tyrimų etikos kodeksu ir sąžiningo duomenų tvarkymo principu, informavo subjektus ir prašė duoti naują sutikimą.

3.1.3. Duomenų tvarkymo skaidrumas

Pagal **ES ir ET duomenų apsaugos teisės aktus** reikalaujama, kad asmens duomenys „subjekto atžvilgiu [būtų] tvarkomi <...> skaidriu būdu“[273].

Šiuo principu nustatoma duomenų valdytojo prievolė imtis bet kokių tinkamų priemonių siekiant nuolat informuoti duomenų subjektus, kurie gali būti naudotojai, pirkėjai arba klientai, apie tai, kaip naudojami jų duomenys[274]. Skaidrumas gali reikšti informaciją, kuri asmeniui pateikiama prieš pradedant tvarkyti duomenis[275], informaciją, kuri duomenų subjektams turėtų būti iš anksto prieinama duomenų tvarkymo metu[276], taip pat informaciją, kuri duomenų subjektams pateikiama gavus jų prašymą susipažinti su savo duomenimis[277].

Pavyzdys. Byloje *Haralambie prieš Rumuniją*[278] pareiškėjui buvo leista susipažinti su slaptosios tarnybos turima informacija tik praėjus penkeriems metams nuo prašymo pateikimo. EŽTT pakartojo, kad asmenys, kurių asmens bylas laikė valdžios institucijos, turėjo gyvybiškai svarbų interesą turėti galimybę

273 Bendrojo duomenų apsaugos reglamento 5 straipsnio 1 dalies a punktas; atnaujintos 108-osios konvencijos 5 straipsnio 4 dalies a punktas ir 8 straipsnis.

274 Bendrojo duomenų apsaugos reglamento 12 straipsnis.

275 *Ten pat*, 13 ir 14 straipsniai.

276 29 straipsnio darbo grupė, *Nuomonė 2/2017 dėl duomenų tvarkymo darbe*, p. 23.

277 Bendrojo duomenų apsaugos reglamento 15 straipsnis.

278 EŽTT, *Haralambie prieš Rumuniją*, Nr. 21737/03, 2009 m. spalio 27 d.

susipažinti su jomis. Institucijos buvo įpareigotos numatyti veiksmingą tokios informacijos gavimo procedūrą. EŽTT nusprendė, kad nei perduotų bylų skaičius, nei archyvavimo sistemos trūkumai nebuvo pagrindas pareiškėjo prašymą susipažinti su savo bylomis patenkinti tik po penkerių metų. Institucijos nepateikė pareiškėjui veiksmingos ir prieinamos procedūros, kuri sudarytų jam sąlygas per pagrįstą terminą susipažinti su savo asmeninėmis bylomis. Teismas padarė išvadą, kad buvo pažeistas EŽTK 8 straipsnis.

Duomenų subjektams privaloma lengvai suprantamu būdu paaiškinti duomenų tvarkymo operacijas ir taip užtikrinti, kad jie suprastų, kas bus daroma su jų duomenimis. Tai reiškia, kad duomenų subjektas asmens duomenų rinkimo metu privalo žinoti asmens duomenų tvarkymo tikslus[279]. Pagal skaidraus duomenų tvarkymo principą reikalaujama vartoti aiškią ir paprastą kalbą[280]. Atitinkamiems asmenims privaloma paaiškinti su jų asmens duomenų tvarkymu susijusią riziką, taisykles, apsaugos priemones ir teises[281].

ET teisėje taip pat konkrečiai nustatyta, kad duomenų valdytojas privalo duomenų subjektams aktyviai teikti tam tikrą esminę privalomą informaciją. Informacija apie duomenų valdytojo (arba bendrų duomenų valdytojų) pavadinimą ir adresą, duomenų tvarkymo teisinį pagrindą ir tikslus, tvarkomų duomenų kategorijas ir gavėjus, taip pat teisių įgyvendinimo priemones gali būti suteikiama bet kuriuo tinkamu formatu (svetainėje, per asmeniniams prietaisams skirtas technologines priemones ir pan.), jeigu informacija duomenų subjektui pateikiama sąžiningai ir veiksmingai. Pateikiama informacija turėtų būti lengvai prieinama, įskaitoma, suprantama ir pritaikyta prie atitinkamų duomenų subjektų (pavyzdžiui, vaikams suprantama kalba, jei to reikia). Bet kuri papildoma informacija, kuri yra būtina siekiant užtikrinti sąžiningą duomenų tvarkymą arba kuri yra naudinga siekiant tokio tikslo, pavyzdžiui, saugojimo laikotarpis, žinios apie duomenų tvarkymo motyvus arba informacija apie duomenų perdavimo kitai susitariančiajai arba nesusitariančiajai šaliai (įskaitant informaciją, ar ta konkreti nesusitariančioji šalis užtikrina tinkamo lygio apsaugą arba ar duomenų valdytojas ėmėsi priemonių, kad garantuotų tokį duomenų apsaugos lygį) atvejus, taip pat turi būti pateikiama[282].

279 Bendrojo duomenų apsaugos reglamento 39 konstatuojamoji dalis.

280 *Ten pat*.

281 *Ten pat*.

282 Atnaujintos 108-osios konvencijos aiškinamosios ataskaitos 68 punktas.

Teisė susipažinti su informacija[283] reiškia, kad duomenų subjektas turi teisę, kad jam paprašius duomenų valdytojas jam praneštų, ar jo asmens duomenys yra tvarkomi, ir, jeigu taip, kokie duomenys yra tvarkomi[284]. Be to, įgyvendindami teisę į informaciją[285], asmenis, kurių duomenys yra tvarkomi, duomenų valdytojai arba duomenų tvarkytojai aktyviai iš esmės prieš prasidedant duomenų tvarkymo veiklai, be kita ko, privalo informuoti apie duomenų tvarkymo tikslus, trukmę ir priemones.

Pavyzdys. Byla *Smaranda Bara ir kt. prieš Preşidentele Casei Naţionale de Asigurări de Sănătate, Casa Naţională de Administrare Fiscală (ANAF)*[286] buvo susijusi su nacionalinio mokesčių administratoriaus mokesčių duomenų apie savarankiškai dirbančių asmenų pajamas perdavimu Rumunijos nacionaliniam sveikatos draudimo fondui, kuriuo remiantis buvo reikalaujama sumokėti sveikatos draudimo įmokų įsiskolinimus. ESTT buvo prašoma nustatyti, ar duomenų subjektui reikėjo pateikti išankstinę informaciją apie duomenų valdytojo tapatybę ir duomenų perdavimo tikslą prieš šiuos duomenis pradedant tvarkyti nacionaliniam sveikatos draudimo fondui. ESTT nusprendė, kad tais atvejais, kai valstybės narės viešojo administravimo įstaiga perduoda asmens duomenis kitai viešojo administravimo įstaigai, kuri toliau tvarko tuos duomenis, duomenų subjektus privaloma informuoti apie tą duomenų perdavimą arba tvarkymą.

Tam tikrose situacijose galima taikyti nukrypti nuo prievolės informuoti duomenų subjektus apie duomenų tvarkymą leidžiančias nuostatas, kurios bus išsamiau aptartos 6.1 skirsnyje dėl duomenų subjekto teisių.

283 Bendrojo duomenų apsaugos reglamento 15 straipsnis.

284 Atnaujintos 108-osios konvencijos 8 straipsnis ir 9 straipsnio 1 dalies b punktas.

285 Bendrojo duomenų apsaugos reglamento 13 ir 14 straipsniai.

286 ESTT, C-201/14, *Smaranda Bara ir kt. prieš Casa Naţională de Asigurări de Sănătate ir kt.*, 2015 m. spalio 1 d., 28–46 punktai.

3.2. Tikslų apribojimo principas

Pagrindiniai faktai

- Duomenų tvarkymo tikslą būtina apibrėžti prieš pradedant tvarkyti duomenis.
- Duomenys negali būti tvarkomi su pradiniu tikslu nesuderinamu būdu, nors Bendrajame duomenų apsaugos reglamente numatytos šios taisyklės dėl archyvavimo tikslų viešojo intereso labui, mokslinių arba istorinių tyrimų tikslais arba statistiniais tikslais išimčių.
- Iš esmės tikslų apribojimo principas reiškia, kad bet koks asmens duomenų tvarkymas turi būti atliekamas siekiant konkretaus aiškiai apibrėžto tikslo ir tik papildomų konkrečių tikslų, kurie yra suderinami su pradiniu tikslu.

Tikslų apribojimo principas yra vienas iš pagrindinių Europos duomenų apsaugos teisės principų. Jis yra glaudžiai susijęs su skaidrumu, nuspėjamumu ir naudotojo kontrole: jeigu duomenų tvarkymo tikslas yra pakankamai konkretus ir aiškus, asmenys žino, ko tikėtis, be to, taip sustiprinamas skaidrumas ir teisinis tikrumas. Kartu svarbu aiškiai apibrėžti tikslą, kad duomenų subjektai galėtų veiksmingai įgyvendinti savo teises, pavyzdžiui, teisę nesutikti su duomenų tvarkymu[287].

Pagal principą reikalaujama, kad bet koks asmens duomenų tvarkymas turi būti atliekamas siekiant konkretaus aiškiai apibrėžto tikslo ir tik papildomų tikslų, kurie yra suderinami su pradiniu tikslu[288]. Todėl asmens duomenų tvarkymas neapibrėžtais ir (arba) neribotais tikslais yra neteisėtas. Asmens duomenų tvarkymas neturint tam tikro tikslo, atsižvelgiant į tai, kad jie kažkada gali būti naudingi ateityje, taip pat yra neteisėtas. Asmens duomenų tvarkymo teisėtumas priklausys nuo duomenų tvarkymo tikslo, kuris turi būti aiškus, konkretus ir teisėtas.

Kiekvienas naujas duomenų tvarkymo tikslas, kuris yra nesuderinamas su pradiniu tikslu, turi būti pagrįstas konkrečiu teisiniu pagrindu ir negali būti grindžiamas tik tuo, kad duomenys iš pradžių buvo įgyti arba tvarkomi kitu teisėtu tikslu. Todėl teisėtas duomenų tvarkymas yra susijęs tik su jo iš pradžių nurodytu tikslu ir bet koks naujas duomenų tvarkymo tikslas turės būti pagrįstas atskiru nauju teisiniu pagrindu. Pavyzdžiui, asmens duomenų atskleidimą trečiosioms šalims siekiant naujo tikslo reikės atidžiai išnagrinėti, nes tikėtina, kad tokiam atskleidimui bus reikalingas papildomas teisinis pagrindas, kuris skirsis nuo duomenų rinkimo tikslo.

287 29 straipsnio darbo grupė (2013 m.), *Nuomonė Nr. 3/2013 dėl tikslų apribojimo*, WP 203, 2013 m. balandžio 2 d.

288 Bendrojo duomenų apsaugos reglamento 5 straipsnio 1 dalies b punktas.

Pavyzdys. Oro linijų bendrovė renka savo keleivių duomenis, kad, naudodamasi užsakymų duomenimis, galėtų sklandžiai vykdyti skrydžius. Oro linijų bendrovei reikės duomenų apie keleivių vietų numerius; specialius fizinius apribojimus, pavyzdžiui, neįgaliųjų vežimėlio poreikį, ir specialius su maistu susijusius reikalavimus, pavyzdžiui, dėl košerinio arba halalinio maisto. Jeigu oro linijų prašoma perduoti šiuos duomenis, kurie laikomi keleivio duomenų įraše, imigracijos institucijoms nusileidimo oro uoste, tuomet šie duomenys naudojami imigracijos kontrolės tikslais, kurie skiriasi nuo pradinio duomenų rinkimo tikslo. Todėl šiuos duomenis perduodant imigracijos institucijai reikės naujo ir atskiro teisinio pagrindo.

Nagrinėjant konkretaus tikslo taikymo sritį ir ribas, pažymėtina, kad atnaujinta 108-oji konvencija ir Bendrasis duomenų apsaugos reglamentas yra grindžiami suderinamumo sąvoka: naudoti duomenis suderinamais tikslais leidžiama remiantis pradiniu teisiniu pagrindu. Todėl tolesnis duomenų tvarkymas negali būti atliekamas nenumatytu, netinkamu arba duomenų subjektui prieštaraujančiu būdu[289]. Siekdamas įvertinti, ar tolesnis duomenų tvarkymas laikytinas suderinamu, duomenų valdytojas (bet kita ko) turėtų atsižvelgti į:

- „sąsajas tarp tų tikslų ir numatomo tolesnio asmens duomenų tvarkymo tikslų;
- aplinkybes, kuriomis asmens duomenys buvo surinkti, visų pirma pagrįstus duomenų subjektų lūkesčius jų santykių su duomenų valdytoju pagrindu dėl tolesnio duomenų naudojimo;
- asmens duomenų pobūdį;
- numatomo tolesnio duomenų tvarkymo pasekmes duomenų subjektams;
- ir tinkamų apsaugos priemonių buvimą tiek pradinėse, tiek numatomose tolesnėse duomenų tvarkymo operacijose“[290]. Tai, pavyzdžiui, būtų galima daryti užšifruojant arba suteikiant pseudonimus.

289 Atnaujintos 108-osios konvencijos aiškinamosios ataskaitos 49 punktas.

290 Bendrojo duomenų apsaugos reglamento 50 konstatuojamoji dalis ir 6 straipsnio 4 dalis; atnaujintos 108-osios konvencijos aiškinamosios ataskaitos 49 punktas.

Pavyzdys. Įmonė *Sunshine* įgyja klientų duomenis valdydama ryšius su klientais. Tuomet ji perduoda šiuos duomenis tiesioginės rinkodaros įmonei *Moonlight*, kuri nori naudoti šiuos duomenis siekdama padėti trečiosioms įmonėms vykdyti rinkodaros kampanijas. Įmonės *Sunshine* atliekamas duomenų perdavimas kitų įmonių vykdomos rinkodaros tikslais reiškia paskesnį duomenų naudojimą nauju tikslu, kuris yra nesuderinamas su ryšių su klientais valdymu, t. y. pradiniu įmonės *Sunshine* klientų duomenų rinkimo tikslu. Todėl duomenų perdavimas įmonei *Moonlight* turi būti grindžiamas atskiru teisiniu pagrindu.

Priešingai, įmonė *Sunshine* naudoja ryšių su klientais valdymo duomenis savo rinkodaros tikslais, t. y. siunčia rinkodaros žinutes apie produktus klientams, o tai paprastai yra laikoma suderinamu tikslu.

Bendrajame duomenų apsaugos reglamente ir atnaujintoje 108-ojoje konvencijoje nustatyta, kad „[t]olesnis duomenų tvarkymas archyvavimo tikslais viešojo intereso labui, mokslinių ar istorinių tyrimų tikslais arba statistiniais tikslais“ *a priori* laikomas suderinamu su pradiniu tikslu[291]. Tačiau toliau tvarkant asmens duomenis, būtina nustatyti tinkamas apsaugos priemones, pavyzdžiui, anoniminti arba pseudoniminti duomenis, taip pat apriboti galimybę susipažinti su duomenimis[292]. Bendrajame duomenų apsaugos reglamente pridedama, kad „[j]ei duomenų subjektas yra davęs sutikimą arba duomenų tvarkymas yra grindžiamas Sąjungos arba valstybės narės teise, o tai demokratinėje visuomenėje yra būtina ir proporcinga priemonė siekiant apsaugoti visų pirma svarbius bendro viešojo intereso tikslus, asmens duomenų valdytojui turėtų būti leidžiama toliau tvarkyti duomenis neatsižvelgiant į tikslų suderinamumą“[293]. Todėl imantis toliau tvarkyti duomenis, duomenų subjektą reikėtų informuoti apie tikslus ir jo teises, pavyzdžiui, teisę nesutikti su duomenų tvarkymu[294].

291 Bendrojo duomenų apsaugos reglamento 5 straipsnio 1 dalies b punktas; atnaujintos 108-osios konvencijos 5 straipsnio 4 dalies b punktas. Tokių nacionalinių nuostatų pavyzdys yra Austrijos duomenų apsaugos aktas (vok. *Datenschutzgesetz*), *Federal Law Gazette* I Nr. 165/1999, 46 paragrafas.

292 Bendrojo duomenų apsaugos reglamento 6 straipsnio 4 dalis; atnaujintos 108-osios konvencijos aiškinamosios ataskaitos 50 punktas.

293 Bendrojo duomenų apsaugos reglamento 50 konstatuojamoji dalis.

294 *Ten pat*.

Pavyzdys. Įmonė *Sunshine* surinko ir saugojo ryšių su klientais valdymo duomenis, susijusius su jos klientais. Tolesnis šių duomenų naudojimas įmonėje *Sunshine* statistinės jos klientų pirkimo įpročių analizės tikslais yra leistinas, nes statistikos sudarymas yra suderinamas tikslas. Nereikia jokio papildomo teisinio pagrindo, pavyzdžiui, duomenų subjekto sutikimo. Tačiau tam, kad toliau tvarkytų duomenis statistiniais tikslais, įmonė *Sunshine* privalo nustatyti tinkamas duomenų subjekto teisių ir laisvių apsaugos priemones. Techninės ir organizacinės priemonės, kurias privalo įgyvendinti įmonė *Sunshine*, gali apimti pseudonimų suteikimą.

3.3. Duomenų kiekio mažinimo principas

Pagrindiniai faktai

- Duomenų tvarkymas turi būti susijęs tik su tuo, kas yra būtina teisėtam tikslui pasiekti.
- Asmens duomenys turėtų būti tvarkomi, tik kai duomenų tvarkymo tikslo negalima pagrįstai pasiekti kitomis priemonėmis.
- Tvarkant duomenis negalima neproporcingai riboti susijusių interesų, teisių ir laisvių.

Tvarkomi tik tokie duomenys, kurie yra „tinkami, svarbūs ir ne pernelyg didelės apimties, kurie atitinka konkrečius tikslus, kuriais jie renkami ir (arba) toliau tvarkomi“[295]. Tvarkyti atrinktų duomenų kategorijos turi būti būtinos siekiant bendro tvarkymo operacijų tikslo ir duomenų valdytojas turėtų užtikrinti, kad būtų renkama tik tokia su duomenimis susijusi informacija, kuri tiesiogiai atitinka konkretų duomenų tvarkymo tikslą.

Pavyzdys. Byloje *Digital Rights Ireland*[296] ESTT nagrinėjo, ar galioja Duomenų saugojimo direktyva, kuria siekta suderinti nacionalines nuostatas dėl asmens duomenų, kuriuos gavo arba tvarkė viešos elektroninių ryšių tarnybos arba tinklai, laikymo ar apdorojimo siekiant juos galimai perduoti su sunkiais nusikaltimais, pavyzdžiui, organizuotu nusikalstamumu ir terorizmu,

295 Atnaujintos 108-osios konvencijos 5 straipsnio 4 dalies c punktas; Bendrojo duomenų apsaugos reglamento 5 straipsnio 1 dalies c punktas.

296 ESTT, sujungtos bylos C-293/12 ir C-594/12, *Digital Rights Ireland Ltd prieš Minister for Communications, Marine and Natural Resources ir kt.* ir Kärntner Landesregierung ir kt. (DK), 2014 m. balandžio 8 d.

kovojančioms kompetentingoms institucijoms. Nepaisant to, kad buvo laikoma, jog šis tikslas iš tikrųjų atitinka bendrojo intereso tikslą, abstrakčios nuostatos, pagal kurias direktyva buvo taikoma „visiems asmenims ir visoms elektroninio ryšio priemonėms bei visiems srauto duomenims visiškai jų nediferencijuojant, nenumatant kokių nors ribojimų ar išimčių pagal kovos su sunkiais nusikaltimais tikslo kriterijų“, buvo laikomos problemiškomis[297].

Be to, pasinaudojant specialiomis privatumą sustiprinančiomis technologijomis, kartais įmanoma apskritai išvengti asmens duomenų naudojimo arba naudoti priemones, kurios padeda sumažinti galimybes priskirti duomenis duomenų subjektui (pavyzdžiui, suteikiant pseudonimus), taip užtikrinant privatumui palankų sprendimo būdo taikymą. Tai visų pirma pasakytina apie sistemas, kuriose tvarkomas didesnis duomenų kiekis.

Pavyzdys. Miesto taryba pasiūlo nuolatiniams miesto viešojo transporto sistemos naudotojams už tam tikrą kainą įsigyti lustinę kortelę. Ant kortelės užrašomas naudotojo vardas ir pavardė, be to, ši informacija elektronine forma taip pat įrašoma kortelės luste. Įlipus į autobusą arba tramvajų, lustinę kortelę reikia priglausti prie, pavyzdžiui, autobusuose arba tramvajuose įtvirtinto kortelių skaitytuvo. Nuskaitytus duomenis skaitytuvas elektroniniu būdu palygina su duomenų bazėje įrašytais kelionės kortelę įsigijusių asmenų vardais ir pavardėmis.

Ši sistema optimaliai neatitinka duomenų kiekio mažinimo principo: patikrinti, ar asmeniui leidžiama naudotis transporto paslaugomis, galima ir nelyginant kortelės lusto duomenų su duomenų bazėje esančiais duomenimis. Pavyzdžiui, pakaktų kortelės luste numatyti specialų elektroninį atvaizdą, pavyzdžiui, brūkšninį kodą, kuris, pridėjus kortelę prie skaitytuvo, patvirtintų kortelės galiojimą. Naudojant tokią sistemą nebūtų įrašomi duomenys apie tai, koks asmuo ir kokiu laiku naudojosi atitinkama transporto priemone. Tai būtų optimalus sprendimas pagal duomenų kiekio mažinimo principą, nes dėl šio principo atsiranda prievolė kuo labiau sumažinti duomenų rinkimą.

Atnaujintos 108-osios konvencijos 5 straipsnio 1 dalyje nustatytas proporcingumo reikalavimas tvarkant asmens duomenis, palyginti su teisėtu siekiamu tikslu. Visais

297 *Ten pat*, 44 ir 57 punktai.

duomenų tvarkymo etapais turi būti užtikrinta tinkama visų susijusių interesų pusiausvyra. Tai reiškia, kad „[d]uomenys, kurie yra adekvatūs ir tinkami, tačiau neproporcingai apribotų pagrindines teises ir laisves, kurioms kyla pavojus, turėtų būti laikomi pernelyg dideliais“[298].

3.4. Duomenų tikslumo principas

Pagrindiniai faktai

- Duomenų valdytojas duomenų tikslumo principą privalo įgyvendinti vykdydamas visas duomenų tvarkymo operacijas.
- Netikslius duomenis privaloma nedelsiant ištrinti arba ištaisyti.
- Siekiant užtikrinti tikslumą, duomenis gali tekti reguliariai tikrinti ir nuolat atnaujinti.

Asmens duomenis turintis duomenų valdytojas naudoja šiuos duomenis tik tuomet, kai imasi priemonių, kurios padeda užtikrinti pagrįstą tikrumą dėl duomenų tikslumo ir naujumo[299].

Prievolę užtikrinti duomenų tikslumą būtina vertinti atsižvelgiant į duomenų tvarkymo tikslo kontekstą.

Pavyzdys. Byloje *Rijkeboer*[300] ESTT nagrinėjo Nyderlandų piliečio prašymą iš Amsterdamo miesto administracijos gauti informaciją apie asmenų, kuriems vietos valdžios institucijos turimi įrašai apie jį buvo perduoti per pastaruosius dvejus metus, tapatybę ir atskleistų duomenų turinį. ESTT nusprendė, kad „teisė į privat[ų] gyvenim[ą] reiškia, kad duomenų subjektas turi galimybę įsitikinti, ar tvarkomi jo asmens duomenys yra tikslūs ir tvarkomi teisėtai, t. y. konkrečiau tariant, ar pagrindiniai duomenys apie jį yra tikslūs ir teikiami teisėtiems jų gavėjams“. ESTT paskui rėmėsi Duomenų apsaugos direktyvos

298 Atnaujintos 108-osios konvencijos aiškinamosios ataskaitos 52 punktas; Bendrojo duomenų apsaugos reglamento 5 straipsnio 1 dalies c punktas.

299 Bendrojo duomenų apsaugos reglamento 5 straipsnio 1 dalies d punktas; atnaujintos 108-osios konvencijos 5 straipsnio 4 dalies d punktas.

300 ESTT, C-553/07, *College van burgemeester en wethouders van Rotterdam prieš M. E. E. Rijkeboer*, 2009 m. gegužės 7 d.

preambule, kurioje nustatyta, kad duomenų subjektams turi būti suteikiamos tokios pat teisės susipažinti su savo asmens duomenimis, kad jie galėtų patikrinti, ar duomenys yra teisingi[301].

Taip pat gali būti atvejų, kai saugomų duomenų atnaujinimas yra teisiškai draudžiamas, nes duomenų saugojimo tikslas iš esmės yra užfiksuoti įvykius kaip istorinę „momentinę nuotrauką".

Pavyzdys. Operacijos medicininis įrašas neturi būti keičiamas, kitaip tariant, „atnaujintas", net jei paaiškėja, kad vėlesniame įraše nurodytos išvados buvo klaidingos. Tokiomis aplinkybėmis galima papildyti tik įrašo pastabas, jei jos aiškiai pažymėtos kaip vėlesniame etape padaryti įnašai.

Kita vertus, gali būti situacijų, kai absoliučiai būtina atnaujinti ir reguliariai patikrinti duomenų tikslumą dėl potencialios žalos, kuri gali būti padaryta duomenų subjektui, jeigu duomenys liktų netikslūs.

Pavyzdys. Jei kas nors nori sudaryti kredito sutartį su banku, bankas paprastai patikrina galimo kliento kreditingumą. Šiuo tikslu galima pasinaudoti specialiomis duomenų bazėmis, kuriose pateikiama privačių asmenų kredito istorija. Jei tokioje duomenų bazėje pateikiami neteisingi arba pasenę duomenys apie asmenį, šis asmuo gali patirti neigiamą poveikį. Todėl tokių duomenų bazių valdytojai turi dėti ypatingas pastangas siekdami laikytis duomenų tikslumo principo.

3.5. Saugojimo trukmės apribojimo principas

Pagrindiniai faktai

- Saugojimo apribojimo principas reiškia, kad asmens duomenys turi būti ištrinti arba anoniminti, kai tik jų nebereikia tiems tikslams, kuriems jie buvo surinkti.

301 Ankstesnės Direktyvos 95/46/EB preambulės 41 konstatuojamoji dalis.

Pagal BDAR 5 straipsnio 1 dalies e punktą ir, panašiai, atnaujintos 108-osios konvencijos 5 straipsnio 4 dalies e punktą reikalaujama, kad asmens duomenys būtų „laikomi tokia forma, kad duomenų subjektų tapatybę būtų galima nustatyti ne ilgiau, nei tai yra būtina tais tikslais, kuriais asmens duomenys" yra tvarkomi. Todėl duomenys turi būti ištrinami arba anoniminami, kai pasiekiami šie tikslai. Šiuo tikslu „duomenų valdytojas turėtų nustatyti duomenų ištrynimo arba periodinės peržiūros terminus" ir taip užtikrinti, kad duomenys nebūtų laikomi ilgiau nei būtina[302].

Byloje *S. ir Marper* EŽTT padarė išvadą, kad pagal pagrindinius principus, kurie įtvirtinti atitinkamuose Europos Tarybos teisės aktuose ir kitų susitariančiųjų šalių teisėje ir praktikoje, duomenų saugojimas, ypač policijos darbo srityje, turi būti proporcingas jų rinkimo tikslui ir jo trukmė turi būti ribota[303].

Pavyzdys. Byloje *S. ir Marper*[304] EŽTT nusprendė, kad abiejų pareiškėjų pirštų atspaudų, ląstelių mėginių ir DNR charakteristikų saugojimas neribotam laikui yra neproporcingas ir nereikalingas demokratinėje visuomenėje, atsižvelgdamas į tai, kad abiejų pareiškėjų baudžiamoji byla buvo nutraukta atitinkamai išteisinimu ir bylos nutraukimu.

Asmens duomenų saugojimo termino apribojimas taikomas tik tiems duomenims, iš kurių, atsižvelgiant į jų saugojimo formą, galima nustatyti duomenų subjektų tapatybę. Todėl nebereikalingus duomenis galima teisėtai saugoti juos anoniminant.

Archyvuoti duomenys viešojo intereso, mokslo ar istorijos tikslais arba statistikos tikslais gali būti saugomi ilgesnį laiką, jei tokie duomenys bus naudojami tik pirmiau nurodytais tikslais[305]. Siekiant apsaugoti duomenų subjekto teises ir laisves, turi būti įgyvendintos tinkamos techninės ir organizacinės nuolatinio asmens duomenų saugojimo ir naudojimo priemonės.

Pagal atnaujintą 108-ąją konvenciją taip pat leidžiama taikyti saugojimo apribojimo principo išimtis, jeigu jos nustatytos įstatyme, jeigu jomis gerbiamos pagrindinės teisės ir laisvės ir jeigu jos yra būtinos ir proporcingos siekiant riboto skaičiaus teisėtų

302 Bendrojo duomenų apsaugos reglamento 39 konstatuojamoji dalis.

303 EŽTT, *S. ir Marper prieš Jungtinę Karalystę* (DK), Nr. 30562/04 ir 30566/04, 2008 m. gruodžio 4 d.; taip pat žr., pvz., EŽTT, *M. M. prieš Jungtinę Karalystę*, Nr. 24029/07, 2012 m. lapkričio 13 d.

304 EŽTT, *S. ir Marper prieš Jungtinę Karalystę* (DK), Nr. 30562/04 ir 30566/04, 2008 m. gruodžio 4 d.

305 Bendrojo duomenų apsaugos reglamento 5 straipsnio 1 dalies e punktas; atnaujintos 108-osios konvencijos 5 straipsnio 4 dalies b punktas ir 11 straipsnio 2 dalis.

tikslų[306]. Tai, be kita ko, apima nacionalinio saugumo užtikrinimą, nusikalstamų veikų tyrimą ir jų baudžiamąjį persekiojimą, baudžiamųjų sankcijų vykdymą, duomenų subjekto apsaugą ir kitų asmenų teisių ir pagrindinių laisvių apsaugą.

Pavyzdys. Byloje *Digital Rights Ireland*[307] ESTT peržiūrėjo Duomenų saugojimo direktyvos, kuria siekta suderinti nacionalines nuostatas, susijusias su asmens duomenų, kuriuos gavo arba tvarkė viešos elektroninių ryšių tarnybos arba tinklai, saugojimu kovos su sunkiais nusikaltimais, pavyzdžiui, organizuotu nusikalstamumu ir terorizmu, tikslais, galiojimo klausimą. Duomenų saugojimo direktyvoje nustatytas duomenų saugojimo laikotarpis, kuris yra „bent šeši mėnesi[ai], visiškai nediferencijuojant šio reikalavimo pagal šios direktyvos 5 straipsnyje numatytas skirtingas duomenų kategorijas, remiantis šių tikėtinu naudingumu siekiamam tikslui arba ryšiu su atitinkamais asmenimis“[308]. ESTT taip pat iškėlė klausimą dėl to, kad Duomenų saugojimo direktyvoje nebuvo objektyvių kriterijų, kuriais remiantis turi būti nustatytas tikslus duomenų saugojimo laikotarpis, kuris gali skirtis nuo mažiausiai šešių mėnesių iki daugiausiai 24 mėnesių, siekiant užtikrinti, kad toks laikotarpis neviršytų to, kas griežtai būtina[309].

3.6. Duomenų saugumo principas

Pagrindiniai faktai

- Asmens duomenų saugumas ir konfidencialumas yra labai svarbūs siekiant užkirsti kelią duomenų subjektui daromam neigiamam poveikiui.
- Saugumo priemonės gali būti techninio ir (arba) organizacinio pobūdžio.
- Pseudonimų suteikimas yra procesas, kuris gali padėti apsaugoti asmens duomenis.
- Saugumo priemonių tinkamumas turi būti nustatomas kiekvienu konkrečiu atveju ir reguliariai peržiūrimas.

306 Atnaujintos 108-osios konvencijos 11 straipsnio 1 dalis; atnaujintos 108-osios konvencijos aiškinamosios ataskaitos 91–98 punktai.

307 ESTT, sujungtos bylos C-293/12 ir C-594/12, *Digital Rights Ireland Ltd prieš Minister for Communications, Marine and Natural Resources ir kt.* ir Kärntner Landesregierung ir kt. (DK), 2014 m. balandžio 8 d.

308 *Ten pat*, 63 punktas.

309 *Ten pat*, 64 punktas.

Pagal duomenų saugumo principą reikalaujama, kad tvarkant asmens duomenis būtų įgyvendinamos tinkamos techninės ar organizacinės priemonės, siekiant apsaugoti duomenis nuo atsitiktinės, neleistinos ar neteisėtos prieigos, naudojimo, pakeitimo, atskleidimo, praradimo, sunaikinimo ar sugadinimo[310]. BDAR nustatyta, kad, įgyvendindamas tokias priemones, duomenų valdytojas ir duomenų tvarkytojas atsižvelgia „į techninių galimybių išsivystymo lygį, įgyvendinimo sąnaudas bei duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, taip pat duomenų tvarkymo keliamus įvairios tikimybės ir rimtumo pavojus fizinių asmenų teisėms ir laisvėms“[311]. Priklausomai nuo kiekvieno atvejo konkrečių aplinkybių, tinkamos techninės ir organizacinės priemonės galėtų apimti, pavyzdžiui, pseudonimų suteikimą ir asmens duomenų šifravimą ir (arba) reguliarų priemonių, kuriomis užtikrinamas duomenų tvarkymo saugumas, testavimą ir vertinimą[312].

Kaip paaiškinta 2.1.1 skirsnyje, pseudonimų duomenims suteikimas reiškia asmens duomenų požymių, pagal kuriuos galima nustatyti duomenų subjekto tapatybę, pakeitimą pseudonimu ir šių požymių atskyrimą taikant technines ar organizacines priemones. Pseudonimų suteikimo proceso nereikia painioti su anoniminimo procesu, kurį taikant panaikinamos visos sąsajos, kuriomis remiantis galima nustatyti asmens tapatybę.

Pavyzdys. Sakinys „Charlesas Spenceris, gimęs 1967 m. balandžio 3 d., yra keturių vaikų (dviejų berniukų ir dviejų mergaičių) tėvas“ gali būti pseudonimizuojamas taip:

„C. S. 1967 yra keturių vaikų, dviejų berniukų ir dviejų mergaičių, šeimos tėvas“ arba

„324 yra keturių vaikų, dviejų berniukų ir dviejų mergaičių, šeimos tėvas“, arba

„YESz320l yra keturių vaikų, dviejų berniukų ir dviejų mergaičių, šeimos tėvas“.

310 Bendrojo duomenų apsaugos reglamento 39 konstatuojamoji dalis ir 5 straipsnio 1 dalies f punktas; atnaujintos 108-osios konvencijos 7 straipsnis.

311 Bendrojo duomenų apsaugos reglamento 32 straipsnio 1 punktas.

312 *Ten pat*.

Naudotojai, turintys prieigą prie duomenų, kuriems suteikti pseudonimai, paprastai negalės atpažinti „Charles Spencer, gimęs 1967 m. balandžio 3 d.“ pagal „324“ arba „YESz3201“. Todėl labiau tikėtina, kad tokie duomenys bus apsaugoti nuo netinkamo naudojimo.

Tačiau pirmasis pavyzdys nėra itin saugus. Jeigu sakinys „C. S. 1967 yra keturių vaikų (dviejų berniukų ir dviejų mergaičių) tėvas“ bus naudojamas mažame kaimelyje, kuriame gyvena Charles Spencer, jį būtų galima lengvai atpažinti. Pseudonimų suteikimo metodas gali turėti įtakos duomenų apsaugos veiksmingumui.

Asmens duomenys, kurių požymiai užšifruoti arba laikomi atskirai, naudojami įvairiomis aplinkybėmis kaip priemonė, padedanti išlaikyti asmenų tapatybės slaptumą. Tai ypač naudinga tais atvejais, kai duomenų valdytojai turi užtikrinti, kad būtų tvarkomi tų pačių duomenų subjektų duomenys, tačiau jiems nereikia ir jie neprivalo žinoti tikrosios duomenų subjektų tapatybės. Taip yra, pavyzdžiui, tuo atveju, kai tyrėjas tiria pacientų, kurių tapatybė žinoma tik ligoninės personalui, o ligoninė tyrėjui pateikė pseudonimines ligų istorijas, ligos eigą. Todėl pseudonimų suteikimas yra svarbi priemonė, susijusi su didesnę privatumo apsaugą padedančia užtikrinti technologija. Ji gali būti naudojama kaip svarbus elementas įgyvendinant pritaikytąją privatumo apsaugą. Tai reiškia, kad duomenų tvarkymo sistemų struktūroje turi būti užtikrinta duomenų apsauga.

BDAR 25 straipsnyje, kuriame aptariami pritaikytosios duomenų apsaugos klausimai, aiškiai nurodoma, kad pseudonimų suteikimas yra pavyzdinė tinkama techninė ir organizacinė priemonė, kurią duomenų valdytojai turėtų įgyvendinti, kad prisitaikytų prie duomenų apsaugos principų ir nustatytų būtinas apsaugos priemones. Tai darydami, duomenų valdytojai turi laikytis reglamento reikalavimų ir apsaugoti duomenų subjektų teises, kai tvarkomi jų asmens duomenys.

Patvirtinto elgesio kodekso arba sertifikavimo mechanizmo laikymasis gali padėti įrodyti, kad laikomasi saugaus duomenų tvarkymo reikalavimo[313]. Savo nuomonėje dėl duomenų apsaugos poveikio keleivio duomenų įrašų tvarkymui Europos Taryba pateikia kitų pavyzdinių tinkamų saugumo priemonių, padedančių apsaugoti asmens duomenis keleivio duomenų įrašų sistemose. Tai apima duomenų laikymą saugioje

313 *Ten pat*, 32 straipsnio 3 dalis.

fizinėje aplinkoje, prieigos kontrolės naudojant kelių lygmenų prisijungimą ribojimą ir duomenų perdavimo naudojant griežtą kriptografiją apsaugą[314].

Pavyzdys. Socialinių tinklų svetainių ir e. pašto paslaugų teikėjai sudaro sąlygas naudotojams įterpti papildomą duomenų saugumo naudojantis jų paslaugomis lygmenį, kuris apima dviejų etapų tapatumo nustatymą. Naudotojai ne tik įveda asmeninį slaptažodį, bet ir dar kartą privalo prisijungti prie savo asmeninės paskyros. Tai, pavyzdžiui, galėtų būti saugumo kodo, siunčiamo mobiliuoju numeriu, susieto su asmenine paskyra, įvedimas. Taip dviejų etapų patikrinimas padeda užtikrinti geresnę asmens duomenų apsaugą nuo neteisėtos prieigos prie asmeninių paskyrų į jas įsilaužiant.

Atnaujintos 108-osios konvencijos aiškinamojoje ataskaitoje pateikiami papildomi tinkamų apsaugos priemonių pavyzdžiai, pavyzdžiui, prievolės saugoti profesinę paslaptį įgyvendinimas arba kvalifikuotų techninių saugumo priemonių, pavyzdžiui, duomenų šifravimo, įgyvendinimas[315]. Nustatydamas konkrečias saugumo priemones, duomenų valdytojas arba, kai taikytina, duomenų tvarkytojas turėtų atsižvelgti į keletą aspektų, pavyzdžiui, į tvarkomų asmens duomenų pobūdį ir kiekį, galimas neigiamas pasekmes duomenų subjektams ir poreikį riboti galimybę susipažinti su duomenimis[316]. Įgyvendinant tinkamas saugumo priemones būtina atsižvelgti į naujausius duomenų saugumo metodus ir duomenų tvarkymo būdus. Tokių priemonių sąnaudos turi būti proporcingos galimos rizikos rimtumui ir tikimybei. Saugumo priemones reikia reguliariai peržiūrėti, kad prireikus jas būtų galima atnaujinti[317].

Jeigu padaromas asmens duomenų saugumo pažeidimas, pagal atnaujintą 108-ąją konvenciją ir BDAR reikalaujama, kad duomenų valdytojas nepagrįstai nedelsdamas praneštų kompetentingai priežiūros institucijai apie pažeidimą, įskaitant riziką, kuri gali kilti asmenų teisėms ir laisvėms[318]. Panaši prievolė pranešti duomenų subjektui galioja tuomet, kai tikėtina, kad asmens duomenų saugumo pažeidimas sukels didelę riziką jo teisėms ir laisvėms[319]. Duomenų subjektams apie tokius pažeidi-

314 Europos Taryba, 108-osios konvencijos komitetas, *Nuomonė dėl duomenų apsaugos poveikio keleivio duomenų įrašų tvarkymui*, T-PD(2016)18rev, 2016 m. rugpjūčio 19 d., p. 9.

315 Atnaujintos 108-osios konvencijos aiškinamosios ataskaitos 56 punktas.

316 *Ten pat*, 62 punktas.

317 *Ten pat*, 63 punktas.

318 Atnaujintos 108-osios konvencijos 7 straipsnio 2 dalis; Bendrojo duomenų apsaugos reglamento 33 straipsnio 1 dalis.

319 Atnaujintos 108-osios konvencijos 7 straipsnio 2 dalis; Bendrojo duomenų apsaugos reglamento 34 straipsnio 1 dalis.

mus turi būti pranešama aiškia ir paprasta kalba[320]. Jeigu duomenų tvarkytojas sužino apie duomenų saugumo pažeidimą, duomenų valdytoją apie tai privaloma nedelsiant informuoti[321]. Tam tikrose situacijose gali būti taikomos prievolės pranešti išimtys. Pavyzdžiui, nereikalaujama, kad duomenų valdytojas informuotų priežiūros instituciją, kai „asmens duomenų saugumo pažeidimas neturėtų kelti pavojaus fizinių asmenų teisėms ir laisvėms“[322]. Duomenų subjekto taip pat nebūtina informuoti, kai dėl įgyvendintų saugumo priemonių duomenys tampa nesuprantami asmeniui, neturinčiam leidimo su jais susipažinti, arba kai vėlesnėmis priemonėmis užtikrinama, kad nebekils didelė rizika[323]. Jeigu duomenų subjektams informuoti apie asmens duomenų saugumo pažeidimą reikėtų neproporcingų duomenų valdytojo pastangų, galima pasinaudoti viešo informavimo arba panašia priemone, kad „duomenų subjektai būtų informuojami taip pat efektyviai“[324].

3.7. Atskaitomybės principas

Pagrindiniai faktai

- Pagal atskaitomybės principą reikalaujama, kad duomenų valdytojai ir duomenų tvarkytojai, vykdydami duomenų tvarkymo veiklą, aktyviai ir nuolat įgyvendintų priemones, padedančias skatinti ir užtikrinti duomenų apsaugą.
- Duomenų valdytojai ir duomenų tvarkytojai privalo užtikrinti, kad jų duomenų tvarkymo operacijos atitiktų duomenų apsaugos teisę ir jiems taikomas atitinkamas prievoles.
- Duomenų valdytojai privalo sugebėti bet kuriuo metu įrodyti duomenų subjektams, plačiajai visuomenei ir priežiūros institucijoms, kad jie laikosi duomenų apsaugos nuostatų. Duomenų valdytojai taip pat privalo laikytis tam tikrų prievolių, kurios yra griežtai susijusios su atskaitomybe (pavyzdžiui, vesti duomenų tvarkymo operacijų registrą ir paskirti duomenų apsaugos pareigūną).

BDAR ir atnaujintoje 108-ojoje konvencijoje nustatyta, kad duomenų valdytojas atsako už šiame skyriuje aprašytų duomenų tvarkymo principų laikymąsi ir privalo sugebėti įrodyti, kad jis tokių principų laikosi[325]. Norėdamas pasiekti šį tikslą,

320 Bendrojo duomenų apsaugos reglamento 34 straipsnio 2 dalis.

321 *Ten pat*, 33 straipsnio 1 punktas.

322 *Ten pat*.

323 *Ten pat*, 34 straipsnio 3 dalies a ir b punktai.

324 *Ten pat*, 34 straipsnio 3 dalies c punktas.

325 *Ten pat*, 5 straipsnio 2 dalis; atnaujintos 108-osios konvencijos 10 straipsnio 1 dalis.

duomenų valdytojas privalo įgyvendinti tinkamas technines ir organizacines priemones[326]. Nepaisant to, kad BDAR 5 straipsnio 2 dalyje nustatytas atskaitomybės principas yra adresuotas tik duomenų valdytojams, taip pat tikimasi, kad atskaitingi bus ir duomenų tvarkytojai, nes jie privalo laikytis tam tikrų prievolių ir yra glaudžiai susiję su atskaitomybe.

ES ir ET duomenų apsaugos teisės aktuose taip pat nustatyta, kad duomenų valdytojai atsako už 3.1–3.6 skirsniuose aptartų duomenų apsaugos principų laikymąsi ir turėtų sugebėti užtikrinti jų laikymąsi[327]. 29 straipsnio darbo grupė atkreipia dėmesį į tai, kad „procedūrų ir mechanizmų rūšys skirtųsi priklausomai nuo duomenų tvarkymo keliamos rizikos ir jų pobūdžio“[328].

Duomenų valdytojai gali įvairiais būdais palengvinti šio reikalavimo laikymąsi, įskaitant:

- duomenų tvarkymo veiklos įrašymą ir įrašo pateikimą priežiūros institucijai paprašius[329];
- duomenų apsaugos pareigūno, kuris dalyvautų sprendžiant visus su asmens duomenų apsauga susijusius klausimus, paskyrimą tam tikrais atvejais[330];
- poveikio asmens duomenų apsaugai vertinimo atlikimą atsižvelgiant į duomenų tvarkymą, dėl kurio gali kilti didelė rizika fizinių asmenų teisėms ir laisvėms[331];
- pritaikytosios ir standartizuotosios duomenų apsaugos užtikrinimą[332];
- duomenų subjektų naudojimosi teisėmis sąlygų ir procedūrų įgyvendinimą[333];
- patvirtintų elgesio kodeksų arba sertifikavimo mechanizmų laikymąsi[334].

326 Bendrojo duomenų apsaugos reglamento 24 straipsnis.

327 *Ten pat*, 5 straipsnio 2 dalis; atnaujintos 108-osios konvencijos 10 straipsnio 1 dalis.

328 29 straipsnio darbo grupė, *Nuomonė Nr. 3/2010 dėl atskaitomybės principo*, WP 173, Briuselis, 2010 m. liepos 13 d., 12 punktas.

329 Bendrojo duomenų apsaugos reglamento 30 straipsnis.

330 *Ten pat*, 37–39 straipsniai.

331 *Ten pat*, 35 straipsnis; atnaujintos 108-osios konvencijos 10 straipsnio 2 dalis.

332 Bendrojo duomenų apsaugos reglamento 25 straipsnis; atnaujintos 108-osios konvencijos 10 straipsnio 2 ir 3 dalys.

333 *Ten pat*, 12 ir 24 straipsniai.

334 *Ten pat*, 40 ir 42 straipsniai.

Nors BDAR 5 straipsnio 2 dalyje nustatytas atskaitomybės principas nėra skirtas būtent duomenų tvarkytojams, reglamente yra su atskaitomybe susijusių nuostatų, kuriose jiems taip pat nustatytos prievolės, pavyzdžiui, duomenų tvarkymo veiklos įrašo laikymas ir duomenų apsaugos pareigūno paskyrimas bet kuriai duomenų tvarkymo veiklai, kuriai toks pareigūnas reikalingas[335]. Duomenų tvarkytojai taip pat privalo užtikrinti, kad būtų įgyvendintos visos saugiam duomenų tvarkymui užtikrinti būtinos priemonės[336]. Teisiškai privalomoje duomenų valdytojo ir duomenų tvarkytojo sutartyje būtina nustatyti, kad duomenų tvarkytojas padeda duomenų valdytojui laikytis tam tikrų reikalavimų, pavyzdžiui, atliekant poveikio duomenų apsaugai vertinimą arba pranešant duomenų valdytojui apie bet kokį asmens duomenų saugumo pažeidimą iš karto, kai tik apie tai sužino[337].

Ekonominio bendradarbiavimo ir plėtros organizacija (EBPO) 2013 m. priėmė privatumo gaires, kuriose atkreipė dėmesį į tai, kad duomenų valdytojai atlieka svarbų vaidmenį užtikrindami praktinę duomenų apsaugą. Gairėse nustatytas atskaitomybės principas, pagal kurį „duomenų valdytojas turėtų būti atskaitingas už priemonių, kuriomis įgyvendinami pirmiau nurodyti [esminiai] principai, laikymąsi“[338].

Pavyzdys. Teisėkūros pavyzdys, kuriame pabrėžiama atskaitomybės principo svarba, yra 2009 m. E. privatumo direktyvos 2002/58/EB pakeitimai[339]. Pagal jos iš dalies pakeistą 4 straipsnį direktyva įpareigojama „užtikrin[ti], kad būtų įgyvendinama saugumo politika asmens duomenų tvarkymo srityje“. Todėl kalbant apie šios direktyvos saugumo nuostatas pažymėtina, kad teisės aktų leidėjas nusprendė, jog būtina įtvirtinti aiškų reikalavimą nustatyti ir įgyvendinti saugumo politiką.

Kaip nurodyta 29 straipsnio darbo grupės nuomonėje[340], atskaitomybės principo esmę sudaro tai, kad duomenų valdytojas privalo:

335 *Ten pat*, 5 straipsnio 2 dalis, 30 ir 37 straipsniai.

336 *Ten pat*, 28 straipsnio 3 dalies c punktas.

337 *Ten pat*, 28 straipsnio 3 dalies d punktas.

338 EBPO (2013 m.), *Privatumo apsaugos ir tarpvalstybinių asmens duomenų judėjimo apsaugos gairių* 14 straipsnis.

339 2009 m. lapkričio 25 d. Europos Parlamento ir Tarybos direktyva 2009/136/EB, iš dalies keičianti Direktyvą 2002/22/EB dėl universaliųjų paslaugų ir paslaugų gavėjų teisių, susijusių su elektroninių ryšių tinklais ir paslaugomis, Direktyvą 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje ir Reglamentą (EB) Nr. 2006/2004 dėl nacionalinių institucijų, atsakingų už vartotojų apsaugos teisės aktų vykdymą, bendradarbiavimo, OL L 337, 2009, p. 11.

340 29 straipsnio darbo grupė, *Nuomonė Nr. 3/2010 dėl atskaitomybės principo*, WP 173, Briuselis, 2010 m. liepos 13 d.

- nustatyti priemones, kurios įprastomis aplinkybėmis padėtų garantuoti, kad vykdant duomenų tvarkymo operacijas būtų laikomasi duomenų apsaugos taisyklių, ir

- turėti prieinamus dokumentus, iš kurių duomenų subjektai ir priežiūros institucijos galėtų matyti priemones, kurių buvo imtasi siekiant užtikrinti atitiktį duomenų apsaugos taisyklėms.

Todėl pagal atskaitomybės principą reikalaujama, kad duomenų valdytojai aktyviai demonstruotų taisyklių laikymąsi, o ne tik lauktų, kol duomenų subjektai arba priežiūros institucijos informuos apie trūkumus.

4

Europos duomenų apsaugos teisės taisyklės

ES	Reglamentuojami klausimai	ET
Teisėto duomenų tvarkymo taisyklės		
Bendrojo duomenų apsaugos reglamento 6 straipsnio 1 dalies a punktas ESTT, C-543/09, *Deutsche Telekom AG prieš Bundesrepublik Deutschland*, 2011 m. ESTT, C-536/15, *Tele2 (Netherlands) BV ir kt. prieš Autoriteit Consument en Markt (AMC)*, 2017 m.	**Sutikimas**	Rekomendacijos dėl profiliavimo 3.4 straipsnio b punktas ir 3.6 straipsnis Atnaujintos 108-osios konvencijos 5 straipsnio 2 dalis
Bendrojo duomenų apsaugos reglamento 6 straipsnio 1 dalies b punktas	**(Iki)sutartiniai santykiai**	Rekomendacijos dėl profiliavimo 3.4 straipsnio b punktas
Bendrojo duomenų apsaugos reglamento 6 straipsnio 1 dalies c punktas	**Duomenų valdytojo teisinės pareigos**	Rekomendacijos dėl profiliavimo 3.4 straipsnio a punktas
Bendrojo duomenų apsaugos reglamento 6 straipsnio 1 dalies d punktas	**Duomenų subjekto gyvybiniai interesai**	Rekomendacijos dėl profiliavimo 3.4 straipsnio b punktas
Bendrojo duomenų apsaugos reglamento 6 straipsnio 1 dalies e punktas ESTT, C-524/06, *Huber prieš Bundesrepublik Deutschland* (DK), 2008 m.	**Viešasis interesas ir oficialių įgaliojimų vykdymas**	Rekomendacijos dėl profiliavimo 3.4 straipsnio b punktas

ES	Reglamentuojami klausimai	ET
Bendrojo duomenų apsaugos reglamento 6 straipsnio 1 dalies f punktas ESTT, C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde prieš Rīgas pašvaldības SIA „Rīgas satiksme“*, 2017 m. ESTT, sujungtos bylos C-468/10 ir C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) ir Federación de Comercio Electrónico y Marketing Directo (FECEMD) prieš Administración del Estado*, 2011 m.	**Teisėti kitų asmenų interesai**	Rekomendacijos dėl profiliavimo 3.4 straipsnio b punktas EŽTT, *Y prieš Turkiją*, Nr. 648/10, 2015 m.
Bendrojo duomenų apsaugos reglamento 6 straipsnio 4 dalis	**Tikslų apribojimo išimtis: tolesnis duomenų tvarkymas kitais tikslais**	Atnaujintos 108-osios konvencijos 5 straipsnio 4 dalies b punktas
Teisėto neskelbtinų duomenų tvarkymo taisyklės		
Bendrojo duomenų apsaugos reglamento 9 straipsnio 1 dalis	**Bendras draudimas tvarkyti duomenis**	Atnaujintos 108-osios konvencijos 6 straipsnis
Bendrojo duomenų apsaugos reglamento 9 straipsnio 2 dalis	**Bendro draudimo išimtys**	Atnaujintos 108-osios konvencijos 6 straipsnis
Saugaus duomenų tvarkymo taisyklės		
Bendrojo duomenų apsaugos reglamento 32 straipsnis	**Prievolė užtikrinti saugų duomenų tvarkymą**	Atnaujintos 108-osios konvencijos 7 straipsnio 1 dalis EŽTT, *I prieš Suomiją*, Nr. 20511/03, 2008 m.
Bendrojo duomenų apsaugos reglamento 28 straipsnis ir 32 straipsnio 1 dalies b punktas	**Prievolė laikytis konfidencialumo principo**	Atnaujintos 108-osios konvencijos 7 straipsnio 1 dalis
Bendrojo duomenų apsaugos reglamento 34 straipsnis Direktyvos dėl privatumo ir elektroninių ryšių 4 straipsnio 2 punktas	**Pranešimai apie duomenų saugumo pažeidimus**	Atnaujintos 108-osios konvencijos 7 straipsnio 2 dalis
Atskaitomybės taisyklės ir reikalavimų laikymosi skatinimas		
Bendrojo duomenų apsaugos reglamento 12, 13 ir 14 straipsniai	**Bendrosios nuostatos dėl skaidrumo**	Atnaujintos 108-osios konvencijos 8 straipsnis
Bendrojo duomenų apsaugos reglamento 37, 38 ir 39 straipsniai	**Duomenų apsaugos pareigūnai**	Atnaujintos 108-osios konvencijos 10 straipsnio 1 dalis

ES	Reglamentuojami klausimai	ET
Bendrojo duomenų apsaugos reglamento 30 straipsnis	Duomenų tvarkymo veiklos įrašai	
Bendrojo duomenų apsaugos reglamento 35 ir 36 straipsniai	Poveikio vertinimas ir išankstinės konsultacijos	Atnaujintos 108-osios konvencijos 10 straipsnio 2 dalis
Bendrojo duomenų apsaugos reglamento 33 ir 34 straipsniai	Pranešimai apie duomenų saugumo pažeidimus	Atnaujintos 108-osios konvencijos 7 straipsnio 2 dalis
Bendrojo duomenų apsaugos reglamento 40 ir 41 straipsniai	Elgesio kodeksai	
Bendrojo duomenų apsaugos reglamento 42 ir 43 straipsniai	Sertifikavimas	
Pritaikytoji ir standartizuotoji duomenų apsauga		
Bendrojo duomenų apsaugos reglamento 25 straipsnio 1 dalis	Pritaikytoji duomenų apsauga	Atnaujintos 108-osios konvencijos 10 straipsnio 2 dalis
Bendrojo duomenų apsaugos reglamento 25 straipsnio 2 dalis	Standartizuotoji duomenų apsauga	Atnaujintos 108-osios konvencijos 10 straipsnio 3 dalis

Principai iš esmės yra bendro pobūdžio. Juos taikant konkrečiose situacijose paliekama tam tikra laisvė savo nuožiūra juos aiškinti ir pasirinkti priemones. Pagal **ET teisę** atnaujintos 108-osios konvencijos šalims paliekama teisė savo nacionalinės teisės aktuose patikslinti šią aiškinimo laisvę. Padėtis pagal **ES teisę** yra kitokia: siekiant sukurti duomenų apsaugą nacionalinėje teisėje, buvo manoma, kad yra būtina ES lygmeniu nustatyti išsamesnes taisykles, siekiant suderinti valstybių narių nacionaliniuose įstatymuose nustatytą duomenų apsaugos lygį. Bendrajame duomenų apsaugos reglamente, remiantis jo 5 straipsnyje išdėstytais principais, kurie tiesiogiai taikomi pagal nacionalinę teisinę tvarką, nustatytas išsamių taisyklių lygmuo. Todėl toliau pateiktos pastabos dėl išsamių duomenų apsaugos taisyklių Europos lygmeniu iš esmės yra susijusios su ES teise.

4.1. Teisėto duomenų tvarkymo taisyklės

Pagrindiniai faktai

- Asmens duomenys gali būti teisėtai tvarkomi, jeigu jie atitinka vieną iš toliau nurodytų kriterijų:
  - duomenų tvarkymas yra pagrįstas duomenų subjekto sutikimu;
  - asmens duomenis reikalaujama tvarkyti pagal sutartinius santykius;
  - duomenis tvarkyti būtina siekiant įvykdyti duomenų valdytojo teisinę prievolę;
  - duomenis tvarkyti būtina dėl duomenų subjektų ar kito asmens gyvybinių interesų;
  - tvarkyti duomenis reikia siekiant atlikti užduotį, vykdomą viešojo intereso labui;
  - duomenys tvarkomi atsižvelgiant į teisėtus duomenų valdytojų arba trečiųjų šalių interesus, tačiau tik tiek, kiek už juos nėra viršesni duomenų subjektų interesai arba pagrindinės teisės.
- Teisėtam neskelbtinų asmens duomenų tvarkymui taikoma speciali, griežtesnė tvarka.

4.1.1. Teisėti duomenų tvarkymo pagrindai

Bendrojo duomenų apsaugos reglamento II skyriuje „Principai“ nustatyta, kad visa asmens duomenų tvarkymo veikla pirmiausia privalo atitikti BDAR 5 straipsnyje nustatytus duomenų kokybės principus. Pagal vieną iš principų asmens duomenys turėtų būti „tvarkomi teisėtu, sąžiningu ir skaidriu būdu“. Antra, tam, kad duomenys būtų tvarkomi teisėtai, duomenų tvarkymas privalo atitikti vieną iš teisėtų pagrindų, išvardytų 6 straipsnyje[341], jei tvarkomi įprasti asmens duomenys, ir 9 straipsnyje, jei tvarkomos specialios duomenų kategorijos (arba neskelbtini duomenys), dėl kurių duomenų tvarkymas tampa teisėtas. Panašiai atnaujintos 108-osios konvencijos II skyriuje, kuriame įtvirtinti „pagrindiniai asmens duomenų apsaugos principai“, nustatyta, kad tam, jog duomenys būtų tvarkomi teisėtai, toks tvarkymas turi būti „proporcingas atsižvelgiant į teisėtą siekiamą tikslą“.

341 ESTT, sujungtos bylos C-465/00, C-138/01 ir C-139/01, *Rechnungshof prieš Österreichischer Rundfunk ir kt.* ir *Christa Neukomm and Jospeh Lauermann prieš Österreichischer Rundfunk*, 20003 m. gegužės 20 d., 65 punktas; ESTT, C-524/06, *Heinz Huber prieš Bundesrepublik Deutschland* (DK), 2008 m. gruodžio 16 d., 48 punktas; ESTT, sujungtos bylos C-468/10 ir C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) ir Federación de Comercio Electrónico y Marketing Directo (FECEMD) prieš Administración del Estado*, 2011 m. lapkričio 24 d., 26 punktas.

Nepaisant teisėto duomenų tvarkymo tikslo, kuriuo duomenų valdytojas remiasi pradėdamas asmens duomenų tvarkymo operaciją, duomenų valdytojas taip pat turės taikyti bendrosiose duomenų apsaugos teisės taisyklėse nustatytas apsaugos priemones.

Sutikimas

ET teisėje sutikimas minimas atnaujintos 108-osios konvencijos 5 straipsnio 2 dalyje. Apie jį taip pat užsimenama EŽTT praktikoje ir keliose ET rekomendacijose[342]. **Pagal ES teisę** sutikimas, kaip teisėto duomenų tvarkymo pagrindas, yra tvirtai nustatytas BDAR 6 straipsnyje ir aiškiai nurodytas Chartijos 8 straipsnyje. Galiojančio sutikimo ypatumai paaiškinti 4 straipsnyje pateiktoje sutikimo apibrėžtyje, o galiojančio sutikimo gavimo sąlygos išsamiai išdėstytos 7 straipsnyje, be to, specialios vaiko sutikimo taisyklės, susijusios su informacinės visuomenės paslaugomis, nustatytos BDAR 8 straipsnyje.

Kaip paaiškinta 2.4 skirsnyje, sutikimas turi būti duotas laisva valia, pagrįstas informacija, konkretus ir nedviprasmiškas. Sutikimas turi būti pareiškimas arba aiškus patvirtinamasis veiksmas, reiškiantis sutikimą tvarkyti duomenis, be to, asmuo turi teisę bet kuriuo metu atšaukti savo sutikimą. Duomenų valdytojų pareiga – saugoti patikrinamą sutikimo įrašą, kurį būtų galima patikrinti.

Laisvas sutikimas

Pagal atnaujintoje 108-ojoje konvencijoje nustatytą **ET** sistemą duomenų subjekto sutikimas turi būti „laisva sąmoningo pasirinkimo išraiška“[343]. Laisvas sutikimas galioja, tik „jei duomenų subjektas gali iš tikrųjų pasirinkti, o jei jis nesutinka, nėra apgaulės, bauginimo, prievartos ar reikšmingų neigiamų pasekmių pavojaus“[344]. Šiuo atžvilgiu pagal **ES teisę** nelaikoma, kad sutikimas buvo duotas laisva valia, „jei duomenų subjektas faktiškai neturi laisvo pasirinkimo ar negali atsisakyti sutikti arba sutikimo atšaukti, nepatirdamas žalos“[345]. BDAR pažymima, kad „[v]ertinant, ar sutikimas duotas laisva valia, labiausiai atsižvelgiama į tai, ar, *inter alia*, sutarties

342 Žr., pavyzdžiui, Europos Taryba, Ministrų Komitetas (2010 m.), 2010 m. lapkričio 23 d. Ministrų Komiteto rekomendacija *CM/Rec(2010)13* valstybėms narėms dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu profiliavimo kontekste, 3 straipsnio 4 dalies b punktas.

343 Atnaujintos 108-osios konvencijos aiškinamosios ataskaitos 42 punktas.

344 Taip pat žr. 29 straipsnio darbo grupės (2011 m.) *Nuomonės 15/2011 dėl sutikimo sąvokos*, WP 187, Briuselis, 2011 m. liepos 13 d., p. 12.

345 Bendrojo duomenų apsaugos reglamento 42 konstatuojamoji dalis.

vykdymui, įskaitant paslaugos teikimą, yra nustatyta sąlyga, kad turi būti duotas sutikimas tvarkyti asmens duomenis, kurie nėra būtini tai sutarčiai vykdyti“[346]. Atnaujintos 108-osios konvencijos aiškinamojoje ataskaitoje nustatyta, kad „[d]uomenų subjektui negali būti daroma nederama tiesioginė ar netiesioginė įtaka ar spaudimas (kuris gali būti ekonominio ar kitokio pobūdžio), taip pat sutikimas neturėtų būti laikomas duotu laisva valia, kai duomenų subjektas neturi tikro pasirinkimo arba negali atsisakyti duoti sutikimą ar jį atšaukti nepatirdamas žalos“[347].

Pavyzdys. Tam tikros A valstybės savivaldybės nusprendė sukurti leidimo gyventi korteles su integruotu lustu. Gyventojai neprivalo įsigyti šių elektroninių kortelių. Tačiau kortelės neturintys gyventojai negali naudotis įvairiomis svarbiomis administracinėmis paslaugomis, pavyzdžiui, neturi galimybės sumokėti internetu savivaldybės mokesčius, pateikti skundus elektroniniu būdu per trijų dienų terminą, per kurį valdžios institucija privalo atsakyti, ir net išvengti eilių, įsigyti pigesnių bilietų lankydamiesi savivaldybės koncertų salėje ir naudotis prie įėjimo įrengtais skeneriais.

Šiame pavyzdyje savivaldybės asmens duomenų negali tvarkyti remdamosi sutikimu. Kadangi gyventojams daromas bent jau netiesioginis spaudimas gauti elektroninę kortelę ir sutikti su duomenų tvarkymu, sutikimas neduodamas laisva valia. Todėl savivaldybių elektroninių kortelių sistemos kūrimas turėtų būti grindžiamas kitu teisėtu pagrindu, pateisinančiu duomenų tvarkymą. Pavyzdžiui, savivaldybės galėtų remtis tuo, kad duomenis tvarkyti būtina siekiant atlikti užduotį, vykdomą viešojo intereso labui, nes tai yra teisėtas duomenų tvarkymo pagrindas pagal BDAR 6 straipsnio 1 dalies e punktą[348].

Dėl sutikimo laisva valia taip pat gali kilti abejonių subordinacijos atvejais, kai tarp duomenų valdytojo, kuris užtikrina sutikimo gavimą, ir sutikimą duodančio duomenų

346 *Ten pat*, 7 straipsnio 4 punktas.

347 Atnaujintos 108-osios konvencijos aiškinamosios ataskaitos 42 punktas.

348 29 straipsnio darbo grupė (2011 m.), *Nuomonė 15/2011 dėl sąvokos „sutikimas“ apibrėžties*, WP 187, Briuselis, 2011 m. liepos 13 d., p. 16. Daugiau atvejų, kai duomenų tvarkymas negali būti grindžiamas sutikimu, bet tam reikia kitokio teisinio pagrindo duomenų tvarkymui įteisinti, pavyzdžių pateikta nuomonės p. 14 ir 17.

subjekto yra didelė ekonominės arba kitokios galios neatitiktis[349]. Tipinis tokios neatitikties ir subordinacijos pavyzdys yra darbdavio vykdomas asmens duomenų tvarkymas atsižvelgiant į darbo santykius. Pasak 29 straipsnio darbo grupės, „[d] arbuotojai dėl savo priklausomumo, kurį lemia darbdavio ir darbuotojo santykiai, beveik niekada negali laisva valia duoti sutikimo, atsisakyti duoti arba atšaukti sutikimą. Atsižvelgiant į galios neatitiktį, darbuotojai gali duoti laisvą sutikimą tik išimtinėmis aplinkybėmis, kai nėra jokių pasekmių, susijusių su pasiūlymo priėmimu ar atmetimu“[350].

Pavyzdys. Didelė įmonė, siekdama paprasčiausiai užtikrinti geresnę vidaus komunikaciją, planuoja sukurti katalogą, kuriame būtų įrašyti visų darbuotojų vardai ir pavardės, jų einamos pareigos ir veiklos adresai. Personalo vadovas siūlo į katalogą įdėti kiekvieno darbuotojo nuotrauką, kad per susitikimus bendradarbiai galėtų lengviau vieni kitus atpažinti. Darbuotojų atstovai teigia, kad tai turėtų būti daroma tik gavus kiekvieno darbuotojo sutikimą.

Tokiu atveju darbuotojo sutikimas turėtų būti pripažintas teisiniu pagrindu tvarkant nuotraukas kataloge, nes tikėtina, kad darbuotojas apskritai nepatirs jokių pasekmių, nesvarbu, ar jis sutiks, ar nesutiks, kad jo nuotrauka būtų paskelbta kataloge.

Pavyzdys. Įmonė A planuoja surengti trijų savo darbuotojų ir įmonės B direktorių susitikimą, kad aptartų galimą bendradarbiavimą dėl projekto. Posėdis vyks įmonės B patalpose, todėl įmonė A turi e. paštu nusiųsti jai susitikimo dalyvių vardus, pavardes, gyvenimo aprašymus ir nuotraukas. Įmonė B teigia, kad jai reikalingi dalyvių vardai, pavardės ir nuotraukos, kad apsaugos darbuotojai prie įėjimo į pastatą galėtų patikrinti, ar jie yra tinkami asmenys, o gyvenimo aprašymai leis direktoriams geriau pasirengti posėdžiui. Šiuo atveju įmonės A atliekamo jos darbuotojų asmens duomenų perdavimo negalima grįsti sutikimu. Sutikimo negalima laikyti duotu „laisva valia“, nes darbuotojai gali susidurti su neigiamomis pasekmėmis, jei atmestų pasiūlymą (pavyzdžiui, juos gali pakeisti kiti bendradarbiai, kurie dalyvautų ne

349 Taip pat žr. 29 straipsnio darbo grupės (2001 m.) *Nuomonę Nr. 8/2001 dėl asmens duomenų tvarkymo užimtumo srityje*, WP 48, Briuselis, 2001 m. rugsėjo 13 d.; 29 straipsnio darbo grupės (2005 m.) *Darbinį dokumentą dėl 1995 m. spalio 24 d. Direktyvos 95/46/EB 26 straipsnio 1 dalies vienodo aiškinimo*, WP 114, Briuselis; 2005 m. lapkričio 25 d.; 29 straipsnio darbo grupės (2017 m.) *Nuomonę Nr. 2/2017 dėl duomenų tvarkymo darbe*, WP 249, Briuselis, 2017 m. birželio 8 d.

350 29 straipsnio darbo grupė, *Nuomonė Nr. 2/2017 dėl duomenų tvarkymo darbe*, WP 249, Briuselis, 2017 m. birželio 8 d.

tik posėdyje, bet ir palaikytų ryšius su įmone B ir apskritai prisidėtų prie projekto). Todėl duomenų tvarkymas turi būti grindžiamas kitu teisėtu duomenų tvarkymo pagrindu.

Vis dėlto tai nereiškia, kad sutikimas niekada negali galioti tais atvejais, kai nesutikimas turėtų neigiamų pasekmių. Pavyzdžiui, jei dėl sutikimo turėti prekybos centro kliento kortelę negaunama tik nedidelė tam tikrų prekių kainos nuolaida, sutikimas galėtų būti galiojantis teisinis pagrindas tvarkyti klientų, kurie sutiko, kad tokia kortelė būtų išduota, asmens duomenis. Įmonė ir klientas nėra subordinuoti, o sutikimo nedavimo pasekmės nėra pakankamai rimtos, kad duomenų subjektui būtų užkirstas kelias laisvai pasirinkti (su sąlyga, kad kainos sumažinimas yra pakankamai mažas, kad nebūtų daromas poveikis jo laisvam pasirinkimui).

Tačiau tais atvejais, kai prekes ar paslaugas galima gauti tik tuo atveju, jei tam tikri asmens duomenys atskleidžiami duomenų valdytojui arba trečiosioms šalims, duomenų subjekto sutikimas atskleisti savo duomenis, kurie nėra būtini sutarčiai sudaryti, negali būti laikomas laisvu sprendimu, todėl jis pagal duomenų apsaugos teisę negalioja[351]. BDAR gana griežtai draudžiama susieti sutikimą su prekių tiekimu ir paslaugų teikimu[352].

Pavyzdys. Keleivių sutikimas, kad oro linijos perduotų vadinamuosius keleivio duomenų įrašus (t. y. duomenis apie jų tapatybę, valgymo įpročius ar sveikatos sutrikimus) konkrečios užsienio šalies imigracijos institucijoms, negali būti laikomas galiojančiu sutikimu pagal duomenų apsaugos teisę, nes keliaujantys keleiviai neturi jokių galimybių pasirinkti, jeigu nori apsilankyti šioje šalyje. Norint tokius duomenis perduoti teisėtai, reikia kito teisinio pagrindo nei sutikimas, greičiausiai – konkretaus įstatymo.

Informuoto asmens sutikimas

Duomenų subjektas prieš priimdamas sprendimą privalo turėti pakankamai informacijos. Informuoto asmens sutikimas paprastai apima tikslų ir lengvai suprantamą dalyko, dėl kurio reikia duoti sutikimą, aprašymą. Kaip paaiškina 29 straipsnio darbo grupė, sutikimas turi būti pagrįstas faktinių aplinkybių ir pasekmių, kurios kils duomenų subjektui sutikus tvarkyti jo duomenis, įvertinimu ir supratimu. Todėl „[a] titinkamam asmeniui privaloma aiškiu ir suprantamu būdu pateikti tikslią ir išsamią

351 Bendrojo duomenų apsaugos reglamento 7 straipsnio 4 dalis.

352 *Ten pat*.

informaciją visais susijusiais klausimais, <...> pavyzdžiui, apie tvarkomų duomenų pobūdį, duomenų tvarkymo tikslus, galimus gavėjus ir duomenų subjekto teises“[353]. Tam, kad duotų informacija pagrįstą sutikimą, asmenys taip pat turi žinoti pasekmes, kurios atsiranda nedavus sutikimo tvarkyti duomenis.

Atsižvelgiant į informuoto asmens sutikimo svarbą, BDAR ir atnaujintos 108-osios konvencijos aiškinamojoje ataskaitoje buvo siekiama paaiškinti sąvoką. BDAR konstatuojamosiose dalyse nustatyta, kad informuoto asmens sutikimas reiškia, kad „duomenų subjektas turėtų bent žinoti duomenų valdytojo tapatybę ir planuojamo asmens duomenų tvarkymo tikslus“[354].

Išimtiniu atveju, kai sutikimas naudojamas kaip nukrypti leidžianti nuostata, ir siekiant užtikrinti teisėtą tarptautinių duomenų perdavimo pagrindą, duomenų valdytojas privalo informuoti duomenų subjektą apie galimus tokio perdavimo pavojus, galinčius kilti dėl to, kad nepriimtas sprendimas dėl tinkamumo ir nenustatytos tinkamos apsaugos priemonės[355].

Atnaujintos 108-osios konvencijos aiškinamojoje ataskaitoje nustatyta, kad būtina pateikti informaciją apie duomenų subjekto sprendimo pasekmes, būtent „ką reiškia sutikimo davimo faktas ir kokiu mastu duodamas sutikimas“[356].

Informacijos kokybė yra svarbi. Informacijos kokybė reiškia, kad informacijos kalba turėtų būti pritaikyta numatomiems jos gavėjams. Informacija turi būti pateikiama nevartojant žargono, aiškia ir paprasta kalba, kurią turėtų galėti suprasti nuolatinis naudotojas[357]. Informacija taip pat turi būti lengvai prieinama duomenų subjektui ir gali būti pateikta žodžiu arba raštu. Informacijos prieinamumas ir matomumas yra svarbūs elementai: informacija turi būti aiškiai matoma ir pastebima. Internetinėje aplinkoje tinkamas sprendimas gali būti kelių lygmenų informaciniai pranešimai, nes jie suteikia duomenų subjektams galimybę pasirinkti – gauti glaustos ar išsamesnės informacijos versijas.

353 29 straipsnio darbo grupė (2007 m.), *Darbinis dokumentas dėl asmens duomenų, susijusių su sveikata elektroniniuose sveikatos įrašuose (EHR), tvarkymo,* WP 131, Briuselis, 2007 m. vasario 15 d.

354 Bendrojo duomenų apsaugos reglamento 42 konstatuojamoji dalis.

355 *Ten pat*, 49 straipsnio 1 dalies a punktas.

356 Atnaujintos 108-osios konvencijos aiškinamosios ataskaitos 42 punktas.

357 29 straipsnio darbo grupė (2011 m.), *Nuomonė 15/2011 dėl sąvokos „sutikimas“ apibrėžties*, WP 187, Briuselis, 2011 m. liepos 13 d., p. 19.

Konkretus sutikimas

Kad sutikimas galiotų, jis taip pat turi būti susijęs su duomenų tvarkymo tikslu, kuris turi būti aiškiai ir nedviprasmiškai apibūdintas. Tai yra glaudžiai susiję su informacijos apie sutikimo tikslą kokybe. Šiomis aplinkybėmis svarbu atkreipti dėmesį į paprasto duomenų subjekto pagrįstus lūkesčius. Duomenų subjekto turi būti dar kartą paprašyta duoti sutikimą, jei duomenų tvarkymo operacijos turi būti papildytos arba pakeistos tokiu būdu, kurio nebuvo galima pagrįstai numatyti, kai buvo duotas pradinis sutikimas, ir dėl to turi būti pakeistas tikslas. Jeigu duomenys tvarkomi įvairiais tikslais, sutikimą reikėtų duoti dėl visų tikslų[358].

Pavyzdžiai. Byloje *Deutsche Telekom AG*[359] ESTT nagrinėjo, ar telekomunikacijų paslaugų teikėjas, kuris abonentų asmens duomenis turėjo perduoti, kad jie būtų paskelbti abonentų knygose, turėjo gauti naują duomenų subjektų sutikimą[360], nes sutikimo davimo metu gavėjai iš pradžių nebuvo įvardyti.

ESTT nusprendė, kad pagal Direktyvos dėl privatumo ir elektroninių ryšių 12 straipsnį prieš perduodant duomenis atnaujintas sutikimas nebuvo būtinas. Kadangi duomenų subjektai turėjo tik galimybę sutikti su duomenų tvarkymo tikslu, t. y. jų duomenų skelbimu, jie negalėjo pasirinkti iš skirtingų abonentų knygų, kuriose šie duomenys galėtų būti skelbiami.

ESTT pažymėjo, kad „[p]agal kontekstą ir sistemiškai aiškinant Privataus gyvenimo apsaugos elektroniniuose ryšiuose direktyvos 12 straipsnį matyti, <...> kad sutikimas pagal šio straipsnio 2 dalį duodamas skelbti asmens duomenis viešoje abonentų knygoje, o ne kad juos skelbtų konkretus abonentų knygų paslaugų teikėjas“[361]. Be to, „abonentui gali būti žalingas būtent asmens duomenų paskelbimas specifinės paskirties abonentų knygoje“[362], o ne paties leidėjo tapatybė.

358 Bendrojo duomenų apsaugos reglamento 32 konstatuojamoji dalis.

359 ESTT, C-543/09, *Deutsche Telekom AG prieš Bundesrepublik Deutschland*, 2011 m. gegužės 5 d. Visų pirma žr. 53 ir 54 punktus.

360 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje, OL L 201, 2002 (Direktyva dėl privatumo ir elektroninių ryšių).

361 ESTT, C-543/09, *Deutsche Telekom AG prieš Bundesrepublik Deutschland*, 2011 m. gegužės 5 d., 61 punktas.

362 *Ten pat*, 62 punktas.

Byla *Tele2 (Netherlands) BV, Ziggo BV, Vodafone Libertel BV prieš Autoriteit Consument en Markt (AMC)*[363] buvo susijusi su Belgijos įmonės prašymu, kad informacijos apie abonentus teikimo paslaugos ir abonentų knygos įmonėms, skiriančioms telefono numerius Nyderlanduose, suteiktų jai prieigą prie duomenų, susijusių su jų abonentais. Belgijos įmonė vykdė prievolę pagal Universaliųjų paslaugų direktyvą[364]. Todėl įmonės, skiriančios telefono numerius, turi suteikti galimybę naudotis numeriais jų prašantiems abonentų knygų leidėjams, jei abonentai sutinka, kad jų numeriai būtų skelbiami. Nyderlandų įmonės atsisakė tai padaryti, teigdamos, kad jos neprivalėjo pateikti atitinkamų duomenų kitoje valstybėje narėje įsteigtai įmonei. Pasak šių įmonių, naudotojai sutinka, kad jų numeriai būtų skelbiami, jei tai bus daroma Nyderlandų abonentų knygoje. ESTT nusprendė, kad Universaliųjų paslaugų direktyva taikoma visiems abonentų knygų paslaugas teikiančių įmonių prašymams, neatsižvelgiant į tai, kurioje valstybėje narėje jos yra įsisteigusios. ESTT taip pat nusprendė, kad tų pačių duomenų perdavimas kitai įmonei, kuri ketina skelbti viešą abonentų knygą negavusi atnaujinto abonentų sutikimo, negali iš esmės pakenkti teisei į asmens duomenų apsaugą[365]. Todėl nebūtina, kad įmonė, kuri priskiria telefono numerius savo abonentams, darytų skirtumą prašyme dėl sutikimo, skirtame abonentui, pagal valstybę narę, kuriai būtų galima siųsti su abonentu susijusius duomenis[366].

Vienareikšmis sutikimas

Bet koks sutikimas turi būti duotas nedviprasmiškai[367]. Tai reiškia, kad negali būti jokios pagrįstos abejonės, kad duomenų subjektas norėjo išreikšti savo sutikimą leisti tvarkyti jo duomenis. Pavyzdžiui, duomenų subjekto neveikimas nereiškia, kad jis duoda vienareikšmį sutikimą.

363 ESTT, C-536/15, *Tele2 (Netherlands) BV ir kt. prieš Autoriteit Consument en Markt (AMC)*, 2017 m. kovo 15 d.

364 2002 m. kovo 7 d. Europos Parlamento ir Tarybos direktyva 2002/22/EB dėl universaliųjų paslaugų ir paslaugų gavėjų teisių, susijusių su elektroninių ryšių tinklais ir paslaugomis (Universaliųjų paslaugų direktyva) (OL L 108, 2002, p. 15), iš dalies pakeista 2009 m. lapkričio 25 d. Europos Parlamento ir Tarybos direktyva 2009/136/EB (Universaliųjų paslaugų direktyva) (OL L 337, 2009, p. 11).

365 ESTT, C-536/15, *Tele2 (Netherlands) BV ir kt. prieš Autoriteit Consument en Markt (AMC)*, 2017 m. kovo 15 d., 36 punktas.

366 *Ten pat*, 40–41 punktai.

367 Bendrojo duomenų apsaugos reglamento 4 straipsnio 11 punktas.

Taip būtų tuo atveju, jeigu duomenų valdytojas gautų sutikimą kartu su jų privatumo apsaugos politikos pareiškimais, pavyzdžiui, „naudodamiesi mūsų paslauga, jūs sutinkate, kad būtų tvarkomi jūsų asmens duomenys“. Tokiu atveju duomenų valdytojams gali prireikti užtikrinti, kad naudotojai su tokia politika sutiktų rankiniu būdu ir individualiai.

Jeigu sutikimas duodamas raštu ir yra neatskiriama sutarties dalis, sutikimas tvarkyti asmens duomenis turi būti individualizuotas ir bet kuriuo atveju „apsaugos priemonėmis turėtų būti užtikrinta, kad duomenų subjektas suvoktų, kad jis duoda sutikimą ir dėl ko jis jį duoda“[368].

Vaikams taikomi sutikimo reikalavimai

BDAR nustatyta konkreti vaikų apsauga tais atvejais, kai teikiamos informacinės visuomenės paslaugos, nes „jie gali nepakankamai suvokti su asmens duomenų tvarkymu susijusius pavojus, pasekmes ar apsaugos priemones ir savo teises“[369]. Todėl pagal **ES teisę**, jeigu informacinės visuomenės paslaugų teikėjai tvarko jaunesnių nei 16 metų vaikų duomenis, remdamiesi sutikimu, toks duomenų tvarkymas bus teisėtas „tik tuo atveju, jeigu tą sutikimą davė arba tvarkyti duomenis leido tėvų pareigų turėtojas, ir tokiu mastu, kokiu duotas toks sutikimas ar leidimas“[370]. Valstybės narės nacionalinėje teisėje gali nustatyti mažesnį amžių, tačiau ne mažiau nei 13 metų[371]. Tėvų pareigų turėtojo sutikimo reikalaujama „tiesiogiai vaikui teikiant prevencijos ar konsultavimo paslaugas“[372]. Jeigu tvarkomi vaiko asmens duomenys, informaciją reikėtų perduoti ir bendrauti aiškia ir vaikui lengvai suprantama kalba[373].

Teisė bet kuriuo metu atšaukti sutikimą

BDAR numatyta bendro pobūdžio teisė bet kuriuo metu atšaukti sutikimą[374]. Duomenų subjektą būtina informuoti apie tokią teisę prieš jam duodant sutikimą ir jis šia teise gali pasinaudoti savo nuožiūra. Atšaukiant sutikimą neturėtų būti reikalaujama

368 *Ten pat*, 42 konstatuojamoji dalis.

369 *Ten pat*, 38 konstatuojamoji dalis.

370 *Ten pat*, 8 straipsnio 1 dalies pirma įtrauka. Informacinės visuomenės paslaugų sąvoka apibrėžta Bendrojo duomenų apsaugos reglamento 4 straipsnio 25 punkte.

371 Bendrojo duomenų apsaugos reglamento 8 straipsnio 1 dalies antra įtrauka.

372 *Ten pat*, 38 konstatuojamoji dalis.

373 *Ten pat*, 58 konstatuojamoji dalis. Taip pat žr. atnaujintos 108-osios konvencijos 15 straipsnio 2 dalies e punktą. Atnaujintos 108-osios konvencijos aiškinamosios ataskaitos 68 ir 125 punktai.

374 Bendrojo duomenų apsaugos reglamento 7 straipsnio 3 dalis. Atnaujintos 108-osios konvencijos aiškinamosios ataskaitos 45 punktas.

nurodyti priežastis ir dėl tokio atšaukimo neturėtų sumažėti bet kokia nauda, kurią duomenų subjektas gavo anksčiau davęs sutikimą naudoti duomenis. Atšaukti sutikimą turėtų būti taip pat paprasta, kaip ir jį duoti[375]. Laisvo sutikimo negali būti, jeigu duomenų subjektas negali atšaukti savo sutikimo nepatirdamas žalos arba jeigu atšaukti sutikimą nėra taip pat lengva, kaip jį duoti[376].

Pavyzdys. Klientas sutinka gauti reklaminį laišką adresu, kurį nurodo duomenų valdytojui. Klientui atšaukus sutikimą, duomenų valdytojas turi nedelsdamas liautis siuntęs reklaminius laiškus. Šiuo atveju neturėtų būti taikomos piniginės sankcijos, pavyzdžiui, mokesčiai. Tačiau atšaukimas taikomas ateityje ir negalioja atgaline data. Laikotarpis, per kurį kliento asmens duomenys buvo tvarkomi teisėtai, gavus kliento sutikimą, buvo teisėtas. Atšaukimas užkerta kelią bet kokiam tolesniam šių duomenų tvarkymui, išskyrus atvejus, kai tai daroma siekiant įgyvendinti teisę reikalauti ištrinti duomenis[377].

Būtinybė vykdyti sutartį

ES teisėje, t. y. BDAR 6 straipsnio 1 dalies b punkte, numatytas kitas teisėto duomenų tvarkymo pagrindas, būtent kai „būtina siekiant įvykdyti sutartį, kurios šalis yra duomenų subjektas“. Ši nuostata taip pat taikoma ikisutartiniams santykiams. Pavyzdžiui, tais atvejais, kai šalis ketina sudaryti sutartį, bet to dar nepadarė, galbūt dėl to, kad dar reikia atlikti tam tikrus patikrinimus. Jeigu vienai šaliai reikia tvarkyti duomenis šiuo tikslu, toks duomenų tvarkymas yra teisėtas, jeigu jis yra būtinas „siekiant imtis priemonių duomenų subjekto prašymu prieš sudarant sutartį“[378].

Atnaujintos 108-osios konvencijos 5 straipsnio 2 dalyje įtvirtinta duomenų tvarkymo, kaip „teisėto įstatyme nustatyto pagrindo“, sąvoka taip pat apima „duomenų tvarkymą siekiant įvykdyti sutartį (arba ikisutartines priemones duomenų subjekto prašymu), kurios šalimi yra duomenų subjektas“[379].

375 Bendrojo duomenų apsaugos reglamento 7 straipsnio 3 dalis.

376 Bendrojo duomenų apsaugos reglamento 42 konstatuojamoji dalis ir atnaujintos 108-osios konvencijos aiškinamosios ataskaitos 42 punktas.

377 Bendrojo duomenų apsaugos reglamento 17 straipsnio 1 dalies b punktas.

378 *Ten pat*, 6 straipsnio 1 dalies b punktas.

379 Atnaujintos 108-osios konvencijos aiškinamoji ataskaita, 46 punktas; Europos Taryba, Ministrų Komitetas, Rekomendacija *CM/Rec(2010)13* valstybėms narėms dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu vykdant profiliavimą, 3.4 straipsnio b punktas, 2010 m. lapkričio 23 d.

Duomenų valdytojo teisinės pareigos

ES teisėje nustatytas kitas teisėto duomenų tvarkymo pagrindas, būtent „tvarkyti duomenis būtina, kad būtų įvykdyta duomenų valdytojui taikoma teisinė prievolė“ (BDAR 6 straipsnio 1 dalies c punktas). Šioje nuostatoje pateikiama nuoroda į privačiajame ir viešajame sektoriuose veikiančius duomenų valdytojus; viešojo sektoriaus duomenų valdytojų teisinės prievolės taip pat gali patekti į BDAR 6 straipsnio 1 dalies e punkto taikymo sritį. Yra daugybė situacijų, kai pagal teisės aktus privačiojo sektoriaus duomenų valdytojai įpareigojami tvarkyti konkrečių duomenų subjektų duomenis, pavyzdžių. Pavyzdžiui, darbdaviai privalo tvarkyti savo darbuotojų duomenis socialinės apsaugos ir mokesčių tikslais, o įmonės privalo tvarkyti savo klientų duomenis mokesčių tikslais.

Teisinė prievolė gali būti nustatyta Sąjungos arba valstybės narės teisėje, kuri galėtų būti vienos arba kelių duomenų tvarkymo operacijų pagrindas. Būtent įstatyme turėtų būti nustatytas duomenų tvarkymo tikslas, duomenų valdytojo nustatymo kriterijai, tvarkomų asmens duomenų rūšis, atitinkami duomenų subjektai, subjektai, kuriems galima atskleisti duomenis, tikslų apribojimo atvejai, saugojimo laikotarpis ir kitos priemonės, kuriomis užtikrinamas teisėtas ir sąžiningas duomenų tvarkymas[380]. Bet kuris toks įstatymas, kuris sudaro asmens duomenų tvarkymo pagrindą, turi atitikti Chartijos 7 ir 8 straipsnius ir EŽTK 8 straipsnį.

Duomenų valdytojo teisinės prievolės **pagal ET teisę** taip pat yra teisėto duomenų tvarkymo pagrindas[381]. Kaip nurodyta pirmiau, privačiojo sektoriaus duomenų valdytojo teisinės prievolės yra tik vienas konkretus atvejis, susijęs su kitų asmenų interesais, kaip paminėta EŽTK 8 straipsnio 2 dalyje. Todėl darbdavių, tvarkančių savo darbuotojų duomenis, pavyzdys taip pat svarbus ET teisei.

Duomenų subjekto arba kito fizinio asmens gyvybiniai interesai

ES teisėje, t. y. BDAR 6 straipsnio 1 dalies d punkte, nustatyta, kad asmens duomenų tvarkymas yra teisėtas, jeigu juos tvarkyti „būtina siekiant apsaugoti gyvybinius duomenų subjekto ar kito fizinio asmens interesus“. Teisėtu asmens duomenų tvarkymo pagrindu gali būti remiamasi, tik jeigu jis grindžiamas kito fizinio asmens gyvybiniais interesais ir jeigu toks duomenų tvarkymas „negali būti akivaizdžiai

380 Bendrojo duomenų apsaugos reglamento 45 konstatuojamoji dalis.

381 Europos Taryba, Ministrų Komitetas (2010), Ministrų Komiteto rekomendacija CM/Rec (2010)13 valstybėms narėms dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu profiliavimo kontekste, 2010 m. lapkričio 23 d., 3.4 straipsnio a punktas.

grindžiamas kitu teisiniu pagrindu“[382]. Kartais duomenų tvarkymo rūšis gali būti grindžiama viešojo intereso ir duomenų subjekto arba to kito asmens gyvybiniais interesais, pavyzdžiui, vykdant epidemijų ir jų vystymosi stebėseną arba susidarius ekstremaliajai humanitarinei situacijai.

Kalbant apie **ET teisę**, pažymėtina, kad duomenų subjekto gyvybiniai interesai neminimi EŽTK 8 straipsnyje. Tačiau duomenų subjekto gyvybiniai interesai laikomi numanomais atsižvelgiant į atnaujintos 108-osios konvencijos 5 straipsnio 2 dalyje vartojamą sąvoką „teisėtas pagrindas“, kurioje aptariamas asmens duomenų tvarkymo teisėtumas[383].

Viešasis interesas ir oficialių įgaliojimų vykdymas

Atsižvelgiant į daugybę viešųjų reikalų organizavimo būdų, BDAR 6 straipsnio 1 dalies e punkte nustatyta, kad asmens duomenys gali būti teisėtai tvarkomi, jeigu „tvarkyti duomenis būtina siekiant atlikti užduotį, vykdomą viešojo intereso labui arba vykdant duomenų valdytojui pavestas viešosios valdžios funkcijas <...>“[384].

Pavyzdys. Byloje *Huber prieš Bundesrepublik Deutschland*[385] Vokietijoje gyvenantis Austrijos pilietis D. Huber paprašė Federalinio migracijos ir pabėgėlių biuro panaikinti jo duomenis centriniame užsieniečių registre (toliau – AZR). Šį registrą, kuriame pateikiami duomenys apie ne Vokietijos ES piliečius, gyvenančius Vokietijoje daugiau nei tris mėnesius, teisėsaugos ir teisminės institucijos naudoja statistiniais tikslais tirdamos baudžiamąsias arba visuomenės saugumui pavojų keliančias veikas ir vykdo jų baudžiamąjį persekiojimą. Prašymą priimti prejudicinį sprendimą pateikęs teismas klausė, ar asmens duomenų tvarkymas, vykdomas registre, pavyzdžiui, centriniame užsienio piliečių registre, su kurio duomenimis gali susipažinti ir valdžios institucijos, yra suderinamas su ES teise atsižvelgiant į tai, kad tokio registro apskritai nėra Vokietijos piliečiams.

382 Bendrojo duomenų apsaugos reglamento 46 konstatuojamoji dalis.

383 Atnaujintos 108-osios konvencijos aiškinamosios ataskaitos 46 punktas.

384 Žr. Bendrojo duomenų apsaugos reglamento 45 konstatuojamąją dalį.

385 ESTT, C-524/06, *Heinz Huber prieš Bundesrepublik Deutschland* (DK), 2008 m. gruodžio 16 d.

ESTT nusprendė, kad pagal Direktyvos 95/46/EB 7 straipsnio e punktą[386] asmens duomenys gali būti teisėtai tvarkomi, jeigu tvarkyti duomenis būtina siekiant atlikti užduotį, vykdomą viešojo intereso labui, arba vykdant duomenų valdytojui pavestas viešosios valdžios funkcijas.

Pasak ESTT, „atsižvelgiant į tikslą užtikrinti lygiaverčio lygio apsaugą visose valstybėse narėse, Direktyvos 95/46/EB 7 straipsnio e punkte minimos būtinumo sąvokos[387] <...> turinys skirtingose valstybėse narėse neturėtų skirtis. Taigi tai yra autonomiška Bendrijos sąvoka, kurią reikia aiškinti taip, kad ji visiškai atitiktų šios direktyvos tikslą, įtvirtintą jos 1 straipsnio 1 dalyje“[388].

ESTT pažymėjo, kad Sąjungos piliečio teisė laisvai judėti valstybės narės teritorijoje, kurios pilietis jis nėra, nėra besąlyginė ir jai gali būti taikomi Europos bendrijos steigimo sutartyje ir jai įgyvendinti priimtose priemonėse nustatyti apribojimai bei sąlygos. Todėl jei valstybė narė iš esmės gali teisėtai naudoti registrą, pavyzdžiui, AZR, kad padėtų atsakingosioms institucijoms taikyti teisės aktus, susijusius su teise turėti gyvenamąją vietą, tokiame registre negali būti informacijos, kuri nėra reikalinga siekiant šio konkretaus tikslo. ESTT padarė išvadą, kad tokia asmens duomenų tvarkymo sistema atitinka ES teisę, tik jeigu joje yra duomenys, būtini tam teisės aktui taikyti, ir jeigu, atsižvelgiant į jos centralizuotą pobūdį, to teisės akto taikymas tampa veiksmingesnis. Nacionalinis teismas privalo įvertinti, ar šios sąlygos tenkinamos konkrečioje byloje. Jeigu ne, asmens duomenų saugojimas ir tvarkymas tokiame registre, kaip, pavyzdžiui, AZR, statistiniais tikslais jokiu pagrindu negali būti laikomas būtinu, kaip apibrėžta Direktyvos 95/46/EB 7 straipsnio e punkte[389] [390].

Galiausiai dėl registre esančių duomenų naudojimo kovojant su nusikalstamumu ESTT nusprendė, kad šis tikslas „reikalauja tirti padarytus nusikaltimus ir pažeidimus, neatsižvelgiant į juos padariusių asmenų pilietybę“.

386 Ankstesnės Duomenų apsaugos direktyvos 7 straipsnio e punktas, dabar – Bendrojo duomenų apsaugos reglamento 6 straipsnio 1 dalies e punktas.

387 *Ten pat*.

388 ESTT, C-524/06, *Heinz Huber prieš Bundesrepublik Deutschland* (DK), 2008 m. gruodžio 16 d., 22 punktas.

389 Ankstesnės Duomenų apsaugos direktyvos 7 straipsnio e punktas, dabar – Bendrojo duomenų apsaugos reglamento 6 straipsnio 1 dalies e punktas.

390 ESTT, C-524/06, *Heinz Huber prieš Bundesrepublik Deutschland* (DK), 2008 m. gruodžio 16 d., 54, 58–59 ir 66–68 punktai.

> Nagrinėjamame registre nėra asmens duomenų, susijusių su atitinkamos valstybės narės piliečiais, ir šis skirtingas vertinimas reiškia diskriminaciją, kuri draudžiama pagal SESV 18 straipsnį. Todėl ESTT nustatė, kad ši nuostata „draudžia valstybei narei kovos su nusikalstamumu tikslu įdiegti specialiai šios valstybės narės pilietybės neturintiems Europos Sąjungos piliečiams skirtą asmens duomenų tvarkymo sistemą“[391].

Jei viešojoje srityje veikiančios institucijos naudoja asmens duomenis, tokiam naudojimui taip pat taikomas **EŽTK** 8 straipsnis ir, kai tinkama, turi būti taikoma atnaujintos 108-osios konvencijos 5 straipsnio 2 dalis[392].

Duomenų valdytojo arba trečiosios šalies teisėti interesai

Pagal **ES teisę** teisėtų interesų turi ne tik duomenų subjektas. BDAR 6 straipsnio 1 dalies f punkte nustatyta, kad asmens duomenys gali būti teisėtai tvarkomi, jeigu tai „būtina siekiant teisėtų duomenų valdytojo arba trečiosios šalies [išskyrus valdžios institucijas joms vykdant savo užduotis, kurioms atskleidžiami duomenys] interesų, išskyrus atvejus, kai tokie duomenų subjekto interesai arba pagrindinės teisės ir laisvės, dėl kurių būtina užtikrinti asmens duomenų apsaugą, yra už juos viršesni <...>“[393].

Kiekvienu konkrečiu atveju reikia atidžiai įvertinti, ar esama teisėto intereso[394]. Jeigu nustatomi duomenų valdytojo teisėti interesai, tuomet būtina nustatyti tų interesų ir duomenų subjekto interesų arba pagrindinių teisių ir laisvių pusiausvyrą[395]. Atliekant tokį vertinimą, būtina atsižvelgti į pagrįstus duomenų subjekto lūkesčius, siekiant išsiaiškinti, ar duomenų valdytojo interesai yra viršesni už duomenų subjekto interesus arba pagrindines teises[396]. Jeigu duomenų subjekto teisės yra viršesnės už duomenų valdytojo teisėtus interesus, duomenų valdytojas gali imtis priemonių ir įgyvendinti apsaugos priemones siekdamas užtikrinti, kad poveikis duomenų subjekto teisėms būtų kuo labiau sumažintas (pavyzdžiui, suteikdamas duomenims

391 *Ten pat*, 78 ir 81 punktai.

392 Atnaujintos 108-osios konvencijos aiškinamosios ataskaitos 46 ir 47 punktai.

393 Kitaip nei Direktyvoje 95/46/EB, Bendrajame duomenų apsaugos reglamente pateikiama daugiau atvejų, susijusių su teisėtu interesu, pavyzdžių.

394 Bendrojo duomenų apsaugos reglamento preambulės 47 konstatuojamoji dalis.

395 29 straipsnio darbo grupė (2014 m.), *Nuomonė Nr. 06/2014 dėl duomenų valdytojo teisėtų interesų sampratos pagal Direktyvos 95/46/EB 7 straipsnį*, 2014 m. balandžio 4 d.

396 *Ten pat*.

pseudonimus), ir pakeisti pusiausvyrą prieš galėdamas teisėtai remtis šiuo teisėtu duomenų tvarkymo pagrindu. Savo nuomonėje dėl duomenų valdytojo teisėtų interesų sąvokos 29 straipsnio darbo grupė atkreipė dėmesį į esminį atskaitomybės ir skaidrumo vaidmenį ir duomenų subjekto teises nesutikti, kad jo duomenys būtų tvarkomi arba kad su jais būtų galima susipažinti, juos pakeisti, ištrinti arba perduoti tais atvejais, kai nustatoma duomenų valdytojo teisėtų interesų ir su duomenų subjekto pagrindinėmis teisėmis susijusių interesų pusiausvyra[397].

BDAR konstatuojamosiose dalyse pateikiama keletas pavyzdžių, iš kurių matyti, kokių teisėtų interesų gali turėti atitinkamas duomenų valdytojas. Pavyzdžiui, asmens duomenis leidžiama tvarkyti be duomenų subjekto sutikimo, kai tai daroma tiesioginės rinkodaros tikslais arba kai toks duomenų tvarkymas yra būtinas „sukčiavimo prevencijos tikslais“[398].

Savo jurisprudencijoje ESTT išplėtojo kriterijus, kuriais remiantis nustatoma, kas laikoma teisėtu interesu.

Pavyzdys. Byla *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde*[399] buvo susijusi su žala, kurią Rygos troleibusų transporto bendrovei padarė taksi automobilio duris staiga atidaręs keleivis. *Rīgas satiksme* norėjo pareikšti keleiviui ieškinį dėl nuostolių atlyginimo. Tačiau policija pateikė tik keleivio vardą ir pavardę ir atsisakė pateikti keleivio tapatybės dokumento numerį ir adresą, teigdama, kad atskleidimas būtų neteisėtas pagal nacionalinius duomenų teisės įstatymus.

Latvijos prašymą priimti prejudicinį sprendimą pateikęs teismas prašė ESTT priimti prejudicinį sprendimą dėl to, ar ES duomenų apsaugos teisės aktuose nustatyta prievolė atskleisti visus asmens duomenis, kurie yra būtini norint iškelti civilinę bylą asmeniui, kuris, kaip įtariama, yra atsakingas už administracinį nusižengimą[400].

397 *Ten pat*.

398 Bendrojo duomenų apsaugos reglamento preambulės 47 konstatuojamoji dalis.

399 ESTT, C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde prieš Rīgas pašvaldības SIA „Rīgas satiksme“*, 2017 m. gegužės 4 d.

400 *Ten pat*, 23 punktas.

ESTT paaiškino, kad ES duomenų apsaugos teisėje numatyta galimybė – ne prievolė – perduoti duomenis trečiajai šaliai atsižvelgiant į tos šalies teisėtus interesus[401]. ESTT nustatė tris sąlygas, kurias visas būtina įvykdyti, kad asmens duomenų tvarkymas, remiantis „teisėtų interesų" pagrindu, būtų teisėtas[402]. Pirma, trečioji šalis, kuriai atskleidžiami duomenys, privalo siekti įgyvendinti teisėtą interesą. Šioje konkrečioje byloje tai reiškia, kad prašymas pateikti asmens duomenis siekiant pareikšti ieškinį asmeniui, padariusiam turtinę žalą, yra teisėtas trečiojo asmens interesas. Antra, asmens duomenis tvarkyti būtina siekiant teisėtų interesų. Šioje byloje asmens duomenų gavimas, pavyzdžiui, adreso ir (arba) tapatybės dokumento numerio, yra griežtai būtinas siekiant nustatyti to asmens tapatybę. Trečia, duomenų subjekto pagrindinės teisės ir laisvės neturi būti viršesnės už duomenų valdytojo arba trečiųjų šalių teisėtus interesus. Interesų pusiausvyrą būtina nustatyti kiekvienu konkrečiu atveju atsižvelgiant į tokius aspektus, kaip duomenų subjekto teisių pažeidimo rimtumas arba net tam tikromis aplinkybėmis – duomenų subjekto amžius. Tačiau šioje konkrečioje byloje ESTT nemanė, kad atsisakymas atskleisti duomenis turi būti pagrįstas vien todėl, kad duomenų subjektas buvo nepilnametis.

Byloje *ASNEF ir FECEMD* ESTT priėmė aiškų sprendimą dėl asmens duomenų tvarkymo, pagrįsto teisėtu „teisėtų interesų" pagrindu, kuris tuo metu buvo nustatytas Duomenų apsaugos direktyvos 7 straipsnio f punkte[403].

Pavyzdys. Byloje *ASNEF ir FECEMD*[404] ESTT paaiškino, kad pagal nacionalinę teisę neleidžiama nustatyti papildomų teisėto duomenų tvarkymo sąlygų, išskyrus tas, kurios paminėtos Duomenų apsaugos direktyvos 7 straipsnio f punkte[405]. Tai apėmė situaciją, kurioje Ispanijos duomenų apsaugos įstatyme

401 *Ten pat*, 26 punktas.

402 *Ten pat*, 28–34 punktai.

403 Ankstesnės Duomenų apsaugos direktyvos 7 straipsnio f punktas, dabar Bendrojo duomenų apsaugos reglamento 6 straipsnio 1 dalies f punktas.

404 ESTT, sujungtos bylos C-468/10 ir C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) ir Federación de Comercio Electrónico y Marketing Directo (FECEMD) prieš Administración del Estado*, 2011 m. lapkričio 24 d.

405 Ankstesnės Duomenų apsaugos direktyvos 7 straipsnio f punktas, dabar Bendrojo duomenų apsaugos reglamento 6 straipsnio 1 dalies f punktas.

buvo įtvirtinta nuostata, pagal kurią kitos privačios šalys galėtų remtis teisėtu asmens duomenų tvarkymo interesu, tik jeigu informacija jau buvo paskelbta viešuose šaltiniuose.

ESTT pirmiausia pažymėjo, kad Direktyva 95/46/EB[406] siekiama visose valstybėse narėse užtikrinti vienodą asmenų teisių ir laisvių apsaugos tvarkant asmens duomenis lygį. Todėl derinant šioje srityje taikytinus nacionalinius įstatymus negali būti nustatyta mažesnė šiais įstatymais užtikrinama apsauga. Iš tiesų būtina siekti užtikrinti aukštą apsaugos lygį ES[407]. Todėl ESTT nusprendė, kad „iš tikslo užtikrinti visose valstybėse narėse lygiavertį apsaugos lygį matyti, kad Direktyvos 95/46/EB[408] 7 straipsnyje pateiktas atvejų, kai asmens duomenų tvarkymas gali būti laikomas teisėtu, sąrašas yra išsamus ir baigtinis“. Be to, „valstybės narės negali papildyti Direktyvos 95/46/EB[409] 7 straipsnyje nurodytų asmens duomenų tvarkymo teisėtumo principų naujais ar numatyti papildomų reikalavimų, kuriais būtų pakeista kurio nors iš šiame straipsnyje numatytų šešių principų apimtis“[410]. ESTT pripažino, kad, atsižvelgiant į pusiausvyros nustatymą, kuris yra būtinas pagal Direktyvos 95/46/EB 7 straipsnio f punktą, įmanoma atsižvelgti į tai, kad duomenų subjekto pagrindinių teisių pažeidimo, kurį lemia duomenų tvarkymas, rimtumas gali būti nevienodas, priklausomai nuo to, ar atitinkami duomenys jau yra paskelbti viešuose šaltiniuose.

Tačiau direktyvos 7 straipsnio f punktu „draudžiama valstybėms narėms kategoriškai ir visais atvejais panaikinti galimybę tvarkyti tam tikrų kategorijų asmens duomenis, neleidžiant palyginti konkrečios situacijos priešingų teisių ir interesų“.

406 Ankstesnė Duomenų apsaugos direktyva, dabar – Bendrasis duomenų apsaugos reglamentas.

407 ESTT, sujungtos bylos C-468/10 ir C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) ir Federación de Comercio Electrónico y Marketing Directo (FECEMD) prieš Administración del Estado*, 2011 m. lapkričio 24 d., 28 punktas. Žr. Bendrojo duomenų apsaugos reglamento 8 ir 10 konstatuojamąsias dalis.

408 Ankstesnės Duomenų apsaugos direktyvos 7 straipsnis, dabar Bendrojo duomenų apsaugos reglamento 6 straipsnio 1 dalies f punktas.

409 Ankstesnė Duomenų apsaugos direktyva, dabar – Bendrasis duomenų apsaugos reglamentas.

410 *Ten pat*.

Atsižvelgdamas į šias aplinkybes, ESTT padarė išvadą, kad Direktyvos 95/46/EB[411] 7 straipsnio f punktą „reikia suprasti taip, kad juo draudžiami nacionalinės teisės aktai, pagal kuriuos duomenų valdytojas arba tretieji asmenys, kuriems atskleidžiami asmens duomenys, turėdami teisėtą tikslą, gali tvarkyti asmens duomenis be duomenų subjekto sutikimo, tik jei paiso duomenų subjekto pagrindinių teisių ir laisvių, ir, be to, šie duomenys yra viešųjų rinkmenų dalis, todėl tokiose rinkmenose nesančių duomenų tvarkymas yra kategoriškai ir jokiais atvejais negalimas“[412].

Kai asmens duomenys tvarkomi remiantis „teisėtų interesų“ pagrindu, asmuo pagal BDAR 21 straipsnio 1 dalį turi teisę bet kuriuo metu nesutikti, kad duomenys būtų tvarkomi, remdamasis pagrindais, susijusiais su jo konkrečia situacija. Duomenų valdytojas privalo sustabdyti duomenų tvarkymą, išskyrus atvejus, kai įrodo, kad yra įtikinamų priežasčių jį tęsti.

Kalbant apie **ET teisę**, pažymėtina, kad panašių formuluočių galima rasti atnaujintoje 108-ojoje konvencijoje[413] ir ET rekomendacijose. Rekomendacijoje dėl profiliavimo pripažįstama, kad asmens duomenų tvarkymas profiliavimo tikslais yra teisėtas, jeigu jis būtinas atsižvelgiant į kitų asmenų teisėtus interesus, „išskyrus atvejus, kai duomenų subjektų pagrindinės teisės ir laisvės yra viršesnės už tokius interesus“[414]. Be to, „kitų asmenų teisių ir laisvių apsauga“ EŽTK 8 straipsnio 2 dalyje minima kaip vienas iš teisėtų teisės į duomenų apsaugą apribojimo pagrindų.

Pavyzdys. Byloje *Y prieš Turkiją*[415] pareiškėjas buvo užsikrėtęs ŽIV. Atvykęs į ligoninę jis buvo nesąmoningas, todėl greitosios medicinos pagalbos darbuotojai informavo ligoninės darbuotojus, kad pareiškėjas yra infekuotas ŽIV.

411 Ankstesnės Duomenų apsaugos direktyvos 7 straipsnio f punktas, dabar Bendrojo duomenų apsaugos reglamento 6 straipsnio 1 dalies f punktas.

412 ESTT, sujungtos bylos C-468/10 ir C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) ir Federación de Comercio Electrónico y Marketing Directo (FECEMD) prieš Administración del Estado*, 2011 m. lapkričio 24 d. 40, 44 ir 48–49 punktai.

413 Atnaujintos 108-osios konvencijos aiškinamosios ataskaitos 46 punktas.

414 Ministrų Taryba, Ministrų Komitetas (2010 m.), Rekomendacija *CM/Rec(2010)13* ir aiškinamasis memorandumas dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu profiliavimo kontekste, 2010 m. lapkričio 23 d., 3.4 straipsnio b punktas (Rekomendacija dėl profiliavimo).

415 EŽTT, *Y prieš Turkiją*, Nr. 648/10, 2015 m. vasario 17 d.

Pareiškėjas EŽTT teigė, kad, atskleidus šią informaciją, buvo pažeista jo teisė į privatų gyvenimą. Tačiau, atsižvelgiant į poreikį užtikrinti ligoninės darbuotojų saugumą, dalijimasis informacija nebuvo laikomas jo teisių pažeidimu.

4.1.2. Specialių kategorijų duomenų (neskelbtinų duomenų) tvarkymas

Pagal **ET teisę** paliekama galimybė nacionalinėje teisėje nustatyti atitinkamas neskelbtinų duomenų naudojimo apsaugos priemones, jeigu įvykdomos atnaujintos 108-osios konvencijos 6 straipsnyje nustatytos sąlygos, būtent jeigu teisėje numatomos tinkamos apsaugos priemonės, kuriomis papildomos kitos Konvencijos nuostatos. Pagal **ES teisę** BDAR 9 straipsnyje nustatyta išsami specialių kategorijų duomenų (kurie taip pat vadinami neskelbtinais duomenimis) tvarkymo sistema. Šie duomenys parodo rasinę ar etninę kilmę, politines pažiūras, religinius ar filosofinius įsitikinimus ir narystę profesinėse sąjungose, taip pat genetinius ir biometrinius duomenis, skirtus tik fizinio asmens tapatybei nustatyti, ir duomenis, susijusius su asmens sveikata, lytiniu gyvenimu ar seksualine orientacija. Neskelbtinus duomenis iš esmės draudžiama tvarkyti[416].

Tačiau reglamento 9 straipsnio 2 dalyje galima rasti išsamų šio draudimo išimčių, kuriomis galima pateisinti neskelbtinų duomenų tvarkymą, sąrašą. Šios išimtys apima situacijas, kai:

- duomenų subjektas aiškiai sutinka, kad duomenys būtų tvarkomi;
- duomenis tvarko ne pelno organizacija, turinti politinių, filosofinių, religinių ar profesinių sąjungų tikslų, vykdydama savo teisėtą veiklą, ir jie yra susiję tik su jos (buvusiais) nariais arba asmenimis, kurie su ja nuolat palaiko ryšius tokiais tikslais;
- duomenų tvarkymas yra susijęs su duomenimis, kuriuos duomenų subjektas yra akivaizdžiai paskelbęs viešai;
- duomenis tvarkyti būtina:

416 Ankstesnės Duomenų apsaugos direktyvos 7 straipsnio f punktas, dabar – Bendrojo duomenų apsaugos reglamento 9 straipsnio 1 dalis.

- siekiant įvykdyti duomenų valdytojo arba duomenų subjekto prievoles arba įgyvendinti konkrečias teises, susijusias su užimtumu, socialiniu draudimu ir socialine apsauga;

- siekiant apsaugoti duomenų subjekto arba kito fizinio asmens gyvybinius interesus (kai duomenų subjektas negali duoti sutikimo);

- siekiant nustatyti, įgyvendinti arba apginti teisinius reikalavimus arba teismams vykdant savo teismines funkcijas;

- prevencinės arba darbo medicinos tikslais; „siekiant įvertinti darbuotojo darbingumą, nustatyti medicininę diagnozę, teikti sveikatos priežiūros arba socialinės rūpybos paslaugas ar gydymą arba valdyti sveikatos priežiūros ar socialinės rūpybos sistemas ir paslaugas remiantis Sąjungos arba valstybės narės teise arba pagal sutartį su sveikatos priežiūros specialistu“;

- archyvavimo tikslais viešojo intereso labui, mokslinių ar istorinių tyrimų tikslais arba statistiniais tikslais;

- dėl viešojo intereso priežasčių visuomenės sveikatos srityje arba

- dėl svarbių viešojo intereso priežasčių.

Todėl tvarkant specialių kategorijų duomenis sutartiniai santykiai su duomenų subjektu paprastai nelaikomi teisėto neskelbtinų duomenų tvarkymo teisiniu pagrindu, išskyrus atvejus, kai sutartis yra sudaryta su sveikatos priežiūros specialistu, kuriam galioja prievolė saugoti profesinę paslaptį[417].

Aiškus duomenų subjekto sutikimas

Pagal **ES teisę** pirmas galimas teisėto bet kurių duomenų tvarkymo pagrindas, nepaisant to, ar tai yra paprasti, ar neskelbtini duomenys, yra duomenų subjekto sutikimas. Neskelbtinų duomenų atveju toks sutikimas turi būti aiškus. Tačiau Sąjungos arba valstybės narės teisėje gali būti numatyta, kad asmuo negali panaikinti draudimo tvarkyti tam tikrų kategorijų duomenis[418]. Taip, pavyzdžiui, turėtų būti tuo atveju, kai tvarkant duomenis duomenų subjektui kyla neįprasta rizika.

417 Bendrojo duomenų apsaugos reglamento 9 straipsnio 2 dalies h ir i punktai.

418 *Ten pat*, 9 straipsnio 2 dalies a punktas.

Užimtumo teisė arba socialinio draudimo ir socialinės apsaugos teisė

Pagal **ES teisę** 9 straipsnio 1 dalies draudimas gali būti panaikintas, jeigu duomenis tvarkyti būtina siekiant vykdyti duomenų valdytojo arba duomenų subjekto pareigas arba teises, susijusias su užimtumo arba socialinio draudimo sritimi. Tačiau duomenų tvarkymas turi būti leistinas pagal ES teisę, nacionalinę teisę arba kolektyvinį susitarimą, sudarytą pagal nacionalinę teisę, kuriame numatytos tinkamos duomenų subjekto pagrindinių teisių ir laisvių apsaugos priemonės[419]. Organizacijos saugomose darbo bylose gali būti neskelbtinų asmens duomenų, kurie tokiais laikomi pagal tam tikras BDAR ir atitinkamoje nacionalinėje teisėje nustatytas sąlygas. Neskelbtinų duomenų pavyzdžiai gali būti narystė profesinėse sąjungose arba informacija apie sveikatą.

Duomenų subjekto arba kito asmens gyvybiniai interesai

Pagal **ES teisę**, kaip ir paprastų duomenų atveju, neskelbtini duomenys gali būti tvarkomi atsižvelgiant į duomenų subjekto arba kito fizinio asmens gyvybinius interesus[420]. Jeigu duomenų tvarkymas yra pagrįstas gyvybiniais kito asmens interesais, šiuo teisėtu pagrindu gali būti remiamasi, tik jeigu toks tvarkymas „negali būti akivaizdžiai grindžiamas kitu teisiniu pagrindu“[421]. Tam tikrais atvejais asmens duomenų tvarkymas gali padėti apsaugoti tiek individualius, tiek visuomenės interesus, pavyzdžiui, kai duomenis tvarkyti būtina humanitariniais tikslais[422].

Kad neskelbtinų duomenų tvarkymas, remiantis šiuo pagrindu, būtų teisėtas, turėtų būti neįmanoma prašyti duomenų subjekto sutikimo, nes, pavyzdžiui, duomenų subjektas buvo nesąmoningas arba jo nebuvo ir jo nebuvo galima pasiekti. Kitaip tariant, asmuo sutikimo negalėjo duoti dėl fizinės negalios arba neveiksnumo.

Labdaros organizacijos arba ne pelno organizacijos

Asmens duomenis taip pat leidžiama tvarkyti vykdant teisėtą fondų, asociacijų ar kitų ne pelno organizacijų, siekiančių politinio, filosofinio, religinio arba profesinės sąjungos tikslo, veiklą. Tačiau duomenų tvarkymas būtinai turi būti susijęs tik su organizacijos esamais arba buvusiais nariais arba nariais, kurie reguliariai palaiko

419 Bendrojo duomenų apsaugos reglamento 9 straipsnio 2 dalies b punktas.

420 *Ten pat*, 9 straipsnio 2 dalies c punktas.

421 *Ten pat*, 46 konstatuojamoji dalis.

422 *Ten pat*.

ryšius su organizacija[423]. Šios organizacijos neskelbtinų duomenų negali atskleisti be duomenų subjekto sutikimo.

Duomenys, kuriuos duomenų subjektas yra akivaizdžiai paskelbęs viešai

BDAR 9 straipsnio 2 dalies e punkte nustatyta, kad tvarkyti duomenų nedraudžiama, jeigu tvarkymas yra susijęs su duomenimis, kuriuos duomenų subjektas yra akivaizdžiai paskelbęs viešai. Nepaisant to, kad sąvoka „duomenys, kuriuos duomenų subjektas yra akivaizdžiai paskelbęs viešai" reglamente neapibrėžta, nes tai yra draudimo tvarkyti neskelbtinus duomenis išimtis, ją būtina aiškinti griežtai ir kaip reiškiančią, kad duomenų subjektas sąmoningai viešai atskleidė savo asmens duomenis. Todėl jeigu televizijoje transliuojamas vaizdo stebėjimo kameros įrašas, kuriame, be kita ko, matomas sužalotas gaisrininkas, bandantis evakuotis iš pastato, negalima manyti, kad gaisrininkas akivaizdžiai viešai paskelbė duomenis. Kita vertus, jeigu gaisrininkas nusprendžia aprašyti incidentą ir paskelbti vaizdo įrašą ir nuotraukas viešame interneto tinklalapyje, jis turėtų atlikti sąmoningą patvirtinamąjį veiksmą, kad atskleistų asmens duomenis. Svarbu pažymėti, kad kurio nors asmens duomenų atskleidimas nereiškia sutikimo, tačiau tai yra kitas leidimas tvarkyti specialių kategorijų duomenis.

Tai, jog duomenų subjektas tvarkomus duomenis yra akivaizdžiai paskelbęs viešai, nereiškia, kad duomenų valdytojai atleidžiami nuo prievolių pagal duomenų apsaugos teisę. Pavyzdžiui, tikslų apribojimo principas toliau taikomas asmens duomenims, net jeigu tokie duomenys buvo paskelbti viešai[424].

Teisiniai reikalavimai

Specialių kategorijų duomenų, kurie „yra būtin[i] siekiant pareikšti, vykdyti arba apginti teisinius reikalavimus", tvarkymas, nepaisant to, ar tai daroma teismo byloje arba administracinėje arba neteisminėje procedūroje[425], taip pat yra leidžiamas pagal BDAR[426]. Šiuo atveju duomenų tvarkymas, kurio gali prašyti bet kuri ginčo šalis,

423 *Ten pat*, 9 straipsnio 2 dalies d punktas.

424 29 straipsnio darbo grupė (2013 m.), *Nuomonė Nr. 3/13 dėl tikslų apribojimo*, WP 203, Briuselis, 2013 m. balandžio 2 d., p. 14.

425 Bendrojo duomenų apsaugos reglamento preambulės 52 konstatuojamoji dalis.

426 *Ten pat*, 9 straipsnio 2 dalies f punktas.

turi būti susijęs su konkrečiu teisiniu reikalavimu ir atitinkamai jo užtikrinimu arba gynimu.

Vykdydami teismines funkcijas, teismai, spręsdami teisinį ginčą, gali tvarkyti tam tikrų kategorijų duomenis[427]. Šiomis aplinkybėmis šių specialių kategorijų tvarkomų duomenų pavyzdžiai gali apimti, pavyzdžiui, genetinius duomenis nustatant tėvystę arba sveikatos būklę, kai tam tikra dalis įrodymų yra susiję su informacija apie nusikaltimo aukos patirtą sužalojimą.

Svarbaus viešojo intereso priežastys

Pagal BDAR 9 straipsnio 2 dalies g punktą valstybės narės gali nustatyti papildomas aplinkybes, kuriomis gali būti tvarkomi neskelbtini duomenys, jeigu:

- duomenys tvarkomi dėl svarbaus viešojo intereso priežasčių;
- jos numatytos Europos arba nacionalinėje teisėje;
- Europos arba nacionalinė teisė yra proporcinga, ja paisoma teisės į duomenų apsaugą ir joje numatytos tinkamos ir konkrečios priemonės, padedančios apsaugoti duomenų subjekto teises ir interesus[428].

Puikus pavyzdys – elektroninės sveikatos bylų sistemos. Tokiose sistemose su sveikatos priežiūros paslaugų teikėjų sveikatos duomenimis, surinktais gydant pacientą, plačiu, paprastai visos šalies, mastu gali susipažinti kiti sveikatos priežiūros paslaugų teikėjai.

29 straipsnio darbo grupė priėjo prie išvados, kad tokios sistemos negali būti sukuriamos pagal dabartines pacientų duomenų tvarkymo teisines taisykles[429]. Tačiau elektroninės sveikatos bylų sistemos gali veikti, jeigu jos grindžiamos „svarbaus viešojo intereso priežastimis“[430]. Tam reikėtų aiškaus teisinio jų sukūrimo pagrindo,

427 *Ten pat*.

428 *Ten pat*, 9 straipsnio 2 dalies g punktas.

429 29 straipsnio darbo grupė (2007 m.), *Darbinis dokumentas dėl asmens duomenų, susijusių su sveikata elektroniniuose sveikatos įrašuose (EHR), tvarkymo*, WP 131, Briuselis, 2007 m. vasario 15 d. Taip pat žr. Bendrojo duomenų apsaugos reglamento 9 straipsnio 3 punktą.

430 Bendrojo duomenų apsaugos reglamento 9 straipsnio 2 dalies g punktas.

kuriame taip pat būtų numatytos būtinos apsaugos priemonės siekiant užtikrinti, kad sistema veiktų saugiai[431].

Kiti neskelbtinų duomenų tvarkymo pagrindai

BDAR nustatyta, kad neskelbtini duomenys gali būti tvarkomi, jeigu juos tvarkyti būtina[432]:

- prevenciniais arba profesiniais medicinos tikslais, siekiant įvertinti darbuotojo darbingumą, nustatyti medicininę diagnozę, teikti sveikatos priežiūros arba socialinės rūpybos paslaugas ar gydymą arba valdyti sveikatos priežiūros ar socialinės rūpybos sistemas ir paslaugas remiantis ES arba valstybės narės teise arba pagal sutartį su sveikatos priežiūros specialistu;

- dėl viešojo intereso priežasčių visuomenės sveikatos srityje, pavyzdžiui, apsauga nuo didelių tarpvalstybinio pobūdžio grėsmių sveikatai arba aukštų sveikatos priežiūros ir vaistų arba medicinos prietaisų kokybės ir saugos standartų užtikrinimas remiantis ES arba valstybės narės teise. Teisės aktuose turi būti numatytos tinkamos ir konkrečios priemonės, kuriomis apsaugomos duomenų subjekto teisės;

- archyvavimo, moksliniais ar istorinių tyrimų arba statistiniais tikslais pagal Sąjungos ar valstybės narės teisę. Teisės aktas turi būti proporcingas atsižvelgiant į siekiamą tikslą, juo turi būti paisoma teisės į duomenų apsaugą ir jame turi būti numatytos tinkamos ir konkrečios priemonės, padedančios apsaugoti duomenų subjekto teises ir interesus.

Papildomos sąlygos pagal nacionalinę teisę

BDAR valstybėms narėms taip pat leidžiama nustatyti arba toliau taikyti papildomas sąlygas, įskaitant genetinių, biometrinių ir su sveikata susijusių duomenų tvarkymo apribojimus[433].

431 29 straipsnio darbo grupė (2007 m.), *Darbinis dokumentas dėl asmens duomenų, susijusių su sveikata elektroniniuose sveikatos įrašuose (EHR), tvarkymo*, WP 131, Briuselis, 2007 m. vasario 15 d.

432 Bendrojo duomenų apsaugos reglamento 9 straipsnio 2 dalies h, i ir j punktai.

433 *Ten pat*, 9 straipsnio 2 dalies h punktas ir 9 straipsnio 4 dalis.

4.2. Duomenų tvarkymo saugumo taisyklės

Pagrindiniai faktai

- Duomenų tvarkymo saugumo taisyklėmis duomenų valdytojas ir duomenų tvarkytojas įpareigojami įgyvendinti tinkamas technines ir organizacines priemones, kuriomis užkertamas kelias bet kokiam neteisėtam kišimuisi į duomenų tvarkymo operacijas.
- Būtinas duomenų saugumo lygis nustatomas atsižvelgiant į:
  - rinkoje prieinamas saugumo priemones, susijusias su bet kurios konkrečios rūšies duomenų tvarkymu;
  - sąnaudas;
  - riziką, kuri duomenų subjektų pagrindinėms teisėms ir laisvėms kyla tvarkant duomenis.
- Asmens duomenų konfidencialumo užtikrinimas yra Bendrajame duomenų apsaugos reglamente pripažįstamo bendrojo principo sudedamoji dalis.

Pagal **ES ir ET teisę** duomenų valdytojai turi bendrą prievolę, tvarkydami asmens duomenis, užtikrinti skaidrumą ir atskaitomybę, visų pirma tai pasakytina apie padarytus duomenų saugumo pažeidimus. Asmens duomenų saugumo pažeidimo atvejais duomenų valdytojai privalo informuoti priežiūros institucijas, išskyrus atvejus, kai asmens duomenų saugumo pažeidimas neturėtų kelti pavojaus fizinių asmenų teisėms ir laisvėms. Duomenų subjektus taip pat reikėtų informuoti apie asmens duomenų saugumo pažeidimą, kai tikėtina, kad jis kels didelį pavojų fizinių asmenų teisėms ir laisvėms.

4.2.1. Duomenų saugumo elementai

Pagal atitinkamas **ES teisės nuostatas**:

> *„Atsižvelgdamas į techninių galimybių išsivystymo lygį, įgyvendinimo sąnaudas bei duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, taip pat duomenų tvarkymo keliamus įvairios tikimybės ir rimtumo pavojus fizinių asmenų teisėms ir laisvėms, duomenų valdytojas ir duomenų*

tvarkytojas įgyvendina tinkamas technines ir organizacines priemones, kad būtų užtikrintas pavojų atitinkančio lygio saugumas <...>.“[434]

Šios priemonės, be kita ko, apima:

- pseudonimų suteikimą duomenims ir jų šifravimą[435];
- gebėjimą užtikrinti nuolatinį duomenų tvarkymo sistemų ir paslaugų konfidencialumą, vientisumą, prieinamumą ir atsparumą[436];
- gebėjimą laiku atkurti sąlygas ir galimybes naudotis asmens duomenimis duomenų praradimo atveju[437];
- reguliarų techninių ir organizacinių priemonių, kuriomis užtikrinamas duomenų tvarkymo saugumas, tikrinimo, vertinimo ir veiksmingumo vertinimo procesą[438].

Panaši nuostata įtvirtinta ir **ET teisėje**:

„Kiekviena Šalis nustato, kad duomenų valdytojas ir, kai taikoma, duomenų tvarkytojas imasi tinkamų saugumo priemonių nuo rizikos, pavyzdžiui, atsitiktinės ar neleistinos prieigos prie asmens duomenų, jų sunaikinimo, praradimo, naudojimo, pakeitimo ar atskleidimo.“[439]

Pagal **ES ir ET teisę** duomenų saugumo pažeidimas, kuris gali turėti įtakos asmenų teisėms ir laisvėms, reiškia, kad duomenų valdytojas turi apie pažeidimą pranešti priežiūros institucijai (žr. 4.2.3 skirsnį).

Dažnai taip pat galioja pramoniniai, nacionaliniai ir tarptautiniai standartai, parengti būtent saugiam duomenų tvarkymui užtikrinti. Europos privatumo apsaugos ženklas („EuroPriSe“), pavyzdžiui, yra ES „eTEN“ (transeuropinių tinklų telekomunikacijų) projektas, kuriuo nagrinėjamos produktų, ypač programinės įrangos, sertifikavimo galimybės, be to, šis ženklas palengvina Europos duomenų apsaugos teisės

434 *Ten pat*, 32 straipsnio 1 punktas.

435 *Ten pat*, 32 straipsnio 1 dalies a punktas.

436 *Ten pat*, 32 straipsnio 1 dalies b punktas.

437 *Ten pat*, 32 straipsnio 1 dalies c punktas.

438 *Ten pat*, 32 straipsnio 1 dalies d punktas.

439 Atnaujintos 108-osios konvencijos 7 straipsnio 1 dalis.

laikymąsi. Europos tinklų ir informacijos apsaugos agentūra (ENISA) buvo įsteigta siekiant sustiprinti ES, ES valstybių narių ir verslo bendruomenės gebėjimus užkirsti kelią tinklų ir informacijos saugumo problemoms, jas spręsti ir į jas reaguoti[440]. ENISA reguliariai skelbia dabartinių saugumo grėsmių analizę ir pataria, kaip jas šalinti[441].

Duomenų saugumas užtikrinamas ne tik vietoje naudojant tinkamą aparatinę ir programinę įrangą. Duomenų saugumui užtikrinti taip pat reikalingos tinkamos vidaus organizacinės taisyklės. Tokiose taisyklėse idealiu atveju reikėtų aptarti šiuos klausimus:

- reguliarus darbuotojų informavimas apie duomenų saugumo taisykles ir jų prievoles pagal duomenų apsaugos teisę, visų pirma atsižvelgiant į jų pareigas išlaikyti konfidencialumą;

- aiškus prievolių pasiskirstymas ir aiškus kompetencijos sprendžiant duomenų tvarkymo klausimus nurodymas, visų pirma atsižvelgiant į sprendimus tvarkyti asmens duomenis ir perduoti duomenis trečiosioms šalims arba duomenų subjektams;

- asmens duomenų naudojimas tik laikantis kompetentingo asmens nurodymų arba visuotinai nustatytų taisyklių;

- prieigos prie duomenų valdytojo arba duomenų tvarkytojo vietų ir aparatinės bei programinės įrangos apsauga, įskaitant leidimo susipažinti su duomenimis patikrinimus;

- užtikrinimas, kad leidimus susipažinti su asmens duomenimis išduotų kompetentingas asmuo, ir reikalavimas, kad tokie leidimai būtų tinkamai fiksuojami dokumentuose;

- automatizuoti protokolai dėl elektroninės prieigos prie asmens duomenų ir vidaus priežiūros tarnybos reguliariai atliekami tokių protokolų patikrinimai (todėl reikia registruoti visą duomenų tvarkymo veiklą);

440 2013 m. gegužės 21 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 526/2013 dėl Europos Sąjungos tinklų ir informacijos apsaugos agentūros (ENISA), kuriuo panaikinamas Reglamentas (EB) Nr. 460/2004, OL L 165, 2013.

441 Pavyzdžiui, ENISA, (2016 m.), *Cyber Security and Resilience of smart cars*; geroji patirtis ir rekomendacijos; ENISA (2016 m.), *Security of Mobile Payments and Digital Wallets*.

- kruopštus kitų nei automatinė prieiga prie duomenų atskleidimo būdų dokumentavimas, kad būtų įrodyta, jog duomenys nebuvo perduoti neteisėtai.

Tinkamas darbuotojų mokymas ir švietimas duomenų saugumo tema taip pat yra veiksminga saugumo priemonių dalis. Be to, siekiant užtikrinti, kad tinkamos priemonės būtų nustatytos ne tik dokumentuose, bet ir įgyvendinamos bei taikomos praktikoje (pavyzdžiui, vidaus ar išorės auditas), turi būti nustatytos tikrinimo procedūros.

Priemonės, padedančios padidinti duomenų valdytojo arba duomenų tvarkytojo saugumo lygį, apima, pavyzdžiui, asmens duomenų apsaugos pareigūnus, darbuotojų švietimą saugumo klausimais, reguliarų auditą, skverbimosi testavimą ir kokybės antspaudus.

Pavyzdys. Byloje *I prieš Suomiją*[442] pareiškėja negalėjo įrodyti, kad kiti ligoninės, kurioje ji dirbo, darbuotojai neteisėtai susipažino su jos sveikatos įrašais. Todėl nacionaliniai teismai atmetė jos ieškinį dėl teisės į duomenų apsaugą pažeidimo. EŽTT nusprendė, kad buvo pažeistas EŽTK 8 straipsnis, nes ligoninių ligos istorijų registravimo sistema „buvo tokia, kad atgaline data nebuvo įmanoma išsiaiškinti, kas naudojosi paciento ligos istorija, nes joje buvo pateikiamos penkios vėliausios gydytojų išvados, be to, ši informacija buvo ištrinama iš karto, kai tik ligos istorija buvo perkeliama į archyvą“. EŽTT manymu, pagrindinė aplinkybė buvo ta, kad ligoninėje veikianti ligos istorijų sistema akivaizdžiai neatitiko nacionalinėje teisėje nustatytų teisinių reikalavimų, ir nacionaliniai teismai šios aplinkybės tinkamai neįvertino.

ES priėmė Direktyvą dėl tinklų ir informacinių sistemų saugumo (TIS direktyva)[443], kuri yra pirmoji ES masto kibernetinio saugumo teisinė priemonė. Direktyva siekiama, viena vertus, pagerinti kibernetinį saugumą nacionaliniu lygmeniu ir, kita vertus, padidinti bendradarbiavimą ES viduje. Joje taip pat nustatytos prievolės esminių paslaugų operatoriams (įskaitant energetikos, sveikatos, bankininkystės, transporto, skaitmeninės infrastruktūros ir kt. sektorių operatorius) ir skaitmeninių paslaugų teikėjams valdyti riziką, užtikrinti savo tinklų ir informacinių sistemų saugumą ir pranešti apie saugumo incidentus.

442 EŽTT, *I prieš Suomiją*, Nr. 20511/03, 2008 m. liepos 17 d.

443 2016 m. liepos 6 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti, OL L 194, 2016.

Ateities perspektyvos

2017 m. rugsėjo mėn. Europos Komisija pasiūlė reglamento, kuriuo siekiama reformuoti ENISA įgaliojimus, projektą, kad būtų atsižvelgta į naujas Agentūros kompetencijos sritis ir prievoles pagal TIS direktyvą. Siūlomo reglamento tikslas – plėtoti ENISA užduotis ir stiprinti jos, kaip „ES kibernetinio saugumo ekosistemos atskaitos taško“, vaidmenį[444]. Siūlomu reglamentu neturėtų būti daromas poveikis BDAR principams, o paaiškinant būtinus Europos kibernetinio saugumo sertifikavimo schemų elementus taip pat turėtų būti sustiprintas asmens duomenų saugumas. Be to, 2017 m. rugsėjo mėn. Europos Komisija pasiūlė įgyvendinimo reglamento projektą, kuriame nurodomi aspektai, į kuriuos skaitmeninių paslaugų teikėjai turi atsižvelgti, kad užtikrintų savo tinklų ir informacinių sistemų saugumą, kaip reikalaujama TIS direktyvos 16 straipsnio 8 dalyje. Rengiant vadovą, dėl šių dviejų pasiūlymų dar buvo diskutuojama.

4.2.2. Konfidencialumas

Pagal ES teisę BDAR pripažįstamas asmens duomenų konfidencialumas, kuris yra bendrojo principo sudedamoji dalis[445]. Viešai prieinamų elektroninių ryšių paslaugų teikėjai privalo užtikrinti konfidencialumą. Jie taip pat privalo užtikrinti savo paslaugų saugumą[446].

Pavyzdys. Draudimo bendrovės darbuotojui darbo metu paskambina asmuo, kuris teigia esąs bendrovės klientas, ir prašo pateikti informaciją apie jo draudimo sutartį.

Vykdydamas prievolę išsaugoti kliento duomenų konfidencialumą, darbuotojas, prieš atskleisdamas asmens duomenis, turi taikyti bent minimalias saugumo priemones. Tai, pavyzdžiui, galima padaryti pasiūlant perskambinti kliento draudimo sutartyje nurodytu telefonu.

444 Pasiūlymas dėl Europos Parlamento ir Tarybos reglamento dėl ENISA (Europos Sąjungos kibernetinio saugumo agentūros) ir informacinių ir ryšių technologijų kibernetinio saugumo sertifikavimo, kuriuo panaikinamas Reglamentas (ES) Nr. 526/2013 (Kibernetinio saugumo aktas), COM(2017) 477, 2017 m. rugsėjo 13 d., p. 6.

445 Bendrojo duomenų apsaugos reglamento 5 straipsnio 1 dalies f punktas.

446 Direktyvos dėl privatumo ir elektroninių ryšių 5 straipsnio 1 dalis.

Pagal 5 straipsnio 1 dalies f punktą asmens duomenys turi būti tvarkomi taip, kad būtų užtikrintas tinkamas asmens duomenų saugumas, įskaitant apsaugą nuo duomenų tvarkymo be leidimo arba neteisėto duomenų tvarkymo ir nuo netyčinio praradimo, sunaikinimo ar sugadinimo (vientisumo ir konfidencialumo principas).

Pagal 32 straipsnį duomenų valdytojas ir duomenų tvarkytojas privalo įgyvendinti technines ir organizacines priemones, kad užtikrintų aukšto lygio saugumą. Tokios priemonės, be kita ko, apima pseudonimų suteikimą asmens duomenims ir asmens duomenų šifravimą, gebėjimą nuolat užtikrinti duomenų tvarkymo konfidencialumą, vientisumą, prieinamumą ir atsparumą, priemonių vertinimą ir veiksmingumo testavimą, taip pat gebėjimą atkurti duomenų tvarkymą fizinio ar techninio incidento atveju. Be to, patvirtinto elgesio kodekso arba sertifikavimo mechanizmo laikymasis gali būti naudojamas kaip priemonė, kuria įrodoma atitiktis vientisumo ir konfidencialumo principui. Be to, pagal BDAR 28 straipsnį sutartyje, kurioje nustatomos duomenų tvarkytojo prievolės duomenų valdytojui, turi būti nustatyta, kad duomenų tvarkytojas užtikrina, kad asmens duomenis tvarkyti įgalioti asmenys būtų įsipareigoję užtikrinti konfidencialumą arba jiems būtų taikoma atitinkama įstatais nustatyta pareiga išlaikyti konfidencialumą.

Pareiga išlaikyti konfidencialumą negalioja tais atvejais, kai asmuo su asmens duomenimis susipažįsta kaip privatus asmuo, o ne duomenų valdytojo arba duomenų tvarkytojo darbuotojas. Šioje byloje BDAR 32 ir 28 straipsniai netaikomi, nes privačių asmenų asmens duomenų naudojimas visiškai nepatenka į reglamento taikymo sritį, jeigu tokiam naudojimui taikoma vadinamoji namų ūkio išimtis[447]. Pagal namų ūkio išimtį asmens duomenys naudojami, jeigu „duomenis tvarko fizinis asmuo, užsiimdamas išimtinai asmenine ar namų ūkio veikla“[448]. Po to, kai ESTT priėmė sprendimą byloje *Bodil Lindqvist*[449], ši išimtis vis dėlto turi būti aiškinama siaurai, visų pirma atsižvelgiant į duomenų atskleidimą. Namų ūkio išimtis visų pirma nebus taikoma asmens duomenų paskelbimui neribotam gavėjų internete skaičiui arba duomenų tvarkymui, kuriam būdingi profesiniai arba komerciniai aspektai (daugiau informacijos apie šį atvejį pateikiama 2.1.2, 2.2.2 ir 2.3.1 skirsniuose).

„Pranešimų konfidencialumas“ yra kitas konfidencialumo aspektas, kuriam taikomas *lex specialis*. Specialiose taisyklėse, kuriomis užtikrinamas elektroninių ryšių konfidencialumas pagal E. privatumo direktyvą, reikalaujama, kad valstybės narės

447 Bendrojo duomenų apsaugos reglamento 2 straipsnio 2 dalies c punktas.

448 *Ten pat*.

449 ESTT, C-101/01, *Baudžiamoji byla prieš Bodil Lindqvist*, 2003 m. lapkričio 6 d.

uždraustų visiems asmenims, išskyrus naudotojus, arba naudotojų sutikimo neturintiems asmenims klausytis, įrašinėti, saugoti arba kitais būdais perimti arba stebėti ryšius ir susijusius metaduomenis[450]. Nacionalinėje teisėje šio principo išimtys gali būti leidžiamos tik nacionalinio saugumo, gynybos, nusikaltimų prevencijos ar atskleidimo sumetimais ir tik tuo atveju, jei tokios priemonės yra būtinos ir proporcingos siekiamiems tikslams[451]. Tos pačios taisyklės bus taikomos pagal būsimą E. privatumo reglamentą, tačiau teisės akto dėl e. privatumo taikymo sritis bus praplėsta ir apims ne tik prieinamas elektroninių ryšių paslaugas, bet ir ryšius, atliekamus naudojant virštinklines paslaugas (pavyzdžiui, mobiliosiomis programomis).

ET teisėje pareiga išlaikyti konfidencialumą yra numanoma atsižvelgiant į atnaujintos 108-osios konvencijos 7 straipsnio 1 dalyje, kurioje aptariamas duomenų saugumas, minimą duomenų saugumo sąvoką.

Duomenų tvarkytojams konfidencialumas reiškia, kad jie negali be leidimo atskleisti duomenų trečiosioms šalims ar kitiems gavėjams. Duomenų valdytojo arba duomenų tvarkytojo darbuotojų pareiga išlaikyti konfidencialumą reiškia, kad jie asmens duomenis turi naudoti vadovaudamiesi tik savo kompetentingų vadovų nurodymais.

Pareiga išlaikyti konfidencialumą turi būti numatyta visose duomenų valdytojų ir duomenų tvarkytojų sudaromose sutartyse. Be to, duomenų valdytojai ir duomenų tvarkytojai turės imtis konkrečių priemonių, kad savo darbuotojams nustatytų teisinę pareigą išlaikyti konfidencialumą, kuri paprastai užtikrinama į darbuotojo darbo sutartį įtraukiant konfidencialumo sąlygas.

Profesinės pareigos išlaikyti konfidencialumą pažeidimas baudžiamas pagal baudžiamąją teisę daugumoje ES valstybių narių ir 108-osios konvencijos šalių.

4.2.3. Pranešimai apie asmens duomenų saugumo pažeidimus

Asmens duomenų saugumo pažeidimas reiškia saugumo pažeidimą, dėl kurio atsitiktinai arba neteisėtai sunaikinami, prarandami, pakeičiami arba be leidimo atskleidžiami tvarkomi asmens duomenys arba leidžiama su jais susipažinti[452]. Nors nau-

450 Direktyvos dėl privatumo ir elektroninių ryšių 5 straipsnio 1 dalis.

451 *Ten pat*, 15 straipsnio 1 punktas.

452 Bendrojo duomenų apsaugos reglamento 4 straipsnio 12 punktas; taip pat žr. 29 straipsnio darbo grupės (2017 m.) *Gaires dėl pranešimo apie asmens duomenų saugumo pažeidimą pagal Reglamentą (ES) 2016/679*, WP 250, 2017 m. spalio 3 d., p. 8.

jos technologijos, pavyzdžiui, šifravimas, dabar suteikia daugiau galimybių užtikrinti duomenų tvarkymo saugumą, duomenų saugumo pažeidimai vis dar yra paplitęs reiškinys. Duomenų saugumo pažeidimų priežastys gali būti įvairios, t. y. susijusios tiek su organizacijoje dirbančių asmenų klaidomis, tiek su išorės grėsmėmis, pavyzdžiui, įsilaužėliais ir kibernetinių nusikaltėlių organizacijomis.

Duomenų saugumo pažeidimai gali labai pakenkti asmenų, kurie dėl pažeidimo praranda savo asmens duomenų kontrolę, privatumo ir duomenų apsaugos teisėms. Pažeidimai gali lemti tapatybės vagystę ar sukčiavimą, finansinius nuostolius ar materialinę žalą, profesine paslaptimi saugomų asmens duomenų konfidencialumo praradimą ir žalą duomenų subjekto reputacijai. Savo gairėse dėl pranešimo apie asmens duomenų saugumo pažeidimus pagal Reglamentą 2016/679 29 straipsnio darbo grupė paaiškina, kad pažeidimai asmens duomenims gali turėti trejopą poveikį, t. y. duomenys gali būti atskleisti, prarasti ir (arba) pakeisti[453]. Be prievolės imtis priemonių duomenų tvarkymo saugumui užtikrinti, kaip paaiškinta 4.2 skirsnyje, lygiai taip pat svarbu užtikrinti, kad tais atvejais, kai padaromas pažeidimas, duomenų valdytojai juos tinkamai ir laiku pašalintų.

Priežiūros institucijos ir asmenys dažnai nežino apie duomenų saugumo pažeidimus, todėl asmenys negali imtis priemonių, kad apsisaugotų nuo tokių pažeidimų neigiamų pasekmių. Siekdami patvirtinti asmenų teises ir riboti duomenų saugumo pažeidimų poveikį, **ES ir ET** duomenų valdytojams nustato reikalavimą tam tikromis aplinkybėmis teikti pranešimą.

Pagal **ET** atnaujintą 108-ąją konvenciją susitariančiosios šalys privalo bent jau reikalauti iš duomenų valdytojų, kad jie praneštų kompetentingai priežiūros institucijai apie duomenų saugumo pažeidimus, dėl kurių gali būti gerokai apribotos duomenų subjektų teisės. Tokio pranešimo forma turėtų būti užpildyta „nedelsiant“[454].

ES teisėje nustatyta išsami tvarka, pagal kurią reglamentuojamas pranešimų pateikimo laikas ir turinys[455]. Atitinkamai duomenų valdytojai apie tam tikrus duomenų saugumo pažeidimus priežiūros institucijoms privalo pranešti nepagrįstai nedelsdami ir, kai įmanoma, per 72 valandas nuo to momento, kai sužinojo apie pažeidimą. Jeigu jie viršija 72 valandų terminą, prie pranešimo reikia pridėti paaiškinimą,

453 29 straipsnio darbo grupė (2017 m.), *Gairės dėl pranešimo apie asmens duomenų saugumo pažeidimą pagal Reglamentą (ES) 2016/679*, WP 250, 2017 m. spalio 3 d., p. 6.

454 Atnaujintos 108-osios konvencijos 7 straipsnio 2 dalis; atnaujintos 108-osios konvencijos aiškinamosios ataskaitos 64–66 punktai.

455 Bendrojo duomenų apsaugos reglamento 33 ir 34 straipsniai.

kuriame nurodomos vėlavimo priežastys. Duomenų valdytojai atleidžiami nuo reikalavimo pranešti tik tuo atveju, kai jie gali įrodyti, kad dėl duomenų saugumo pažeidimo greičiausiai nekils pavojus atitinkamų asmenų teisėms ir laisvėms.

Reglamente nurodyta būtiniausia informacija, kuri turi būti pateikiama pranešime, kad priežiūros institucija galėtų imtis reikalingų veiksmų[456]. Pranešime būtina bent jau pateikti duomenų saugumo pažeidimo pobūdžio ir kategorijų aprašymą, taip pat nurodyti apytikslį nukentėjusių duomenų subjektų skaičių, aprašyti galimas saugumo pažeidimo pasekmes ir duomenų valdytojo įgyvendintas priemones, padedančias pašalinti ir sumažinti pažeidimo pasekmes. Be to, reikėtų nurodyti duomenų apsaugos pareigūno arba kito kontaktinio asmens vardą ir pavardę bei kontaktus, kad kompetentinga priežiūros institucija prireikus galėtų gauti papildomos informacijos.

Jeigu tikėtina, kad duomenų saugumo pažeidimas kels didelį pavojų asmenų teisėms ir laisvėms, duomenų valdytojai privalo nedelsdami informuoti šiuos asmenis (duomenų subjektus) apie saugumo pažeidimą[457]. Informacija apie duomenų subjektus, įskaitant duomenų saugumo pažeidimo aprašymą, turi būti užrašyta aiškia ir suprantama kalba, be to, tokiame aprašyme pateikiama informacija, panaši į tą, kurios reikalaujama teikiant pranešimus priežiūros institucijoms. Tam tikromis aplinkybėmis duomenų valdytojams gali būti taikoma prievolės pranešti duomenų subjektams apie tokius pažeidimus išimtis. Išimtys taikomos tais atvejais, kai duomenų valdytojas įgyvendino tinkamas technines ir organizacines apsaugos priemones ir šios priemonės buvo taikomos asmens duomenims, kuriems poveikį darė asmens duomenų saugumo pažeidimas, visų pirma tai yra tokios priemonės, kurias taikant asmens duomenys tampa neatpažįstami bet kuriam asmeniui, kuris neturi leidimo su jais susipažinti, pavyzdžiui, šifravimas. Dėl veiksmų, kurių po pažeidimo imasi duomenų valdytojas, siekdamas užtikrinti, kad nebebūtų daroma žala duomenų subjektų teisėms, duomenų valdytojas taip pat gali būti atleidžiamas nuo prievolės pranešti duomenų subjektams. Galiausiai jeigu pranešimui parengti duomenų valdytojas turi įdėti neproporcingai daug pastangų, duomenų subjektai apie pažeidimą gali būti informuojami kitomis priemonėmis, pavyzdžiui, viešu skelbimu arba panašiomis priemonėmis[458].

456 *Ten pat*, 33 straipsnio 3 punktas.

457 *Ten pat*, 34 straipsnis.

458 *Ten pat*, 34 straipsnio 3 dalies c punktas.

Prievolė pranešti apie duomenų saugumo pažeidimus priežiūros institucijoms ir duomenų subjektams taikoma duomenų valdytojams. Tačiau duomenų saugumo pažeidimai gali būti padaromi nepaisant to, ar duomenis tvarko duomenų valdytojas, ar duomenų tvarkytojas. Dėl šios priežasties labai svarbu užtikrinti, kad duomenų tvarkytojai taip pat būtų įpareigoti pranešti apie duomenų saugumo pažeidimus. Šiuo atveju duomenų tvarkytojai privalo nedelsdami pranešti apie duomenų saugumo pažeidimus duomenų valdytojui[459]. Tuomet duomenų valdytojas privalo pranešti priežiūros institucijoms ir nukentėjusiems duomenų subjektams laikydamasis pirmiau minėtų taisyklių ir terminų.

4.3. Atskaitomybės taisyklės ir reikalavimų laikymosi skatinimas

Pagrindiniai faktai

- Siekdami užtikrinti atskaitomybę už asmens duomenų tvarkymą, duomenų valdytojai ir duomenų tvarkytojai privalo laikyti duomenų tvarkymo veiklos, už kurią jie atsako, įrašus ir pateikti juos priežiūros institucijoms paprašius.
- Bendrajame duomenų apsaugos reglamente nustatyta keletas priemonių, kuriomis skatinama laikytis reikalavimų:
  - duomenų apsaugos pareigūnų paskyrimas tam tikrose situacijose;
  - poveikio vertinimo atlikimas prieš pradedant duomenų tvarkymo veiklą, kuri, tikėtina, gali kelti didelę riziką asmenų teisėms ir laisvėms;
  - išankstinės konsultacijos su atitinkama priežiūros institucija, jeigu iš poveikio vertinimo matyti, kad duomenų tvarkymas kelia riziką, kurios negalima sumažinti;
  - duomenų valdytojams ir duomenų tvarkytojams skirti elgesio kodeksai, kuriuose nurodoma, kaip taikyti reglamentą įvairiuose duomenų tvarkymo sektoriuose;
  - sertifikavimo mechanizmai, atspaudai ir ženklai.
- ET teisėje siūlomos panašios priemonės, padedančios skatinti laikytis atnaujintos 108-osios konvencijos.

459 *Ten pat*, 33 straipsnio 2 punktas.

Atskaitomybės principas yra ypač svarbus siekiant garantuoti duomenų apsaugos taisyklių vykdymą Europoje. Duomenų valdytojas yra atsakingas už duomenų apsaugos taisyklių laikymąsi ir privalo sugebėti tai įrodyti. Atskaitomybė turėtų būti užtikrinama visada, o ne tik padarius pažeidimą. Iš tiesų, duomenų valdytojai turi „aktyvią" prievolę vadovautis tinkama duomenų valdymo politika visuose duomenų tvarkymo etapuose. Pagal Europos duomenų apsaugos teisės aktus reikalaujama, kad duomenų valdytojai įgyvendintų technines ir organizacines priemones, kuriomis užtikrinama, kad duomenys būtų tvarkomi laikantis teisės aktų, ir galėtų tai įrodyti. Tarp šių priemonių yra duomenų apsaugos pareigūnų paskyrimas, su duomenų tvarkymu susijusių įrašų ir dokumentų saugojimas ir poveikio privatumui vertinimas.

4.3.1. Duomenų apsaugos pareigūnai

Duomenų apsaugos pareigūnai (DAI) – tai duomenis tvarkančiose organizacijose dirbantys asmenys, kurie konsultuoja duomenų apsaugos taisyklių laikymosi klausimais. Jie yra esminis atskaitomybės pagrindas, nes padeda laikytis reikalavimų, taip pat veikia kaip priežiūros institucijų, duomenų subjektų ir organizacijos, kurioje jie paskirti, tarpininkai.

Pagal ES teisę, t. y. atnaujintos 108-osios konvencijos 10 straipsnio 1 dalį, duomenų valdytojams ir duomenų tvarkytojams nustatoma bendra prievolė užtikrinti atskaitomybę. Tam reikia, kad duomenų valdytojai ir duomenų tvarkytojai imtųsi visų tinkamų priemonių, kad laikytųsi Konvencijoje nustatytų duomenų apsaugos taisyklių ir sugebėtų įrodyti, kad jų kontroliuojamas duomenų tvarkymas atitinka Konvencijos nuostatas. Nors Konvencijoje nenustatytos konkrečios priemonės, kurias turėtų priimti duomenų valdytojai ir duomenų tvarkytojai, atnaujintos 108-osios konvencijos aiškinamojoje ataskaitoje nurodyta, kad DAP paskyrimas būtų viena iš galimų priemonių, padedančių įrodyti reikalavimų laikymąsi. Duomenų apsaugos pareigūnams reikėtų suteikti visas priemones, būtinas jų įgaliojimams vykdyti[460].

Kitaip nei ET teisėje, **Europos Sąjungoje** duomenų valdytojai ir duomenų tvarkytojai ne visada gali savo nuožiūra paskirti DAP, nes tam tikromis sąlygomis jį paskirti yra privaloma. BDAR pripažįstama, kad DAP atlieka pagrindinį vaidmenį naujoje valdymo sistemoje, ir pateikiamos išsamios nuostatos, susijusios su pareigūno paskyrimu, padėtimi, pareigomis ir užduotimis[461].

460 Atnaujintos 108-osios konvencijos aiškinamosios ataskaitos 87 punktas.

461 Bendrojo duomenų apsaugos reglamento 37–39 straipsniai.

Vadovaujantis BDAR, DAP privaloma paskirti trimis konkrečiais atvejais: kai duomenis tvarko valdžios institucija arba įstaiga; kai duomenų valdytojo arba duomenų tvarkytojo veikla apima duomenų tvarkymo operacijas, kurias duomenų subjektai turi reguliariai ir sistemiškai stebėti plačiu mastu, arba kai pagrindinę veiklą sudaro didelio masto specialių kategorijų duomenų arba asmens duomenų, susijusių su apkaltinamaisiais nuosprendžiais ir nusikalstamomis veikomis, tvarkymas dideliu mastu[462]. Nors tokios sąvokos kaip „sisteminga didelio masto stebėsena" ir „pagrindinė veikla" reglamente neapibrėžtos, 29 straipsnio darbo grupė paskelbė gaires, kaip jas reikėtų aiškinti[463].

Pavyzdys. Tikėtina, kad socialinių tinklų įmonės ir paieškos sistemos bus laikomos duomenų valdytojomis, kurių tvarkymo operacijos reikalauja reguliariai ir sistemingai dideliu mastu stebėti duomenų subjektus. Tokių įmonių verslo modelis yra pagrįstas didelio kiekio asmens duomenų tvarkymu ir jos, siūlydamos tikslinės reklamos paslaugas ir leisdamos įmonėms reklamuotis jų svetainėse, gauna nemažai pajamų. Tikslinė reklama – tai būdas rodyti reklamas, remiantis demografiniais duomenimis ir ankstesne vartotojų pirkimo istorija ar elgesiu. Todėl tam reikia sistemingai stebėti duomenų subjektų įpročius ir elgesį internete.

Pavyzdys. Ligoninė ir sveikatos priežiūros draudimo bendrovė yra tipiški duomenų valdytojų, kurių veiklą sudaro didelio masto specialių kategorijų asmens duomenų tvarkymas, pavyzdžiai. Duomenys, kuriais atskleidžiama informacija, susijusi su asmens sveikata, yra specialios kategorijos asmens duomenys pagal ET ir ES teisę, todėl jiems turi būti taikoma griežtesnė apsauga. ES teisėje genetiniai ir biometriniai duomenys taip pat pripažįstami specialiomis kategorijomis. Jeigu tokius duomenis dideliu mastu tvarko medicinos įstaigos ir draudimo bendrovės, jos pagal BDAR privalo paskirti duomenų apsaugos pareigūną.

Be to, BDAR 37 straipsnio 4 dalyje nustatyta, kad visais atvejais, išskyrus tris privalomus atvejus pagal 37 straipsnio 1 dalį, duomenų valdytojas, duomenų tvarkytojas arba asociacijos ir kitos įstaigos, atstovaujančios tam tikrų kategorijų duomenų

462 *Ten pat*, 37 straipsnio 1 punktas.

463 29 straipsnio darbo grupė (2017 m.), *Gairės dėl duomenų apsaugos pareigūnų (DAI)*, WP 243, 01 red., paskutinį kartą peržiūrėtos ir patvirtintos 2017 m. balandžio 5 d.

valdytojams arba duomenų tvarkytojams, gali arba, jei to reikalaujama pagal Sąjungos arba valstybės narės teisę, privalo paskirti duomenų apsaugos pareigūną.

Visos kitos organizacijos nėra teisiškai įpareigotos paskirti DAP. Tačiau BDAR nustatyta, kad duomenų valdytojai ir duomenų tvarkytojai gali savanoriškai nuspręsti paskirti DAP, kartu suteikiant galimybę valstybėms narėms nustatyti, kad tokius pareigūnus privalo paskirti ir kitų rūšių organizacijos nei tos, kurios numatytos reglamente[464].

Duomenų valdytojas, paskyręs DAP, privalo užtikrinti, kad jis „būtų tinkamai ir laiku įtraukiamas į visų su asmens duomenų apsauga susijusių klausimų nagrinėjimą" organizacijoje[465]. Pavyzdžiui, DAP turėtų dalyvauti teikiant konsultacijas dėl poveikio duomenų apsaugai vertinimo atlikimo ir įrašų apie duomenų tvarkymo veiklą organizacijoje sukūrimą ir laikymą. Kad DAP galėtų veiksmingai vykdyti savo užduotis, duomenų valdytojai ir duomenų tvarkytojai privalo jiems suteikti reikalingus išteklius, įskaitant pinigines lėšas, infrastruktūrą ir įrangą. Taip pat reikalaujama, kad DAP būtų duota pakankamai laiko jų funkcijoms įgyvendinti, be to, būtina užtikrinti nuolatinį DAP mokymą, kad jie galėtų kelti kompetenciją ir turėti naujausių žinių apie visus duomenų apsaugos teisės pokyčius[466].

BDAR nustatytos tam tikros pagrindinės garantijos, kuriomis užtikrinama, kad DAP veiktų nepriklausomai. Duomenų valdytojai ir duomenų tvarkytojai privalo užtikrinti, kad, vykdydami savo užduotis, susijusias su duomenų apsauga, DAP iš įmonės, įskaitant aukščiausio lygio vadovus, negautų jokių nurodymų. Be to, jie negali būti kaip nors atleidžiami iš darbo ar baudžiami už savo užduočių vykdymą[467]. Kaip pavyzdį galima pateikti atvejį, kai DAP pataria duomenų valdytojui arba duomenų tvarkytojui atlikti poveikio duomenų apsaugai vertinimą, nes, jo manymu, tikėtina, kad duomenų tvarkymas kels didelį pavojų duomenų subjektams. Įmonė neatsižvelgia į DAP patarimą ir nemano, kad jis yra pagrįstas, todėl nusprendžia neatlikti poveikio vertinimo. Įmonė gali nepaisyti patarimo, tačiau negali atleisti DAP arba jį nubausti už tokį patarimą.

464 Bendrojo duomenų apsaugos reglamento 37 straipsnio 3 ir 4 dalys.

465 *Ten pat*, 38 straipsnio 1 punktas.

466 29 straipsnio darbo grupė (2017 m.), *Gairės dėl duomenų apsaugos pareigūnų (DAI)*, WP 243, 01 red., paskutinį kartą peržiūrėtos ir patvirtintos 2017 m. balandžio 5 d., 3.1 punktas.

467 Bendrojo duomenų apsaugos reglamento 38 straipsnio 2 ir 3 dalys.

Galiausiai DAP užduotys ir pareigos išsamiai aprašytos BDAR 39 straipsnyje. Tai apima reikalavimus informuoti duomenis tvarkančias įmones ir darbuotojus apie jų pareigas pagal teisės aktus ir juos konsultuoti, taip pat atliekant auditą ir mokant duomenų tvarkymo operacijose dalyvaujančius darbuotojus stebėti, kaip laikomasi ES ir nacionalinių duomenų apsaugos taisyklių. DAP taip pat privalo bendradarbiauti su priežiūros institucija ir atlikti jos kontaktinio asmens funkcijas, susijusias su duomenų tvarkymo klausimais, pavyzdžiui, duomenų saugumo pažeidimais.

Kalbant apie ES institucijų ir įstaigų tvarkomus asmens duomenis, pažymėtina, kad Reglamente (EB) Nr. 45/2001 nustatyta, kad kiekviena Sąjungos institucija ir įstaiga privalo paskirti DAP. DAP pavesta užtikrinti, kad ES institucijose ir įstaigose būtų tinkamai taikomos reglamento nuostatos ir kad tiek duomenų subjektai, tiek duomenų valdytojai būtų informuojami apie jų teises ir pareigas[468]. Jis taip pat atsako į EDAPP prašymus ir prireikus su juo bendradarbiauja. Panašiai kaip ir BDAR, Reglamente (EB) Nr. 45/2001 yra nuostatų dėl DAP nepriklausomumo jiems vykdant savo užduotis ir būtinybės aprūpinti juos reikiamais darbuotojais ir ištekliais[469]. DAP turi būti pranešta prieš ES institucijai ar įstaigai (arba šių organizacijų departamentams) atliekant bet kokias duomenų tvarkymo operacijas, apie kurias pranešta, ir jie turi tvarkyti visų duomenų tvarkymo operacijų, apie kurias pranešta, registrą[470].

4.3.2. Duomenų tvarkymo veiklos įrašai

Kad įmonės galėtų įrodyti, jog laikosi reikalavimų, ir prisiimti atsakomybę, dažnai teisiškai reikalaujama, kad jos dokumentuotų ir registruotų savo veiklą. Svarbus pavyzdys – mokesčių teisė ir audito veikla, nes šiose srityse reikalaujama, kad visos įmonės tvarkytų ir laikytų didelį kiekį dokumentų ir įrašų. Kitose teisės srityse, visų pirma duomenų apsaugos teisėje, taip pat svarbu nustatyti panašius reikalavimus, nes įrašų laikymas yra svarbus būdas, palengvinantis duomenų apsaugos taisyklių laikymąsi. Todėl **ES teisėje** nustatyta, kad duomenų valdytojai arba jų atstovai privalo tvarkyti duomenų tvarkymo veiklos, už kurią jie atsako, įrašus[471]. Šia prievole siekiama užtikrinti, kad prireikus priežiūros institucijos turėtų reikiamus dokumentus ir galėtų patvirtinti duomenų tvarkymo teisėtumą.

468 Žr. Reglamento (EB) Nr. 45/2001 24 straipsnio 1 dalį, kurioje pateikiamas išsamus DAP užduočių sąrašas.

469 Reglamento (EB) Nr. 45/2001 24 straipsnio 6 ir 7 dalys.

470 *Ten pat*, 25 ir 26 straipsniai.

471 Bendrojo duomenų apsaugos reglamento 30 straipsnis.

Dokumentuose turi būti nurodoma ši informacija:

- duomenų valdytojo ir, kai taikoma, bendro duomenų valdytojo, duomenų valdytojo atstovo ir duomenų apsaugos pareigūno vardas, pavardė (pavadinimas) ir kontaktiniai duomenys;
- duomenų tvarkymo tikslai;
- duomenų subjektų kategorijų ir su duomenų tvarkymu susijusių asmens duomenų kategorijų aprašymas;
- informacija apie duomenų gavėjų, kuriems buvo arba bus atskleisti asmens duomenys, kategorijas;
- informacija apie tai, ar asmens duomenys buvo arba bus perduoti trečiosioms šalims arba tarptautinėms organizacijoms;
- jei įmanoma, numatomi įvairių kategorijų asmens duomenų ištrynimo terminai, taip pat techninių priemonių, priimtų siekiant užtikrinti duomenų tvarkymo saugumą, apžvalga[472].

Prievolė saugoti duomenų tvarkymo veiklos įrašus pagal BDAR taikoma ne tik duomenų valdytojams, bet ir duomenų tvarkytojams. Tai svarbus pokytis, nes prieš priimant reglamentą duomenų valdytojo ir duomenų tvarkytojo sudaryta sutartis pirmiausia apėmė duomenų tvarkytojo prievoles. Dabar jų prievolė saugoti duomenis yra tiesiogiai numatyta teisės aktuose.

BDAR numatyta šios prievolės išimtis. Reikalavimas saugoti įrašus netaikomas įmonei arba organizacijai (duomenų valdytojui arba duomenų tvarkytojui), kurioje dirba mažiau nei 250 darbuotojų. Tačiau šia išimtimi atitinkama organizacija gali pasinaudoti, tik jei ji nevykdo tokio duomenų tvarkymo, kuris gali kelti pavojų duomenų subjektų teisėms ir laisvėms, kai duomenys tvarkomi tik retkarčiais ir kai duomenų tvarkymas neapima specialių kategorijų duomenų, nurodytų 9 straipsnio 1 dalyje, arba asmens duomenų, susijusių su 10 straipsnyje nurodytais apkaltinamaisiais nuosprendžiais ir nusikalstamomis veikomis.

472 *Ten pat*, 30 straipsnio 1 punktas.

Duomenų tvarkymo veiklos įrašų laikymas turėtų sudaryti sąlygas duomenų valdytojams ir duomenų tvarkytojams įrodyti, kad jie laikosi reglamento. Tai taip pat turėtų sudaryti sąlygas priežiūros institucijoms stebėti duomenų tvarkymo teisėtumą. Jeigu priežiūros institucija prašo leisti susipažinti su šiais įrašais, duomenų valdytojai ir duomenų tvarkytojai privalo bendradarbiauti ir leisti su jais susipažinti.

4.3.3. Poveikio duomenų apsaugai vertinimas ir išankstinės konsultacijos

Duomenų tvarkymo operacijos yra neatsiejamos nuo asmenų teisėms būdingos rizikos. Asmens duomenys gali būti prarasti, atskleisti įgaliojimų neturinčioms šalims arba tvarkomi neteisėtai. Savaime suprantama, rizika priklauso nuo duomenų tvarkymo pobūdžio ir masto. Pavyzdžiui, didelio masto operacijos, susijusios su neskelbtinų duomenų tvarkymu, kelia daug didesnę riziką duomenų subjektams, palyginti su galima rizika, kai maža įmonė tvarko savo darbuotojų adresus ir asmeninius telefono numerius.

Kadangi atsiranda naujų technologijų ir duomenų tvarkymas tampa vis sudėtingesnis, duomenų valdytojai, prieš pradėdami duomenų tvarkymo operaciją, privalo išnagrinėti tikėtiną numatomo duomenų tvarkymo poveikį. Tai suteikia organizacijoms galimybę iš anksto tinkamai nustatyti, spręsti ir mažinti riziką, gerokai sumažinant neigiamo duomenų tvarkymo poveikio asmenims tikimybę.

Poveikio duomenų apsaugai vertinimas numatytas **tiek ET teisėje, tiek ES teisėje**. ET teisinėje sistemoje, t. y. atnaujintos 108-osios konvencijos 10 straipsnio 2 dalyje, nustatyta, kad susitariančiosios šalys privalo užtikrinti, kad duomenų valdytojai ir duomenų tvarkytojai „prieš pradėdami tokį duomenų tvarkymą išnagrinėtų tikėtiną numatomo duomenų tvarkymo poveikį duomenų subjektų teisėms ir pagrindinėms laisvėms“ ir, atlikę vertinimą, duomenis tvarkytų taip, kad būtų išvengta su duomenų tvarkymu susijusios rizikos arba kad ji būtų kuo mažesnė.

ES teisėje nustatyta panaši išsamesnė duomenų valdytojų prievolė, kuriai taikomas BDAR. 35 straipsnyje nustatyta, kad poveikio vertinimą būtina atlikti, kai tikėtina, kad dėl duomenų tvarkymo kils didelė rizika asmenų teisėms ir laisvėms. Reglamente neapibrėžiama, kaip turi būti vertinama rizikos tikimybė, bet nurodoma, kokie tai gali būti rizikos veiksniai[473]. Jame pateikiamas duomenų tvarkymo operacijų,

473 Bendrojo duomenų apsaugos reglamento preambulės 75 konstatuojamoji dalis.

kurios laikomos keliančiomis didelę riziką ir kurių atžvilgiu ypač reikalingas išankstinis poveikio vertinimas, sąrašas, t. y. tais atvejais, kai:

- asmens duomenys tvarkomi siekiant priimti sprendimus dėl fizinių asmenų, atlikus bet kokį sisteminį ir plataus masto su asmenimis susijusių asmeninių aplinkybių vertinimą (profiliavimas);

- dideliu mastu tvarkomi neskelbtini duomenys arba asmens duomenys, susiję su apkaltinamaisiais nuosprendžiais ir nusikalstamomis veikomis;

- duomenų tvarkymas yra susijęs su didelio masto sistemine viešai prieinamų vietų stebėsena.

Priežiūros institucijos privalo patvirtinti ir paskelbti sąrašą tų asmens duomenų tvarkymo operacijų, dėl kurių reikia atlikti poveikio vertinimą. Jos taip pat gali sudaryti duomenų tvarkymo operacijų, kurioms šis įpareigojimas netaikomas, sąrašą[474].

Jeigu reikalaujama atlikti poveikio vertinimą, duomenų valdytojai privalo įvertinti duomenų tvarkymo būtinumą ir proporcingumą, taip pat galimą riziką asmenų teisėms. Poveikio vertinime taip pat turi būti nurodytos planuojamos saugumo priemonės nustatytai rizikai pašalinti. Siekdamos nustatyti sąrašus, valstybių narių priežiūros institucijos turi bendradarbiauti tarpusavyje ir su Europos duomenų apsaugos valdyba. Taip visoje ES bus užtikrintas nuoseklus požiūris į tas operacijas, kurioms reikia atlikti poveikio vertinimą, o duomenų valdytojams, neatsižvelgiant į jų buvimo vietą, bus taikomi panašūs reikalavimai.

Jeigu atlikus poveikio vertinimą paaiškėja, kad duomenų tvarkymas kels didelę riziką asmenų teisėms ir nebuvo nustatyta jokių rizikos mažinimo priemonių, duomenų valdytojas, prieš pradėdamas duomenų tvarkymo operaciją, privalo konsultuotis su atitinkama priežiūros institucija[475].

29 straipsnio darbo grupė paskelbė gaires dėl poveikio duomenų apsaugai vertinimo ir kaip nustatyti, ar duomenų tvarkymas gali kelti didelę riziką[476]. Ji parengė

474 *Ten pat*, 35 straipsnio 4 ir 5 dalys.

475 *Ten pat*, 36 straipsnio 1 dalis; 29 straipsnio darbo grupė (2017 m.), *Gairės dėl poveikio duomenų apsaugai vertinimo (PDAV) ir kaip nustatyti, ar duomenų tvarkymas „gali kelti didelį pavojų" pagal Reglamentą 2016/679*, WP 248, 01 red., Briuselis, 2017 m. spalio 4 d.

476 29 straipsnio darbo grupė (2017 m.), *Gairės dėl poveikio duomenų apsaugai vertinimo (PDAV) ir kaip nustatyti, ar duomenų tvarkymas „gali kelti didelį pavojų" pagal Reglamentą 2016/679*, WP 48, 01 red., Briuselis, 2017 m. spalio 4 d.

devynis kriterijus, kurie padeda nustatyti, ar konkrečiu atveju reikia atlikti poveikio duomenų apsaugai vertinimą[477]: 1) vertinimas arba balų skyrimas; 2) automatizuotas sprendimų priėmimas, turintis teisinį ar panašų reikšmingą poveikį; 3) sisteminga stebėsena; 4) neskelbtini duomenys; 5) dideliu mastu tvarkomi duomenys; 6) duomenų rinkiniai, kurie buvo suderinti arba sujungti; 7) duomenys apie pažeidžiamus duomenų subjektus; 8) naujoviškas naudojimas arba technologinių ar organizacinių sprendimų taikymas; 9) kai pats duomenų tvarkymas „užkerta kelią duomenų subjektams naudotis teise arba naudotis paslauga ar sutartimi“. 29 straipsnio darbo grupė nustatė pagrindinę taisyklę, pagal kurią duomenų tvarkymo operacijos, kurios atitinka mažiau nei du kriterijus, kelia mažesnę riziką ir dėl jos nereikia atlikti poveikio duomenų apsaugai vertinimo, o jeigu operacija atitinka du ar daugiau kriterijų, dėl jos reikės atlikti tokį vertinimą. Tais atvejais, kai neaišku, ar reikia atlikti poveikio duomenų apsaugai vertinimą, 29 straipsnio darbo grupė rekomenduoja atlikti tokį vertinimą, nes tai yra „naudinga priemonė, padedanti duomenų valdytojams laikytis duomenų apsaugos teisės aktų“[478]. Jeigu naudojama nauja duomenų tvarkymo technologija, svarbu, kad poveikio duomenų apsaugai vertinimas būtų atliktas[479].

4.3.4. Elgesio kodeksai

Elgesio kodeksai skirti naudoti tam tikruose pramonės sektoriuose, siekiant apibrėžti ir patikslinti BDAR taikymą tuose konkrečiuose sektoriuose. Asmens duomenų valdytojai ir tvarkytojai, kurie kuria tokius kodeksus, gali gerokai pagerinti reikalavimų laikymąsi ir sustiprinti ES duomenų apsaugos taisyklių įgyvendinimą. Sektoriaus narių specialiosios žinios padės rasti praktinius sprendimus, kurių, tikėtina, bus paisoma. BDAR pripažįstama tokių kodeksų svarba veiksmingai taikant duomenų apsaugos teisę, be to, valstybės narės, priežiūros institucijos, Komisija ir Europos duomenų apsaugos valdyba raginamos skatinti elgesio kodeksų, kuriais būtų prisidedama prie tinkamo reglamento taikymo visoje ES, rengimą[480]. Kodeksuose galėtų būti aptartas reglamento taikymas konkrečiuose sektoriuose, įskaitant tokius klausimus kaip asmens duomenų rinkimas, duomenų subjektams ir visuomenei teiktina informacija ir naudojimasis duomenų subjektų teisėmis.

Siekiant užtikrinti, kad elgesio kodeksai atitiktų BDAR nustatytas taisykles, juos pirmiausia reikia pateikti kompetentingai priežiūros institucijai ir tik paskui patvirtinti.

477 *Ten pat*, p. 9–11.

478 *Ten pat*, p. 9.

479 *Ten pat*.

480 Bendrojo duomenų apsaugos reglamento 40 straipsnio 1 punktas.

Tada priežiūros institucija parengia nuomonę, ar pateiktas kodekso projektas padeda laikytis reglamento, ir nustačiusi, kad kodekse numatytos tinkamos apsaugos priemonės, jį patvirtina[481]. Priežiūros institucijos privalo paskelbti patvirtintus elgesio kodeksus, taip pat kriterijus, kuriais remdamosi jos tai padarė. Jeigu elgesio kodekso projektas yra susijęs su duomenų tvarkymo veikla keliose valstybėse narėse, kompetentinga priežiūros institucija prieš patvirtindama kodekso projektą, jo pakeitimą ar taikymo srities praplėtimą, pateikia jį Europos duomenų apsaugos valdybai, kuri pateikia nuomonę dėl kodekso atitikties BDAR. Komisija, priimdama įgyvendinimo aktus, gali nuspręsti, kad jai pateiktas patvirtintas elgesio kodeksas galioja visoje Sąjungoje.

Elgesio kodekso laikymasis yra visokeriopai naudingas duomenų subjektams, duomenų valdytojams ir duomenų tvarkytojams. Tokiuose kodeksuose pateikiamos išsamios rekomendacijos, kurios padeda pritaikyti teisinį reikalavimą prie konkrečių sektorių specifikos ir dar labiau padidinti duomenų tvarkymo veiklos skaidrumą. Duomenų valdytojai ir duomenų tvarkytojai laikydamiesi kodeksų taip pat gali įrodyti, kad jie laikosi ES teisės ir taip visuomenėje formuoja savo, kaip organizacijų, kurios, vykdydamos duomenų tvarkymo operacijas, pirmenybę teikia duomenų apsaugai ir įsipareigoja ją užtikrinti, įvaizdį. Patvirtinti elgesio kodeksai kartu su privalomais ir vykdytinais įsipareigojimais gali būti naudojami kaip tinkamos apsaugos priemonės perduodant duomenis trečiosioms šalims. Siekiant užtikrinti, kad organizacija iš tikrųjų laikytųsi elgesio kodeksų, gali būti paskiriama speciali įstaiga (kuriai akreditaciją suteikė atitinkama priežiūros institucija), kuri stebėtų ir užtikrintų kodekso laikymąsi. Kad galėtų vykdyti savo užduotis, įstaiga turi būti nepriklausoma, turėti kompetencijų elgesio kodekso reguliuojamais klausimais ir nustatytas skaidrumo procedūras bei struktūrą, kad galėtų nagrinėti skundus dėl kodekso pažeidimo[482].

Pagal **ET teisę**, t. y. atnaujintoje 108-ojoje konvencijoje, nustatyta, kad nacionalinėje teisėje garantuojamas duomenų apsaugos lygis gali būti naudingai sustiprintas numatant savanoriškas reguliavimo priemones, pavyzdžiui, gerosios patirties kodeksus arba profesinio elgesio kodeksus. Tačiau pagal atnaujintą 108-ąją konvenciją tai yra tik savanoriškos priemonės: tokių priemonių nustatymas negali būti grindžiamas kokia nors teisine prievole, tačiau jos yra rekomenduojamos, be to, bet

481 *Ten pat*, 40 straipsnio 5 punktas.

482 *Ten pat*, 41 straipsnio 1 ir 2 dalys.

kokios tokios priemonės pačios savaime nėra pakankamos siekiant užtikrinti visišką atitiktį Konvencijai[483].

4.3.5. Sertifikavimas

Be elgesio kodeksų, sertifikavimo mechanizmai ir duomenų apsaugos antspaudai ir ženklai yra kitos priemonės, kurias naudodami duomenų valdytojai ir duomenų tvarkytojai gali įrodyti BDAR reikalavimų laikymąsi. Šiuo tikslu reglamente nustatyta savanoriška sertifikavimo sistema, kuria naudodamosi tam tikros įstaigos arba priežiūros institucijos gali išduoti sertifikatus. Duomenų valdytojai ir duomenų tvarkytojai, kurie nusprendžia naudoti sertifikavimo mechanizmą, gali būti labiau matomi ir įgyti daugiau patikimumo, nes sertifikatai, antspaudai ir ženklai sudaro sąlygas duomenų subjektams greitai įvertinti organizacijos apsaugos lygį duomenų tvarkymo srityje. Svarbu tai, jog dėl turimo tokio sertifikato nesumažėja duomenų valdytojų arba duomenų tvarkytojų pareigos ir atsakomybė laikytis visų reglamento reikalavimų.

4.4. Pritaikytoji ir standartizuotoji duomenų apsauga

Pritaikytoji duomenų apsauga

ES teisėje reikalaujama, kad duomenų valdytojai nustatytų veiksmingas duomenų apsaugos principų įgyvendinimo priemones ir integruotų būtinas apsaugos priemones, kad įvykdytų reglamento reikalavimus ir apsaugotų duomenų subjektų teises[484]. Šios priemonės turėtų būti įgyvendinamos tvarkant duomenis ir nustatant duomenų tvarkymo priemones. Įgyvendindamas šias priemones, duomenų valdytojas turi atsižvelgti į techninių galimybių išsivystymo lygį, įgyvendinimo sąnaudas bei duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, taip pat į duomenų subjekto teisėms ir laisvėms kylančią riziką ir tokios rizikos rimtumą[485].

483 Atnaujintos 108-osios konvencijos aiškinamosios ataskaitos 33 punktas.

484 Bendrojo duomenų apsaugos reglamento 25 straipsnio 1 punktas.

485 Žr. 29 straipsnio darbo grupės (2017 m.) *Gaires dėl poveikio duomenų apsaugai vertinimo (PDAV) ir kaip nustatyti, ar duomenų tvarkymas „gali kelti didelį pavojų" pagal Reglamentą 2016/679*, WP 248, pirma red., 2017 m. spalio 4 d. Taip pat žr. ENISA (2015 m.), *Privacy and Data Protection by Design-from policy to engineering*, 2015 m. sausio 12 d.

Pagal **ET teisę** reikalaujama, kad duomenų valdytojai ir duomenų tvarkytojai prieš pradėdami tvarkyti duomenis įvertintų tikėtiną asmens duomenų tvarkymo poveikį duomenų subjektų teisėms ir laisvėms. Be to, duomenų valdytojai ir duomenų tvarkytojai privalo nustatyti tokią duomenų tvarkymo struktūrą, kad būtų užkirstas kelias tų teisių ir laisvių apribojimo rizikai arba kad ji būtų kuo labiau sumažinta, ir įgyvendinti technines ir organizacines priemones, kuriose būtų atsižvelgiama į pasekmes teisei į asmens duomenų apsaugą visais duomenų tvarkymo etapais[486].

Standartizuotoji duomenų apsauga

Pagal **ES teisę** reikalaujama, kad duomenų valdytojas įgyvendintų priemones, kuriomis užtikrinama, kad standartizuotoji duomenų apsauga būtų taikoma tik tiems asmens duomenims, kuriuos būtina tvarkyti atsižvelgiant į numatytus tikslus. Ši prievolė taikoma surinktų asmens duomenų kiekiui, duomenų tvarkymo mastui, saugojimo laikotarpiui ir galimybei susipažinti[487]. Tokia priemone turi būti užtikrinama, pavyzdžiui, kad ne visi duomenų valdytojo darbuotojai turėtų galimybę susipažinti su duomenų subjektų asmens duomenimis. Išsamesnes EDAPP parengtas rekomendacijas galima rasti *Būtinumo vertinimo priemonių rinkinyje*[488].

Pagal **ET teisę** reikalaujama, kad duomenų valdytojai ir duomenų tvarkytojai įgyvendintų technines ir organizacines priemones, kad išnagrinėtų teisės į duomenų apsaugą poveikį ir įgyvendintų technines ir organizacines priemones, kuriose būtų atsižvelgiama į pasekmes teisei į asmens duomenų apsaugą visais duomenų tvarkymo etapais[489].

2016 m. ENISA paskelbė ataskaitą apie prieinamas privatumo priemones ir paslaugas[490]. Be kita ko, šiame vertinime pateikiama kriterijų ir parametrų, kurie yra geros arba prastos privatumo praktikos rodikliai, rodyklė. Kai kurie kriterijai yra tiesiogiai susiję su BDAR nuostatomis, pavyzdžiui, pseudonimų suteikimo ir patvirtintų sertifikavimo mechanizmų naudojimas, o kiti kriterijai yra naujoviškos iniciatyvos, kuriomis

486 Atnaujintos 108-osios konvencijos 10 straipsnio 2 ir 3 dalys, atnaujintos 108-osios konvencijos aiškinamosios ataskaitos 89 punktas.

487 Bendrojo duomenų apsaugos reglamento 25 straipsnio 2 dalis.

488 Europos duomenų apsaugos priežiūros pareigūnas (EDAPP) (2017), *Būtinumo vertinimo priemonių rinkinys*, Briuselis, 2017 m. balandžio 11 d.

489 Atnaujintos 108-osios konvencijos 10 straipsnio 3 dalis, atnaujintos 108-osios konvencijos aiškinamosios ataskaitos 89 punktas.

490 ENISA, *PETs controls matrix: A systematic approach for assessing online and mobile privacy tools*, 2016 m. gruodžio 20 d.

siekiama užtikrinti pritaikytąją ir standartizuotąją privatumo apsaugą. Pavyzdžiui, naudojimo kriterijus, kuris nėra tiesiogiai susijęs su privatumu, gali padidinti privatumą, nes gali sudaryti sąlygas plačiau taikyti privatumo priemonę ar paslaugą. Iš tiesų, privatumo priemonių, kurias sunku praktiškai įgyvendinti, įdiegimo lygis plačiojoje visuomenėje gali būti labai žemas, net jei jos suteikia labai tvirtas privatumo garantijas. Be to, itin svarbus privatumo priemonės brandos ir stabilumo kriterijus, t. y. tai, kaip priemonė ilgainiui kinta ir kaip ji reaguoja į esamus ar naujus iššūkius, susijusius su privatumu. Kitos privatumą didinančios technologijos, pavyzdžiui, saugaus ryšio srityje, apima ištisinį šifravimą (ryšį, kai pranešimus gali skaityti tik bendraujantys asmenys); kliento ir serverio šifravimą (tarp kliento ir serverio sukurto ryšio kanalo šifravimas); autentiškumo patvirtinimą (bendraujančių šalių tapatybės tikrinimas) ir anoniminį bendravimą (jokia trečioji šalis negali nustatyti bendraujančių šalių).

5 Nepriklausoma priežiūra

ES	Reglamentuojami klausimai	ET
Chartijos 8 straipsnio 3 dalis Sutarties dėl ES veikimo 16 straipsnio 2 dalis Bendrojo duomenų apsaugos reglamento 51–59 straipsniai ESTT, C-518/07, *Europos Komisija prieš Vokietijos Federacinę Respubliką* (DK), 2010 m. ESTT, C-614/10, *Europos Komisija prieš Austriją* (DK), 2012 m. ESTT, C-288/12, *Europos Komisija prieš Vengriją* (DK), 2014 m. ESTT, C-362/14, *Maximilian Schrems prieš Data Protection Commissioner* (DK), 2015 m.	**Priežiūros institucijos**	Atnaujintos 108-osios konvencijos 15 straipsnis
Bendrojo duomenų apsaugos reglamento 60–67 straipsniai	**Priežiūros institucijų bendradarbiavimas**	Atnaujintos 108-osios konvencijos 16–21 straipsniai
Bendrojo duomenų apsaugos reglamento 68–76 straipsniai	**Europos duomenų apsaugos valdyba**	

Pagrindiniai faktai

- Nepriklausoma priežiūra yra esminis Europos duomenų apsaugos teisės elementas, numatytas Chartijos 8 straipsnio 3 dalyje.
- Siekiant užtikrinti veiksmingą duomenų apsaugą, pagal nacionalinę teisę būtina sukurti nepriklausomas priežiūros institucijas.
- Priežiūros institucijos privalo veikti visiškai nepriklausomai ir tai turi būti garantuojama įstatyme, kuriuo įsteigiama institucija, ir atsispindėti konkrečioje priežiūros institucijos organizacinėje struktūroje.
- Priežiūros institucijos turi konkrečius įgaliojimus ir užduotis. Tai, be kita ko, apima:
  - duomenų apsaugos stebėseną ir skatinimą nacionaliniu lygmeniu;
  - duomenų subjektų ir duomenų valdytojų, taip pat vyriausybės ir plačiosios visuomenės konsultavimą;
  - skundų nagrinėjimą ir pagalbą duomenų subjektams, susijusią su tariamais duomenų apsaugos teisių pažeidimais;
  - duomenų valdytojų ir duomenų tvarkytojų priežiūrą.
- Priežiūros institucijos taip pat turi įgaliojimus įsikišti, jei tai būtina, ir taikyti šias priemones:
  - įspėti duomenų valdytojus ir duomenų tvarkytojus, pareikšti jiems papeikimą ar net skirti baudas;
  - nurodyti ištaisyti, užblokuoti arba ištrinti duomenis;
  - uždrausti tvarkyti duomenis arba skirti administracinę nuobaudą;
  - perduoti klausimus spręsti teismui.
- Kadangi tvarkant asmens duomenis dažnai dalyvauja duomenų valdytojai, duomenų tvarkytojai ir duomenų subjektai iš skirtingų valstybių, reikalaujama, kad priežiūros institucijos bendradarbiautų tarpusavyje tarpvalstybiniais klausimais ir užtikrintų veiksmingą asmenų apsaugą Europoje.
- ES lygmeniu Bendrajame duomenų apsaugos reglamente nustatytas vieno langelio principu grindžiamas tarpvalstybinių duomenų tvarkymo bylų mechanizmas. Kai kurios įmonės vykdo tarpvalstybinę duomenų tvarkymo veiklą, nes asmens duomenis, vykdydami savo veiklą, tvarko daugiau nei vienoje valstybėje narėje esantys padaliniai arba juos tvarko vienas padalinys Sąjungoje, tačiau tai daro didelį poveikį duomenų subjektams daugiau nei vienoje valstybėje narėje. Taikant mechanizmą, tokios įmonės turės bendrauti tik su viena nacionaline duomenų apsaugos priežiūros institucija.

- Bendradarbiavimo ir nuoseklumo užtikrinimo mechanizmas sudaro sąlygas laikytis koordinuoto požiūrio tarp visų su byla susijusių priežiūros institucijų. Vadovaujanti pagrindinės arba vienintelės buveinės priežiūros institucija konsultuosis su kitomis susijusiomis priežiūros institucijomis ir pateiks savo sprendimo projektą.
- Panašiai kaip ir dabartinėje 29 straipsnio darbo grupėje, kiekvienos valstybės narės priežiūros institucija ir Europos duomenų apsaugos priežiūros pareigūnas (EDAPP) dalyvauja Europos duomenų apsaugos valdyboje.
- Europos duomenų apsaugos valdybos užduotys, pavyzdžiui, apima teisingo reglamento taikymo stebėseną, Komisijos konsultavimą įvairiais klausimais ir nuomonių, rekomendacijų arba gerosios patirties įvairiomis temomis priėmimą.
- Pagrindinis skirtumas yra tas, kad Europos duomenų apsaugos valdyba ne tik rengia nuomones, kaip tai buvo numatyta Direktyvoje 95/46/EB. Ji taip pat priima privalomus sprendimus tais atvejais, kai priežiūros institucija pareiškė svarbų ir pagrįstą prieštaravimą pagal vieno langelio mechanizmą; kai yra prieštaringų nuomonių dėl to, kuri priežiūros institucija yra vadovaujanti, ir galiausiai kai kompetentinga priežiūros institucija neprašo EDAV nuomonės arba nesivadovauja priimta EDAV nuomone. Taip siekiama užtikrinti nuoseklų reglamento taikymą visose valstybėse narėse.

Nepriklausoma priežiūra yra esminis Europos duomenų apsaugos teisės elementas. Tiek ES, tiek ET teisėje nepriklausomų priežiūros institucijų veikimas laikomas būtinu siekiant veiksmingai apsaugoti asmenų teises ir laisves tvarkant jų asmens duomenis. Kadangi duomenų tvarkymas šiuo metu nuolat vyksta ir asmenims tampa vis sunkiau jį suprasti, šios institucijos yra skaitmeninio amžiaus sergėtojos. ES nepriklausomų priežiūros institucijų buvimas laikomas vienu iš svarbiausių pirminėje ES teisėje įtvirtintos teisės į asmens duomenų apsaugą aspektų. ES pagrindinių teisių chartijos 8 straipsnio 3 dalyje ir SESV 16 straipsnio 2 dalyje asmens duomenų apsauga pripažįstama kaip pagrindinė teisė ir patvirtinama, kad duomenų apsaugos taisyklių laikymąsi privalo kontroliuoti nepriklausoma institucija.

Teismų praktikoje taip pat pripažinta nepriklausomos duomenų apsaugos teisės priežiūros svarba.

Pavyzdys. Byloje *Schrems*[491] ESTT nagrinėjo klausimą, ar asmens duomenų perdavimas Jungtinėms Amerikos Valstijoms (JAV) pagal pirmąjį ES ir JAV „saugaus uosto“ susitarimą atitiko ES duomenų apsaugos teisę atsižvelgiant į Edwardo Snowdeno atskleistą informaciją apie JAV nacionalinės saugumo agentūros vykdomą masinį sekimą. Asmens duomenų perdavimas į JAV

491 ESTT, C-362/14, *Maximillian Schrems prieš Data Protection Commissioner* (DK), 2015 m. spalio 6 d.

buvo pagrįstas 2000 m. Europos Komisijos priimtu sprendimu, pagal kurį asmens duomenis iš ES buvo leidžiama perduoti JAV organizacijoms, kurios pagal „saugaus uosto“ schemą pačios išdavė sau sertifikatą, remiantis tuo, kad pagal schemą užtikrinamas tinkamas asmens duomenų apsaugos lygis. Gavusi prašymą ištirti pareiškėjo skundą dėl duomenų perdavimo teisėtumo po E. Snowdeno atskleistos informacijos, Airijos priežiūros institucija atmetė skundą motyvuodama tuo, kad dėl to, jog Komisija priėmė sprendimą dėl JAV duomenų apsaugos sistemos tinkamumo pagal „saugaus uosto“ principus (toliau – „saugaus uosto“ sprendimas), ji negalėjo toliau nagrinėti skundo.

Tačiau ESTT nusprendė, kad Komisijos sprendimo, pagal kurį buvo leidžiama perduoti duomenis trečiosioms šalims, kurios užtikrina tinkamą apsaugos lygį, buvimas nereiškia, kad nacionalinių priežiūros institucijų įgaliojimai yra panaikinti arba sumažinti. ESTT pažymėjo, kad šių institucijų įgaliojimai stebėti ir užtikrinti atitiktį ES duomenų apsaugos taisyklėms kildinami iš ES pirminės teisės, visų pirma Chartijos 8 straipsnio 3 dalies ir SESV 16 straipsnio 2 dalies. „[N]epriklausomų priežiūros institucijų įsteigimas valstybėse narėse yra esminis asmenų apsaugos tvarkant asmens duomenis elementas“[492].

Todėl ESTT nusprendė, kad net jeigu asmens duomenys buvo perduoti pagal Komisijos sprendimą dėl tinkamumo, tuo atveju, kai skundas pateikiamas nacionalinei priežiūros institucijai, ji skundą privalo kruopščiai išnagrinėti. Priežiūros institucija gali atmesti skundą, jeigu nustato, kad jis yra nepagrįstas. Tokiu atveju ESTT pabrėžė, kad teisė į veiksmingą teisinę gynybą reikalauja, kad asmenys galėtų ginčyti tokį sprendimą nacionaliniuose teismuose, kurie gali kreiptis į ESTT su prašymu priimti prejudicinį sprendimą dėl Komisijos sprendimo galiojimo. Jeigu priežiūros institucija mano, kad skundas yra pagrįstas, ji privalo sugebėti dalyvauti teisminiame procese ir iškelti bylą dėl klausimo nacionaliniuose teismuose. Nacionaliniai teismai gali perduoti bylą ESTT, nes tai yra vienintelė įstaiga, turinti įgaliojimus priimti sprendimą, susijusį su Komisijos sprendimo dėl tinkamumo galiojimu[493].

Tuomet ESTT, siekdamas nustatyti, ar duomenų perdavimo sistema atitiko ES duomenų apsaugos taisykles, nagrinėjo „saugaus uosto“ sprendimo galiojimą. Jis nustatė, kad „saugaus uosto“ sprendimo 3 straipsniu buvo apriboti

492 ESTT, C-362/14, *Maximillian Schrems prieš Data Protection Commissioner* (DK), 2015 m. spalio 6 d., 41 punktas.

493 *Ten pat*, 53–66 punktai.

nacionalinių priežiūros institucijų įgaliojimai (nustatyti Duomenų apsaugos direktyvoje) imtis veiksmų siekiant užkirsti kelią duomenų perdavimui tuo atveju, kai JAV užtikrinamas asmens duomenų apsaugos lygis nebuvo pakankamas. Atsižvelgdamas į nepriklausomų priežiūros institucijų svarbą užtikrinant atitiktį duomenų apsaugos teisei, ESTT nusprendė, kad pagal Duomenų apsaugos direktyvą, skaitant ją kartu su Chartija, Komisija neturėjo teisės taip apriboti nepriklausomos priežiūros institucijos įgaliojimų. Priežiūros institucijų įgaliojimų apribojimai buvo viena iš priežasčių, kuria remdamasis ESTT pripažino „saugaus uosto“ sprendimą negaliojančiu.

Todėl pagal Europos teisę reikalaujama nepriklausoma priežiūra, nes ji yra svarbus veiksmingos duomenų apsaugos užtikrinimo mechanizmas. Nepriklausomos priežiūros institucijos yra pirmieji kontaktiniai centrai, į kuriuos kreipiasi duomenų subjektai privatumo pažeidimų atveju[494]. Pagal ES ir ET teisę priežiūros institucijas įsteigti privaloma. Abiejose teisinėse sistemose šių institucijų užduotys ir įgaliojimai aprašomi panašiai kaip BDAR. Todėl priežiūros institucijos iš esmės turėtų veikti taip pat tiek pagal ES teisę, tiek pagal ET teisę[495].

5.1. Nepriklausomumas

Pagal **ES teisę** ir **ET teisę** reikalaujama, kad priežiūros institucija, vykdydama savo užduotis ir įgyvendindama įgaliojimus, veiktų visiškai nepriklausomai[496]. Priežiūros institucijos ir jos narių, taip pat darbuotojų nepriklausomumas nuo tiesioginės ar netiesioginės išorės įtakos yra labai svarbus siekiant užtikrinti visišką objektyvumą priimant sprendimus duomenų apsaugos klausimais. Įstatyme, kuriuo grindžiamas priežiūros institucijos įsteigimas, turi būti ne tik nuostatos, kuriomis konkrečiai užtikrinamas nepriklausomumas, bet ir nustatoma organizacinė struktūra, iš kurios matyti, kad institucija iš tikrųjų yra nepriklausoma. 2010 m. ESTT pirmą kartą nagrinėjo reikalaujamą duomenų apsaugos priežiūros institucijų nepriklausomumo laipsnį[497]. Pateiktuose pavyzdžiuose aptariama ESTT apibrėžties „visiškas nepriklausomumas“ reikšmė.

494 Bendrojo duomenų apsaugos reglamento 13 straipsnio 2 dalies d punktas.

495 *Ten pat*, 51 straipsnis; atnaujintos 108-osios konvencijos 2 dalis.

496 Bendrojo duomenų apsaugos reglamento 52 straipsnio 1 dalis; atnaujintos 108-osios konvencijos 15 straipsnio 5 punktas.

497 FRA (2010 m.), *Fundamental rights: challenges and achievements in 2010*, 2010 m. metinė ataskaita, p. 59; FRA (2010 m.), *Data protection in the European Union: the role of National Data Protection Authorities*, 2010 m. gegužės mėn.

Pavyzdys. Byloje *Europos Komisija prieš Vokietijos Federacinę Respubliką*[498] Europos Komisija prašė ESTT pripažinti, kad Vokietija neteisingai į nacionalinę teisę perkėlė už duomenų apsaugos užtikrinimą atsakingų priežiūros institucijų „visiško nepriklausomumo“ reikalavimą ir taip neįvykdė savo prievolių pagal Duomenų apsaugos direktyvos 28 straipsnio 1 dalį. Komisijos manymu, tai, kad Vokietija priežiūros institucijoms, kontroliuojančioms asmens duomenų tvarkymą įvairiose federalinėse žemėse (*Länder*), taikė valstybinę stebėseną, siekdama užtikrinti, kad būtų laikomasi duomenų apsaugos teisės aktų, pažeidė nepriklausomumo reikalavimą.

ESTT pažymėjo, kad žodžiai „visiškas nepriklausomumas“ turi būti aiškinami remiantis faktine tos nuostatos formuluote ir ES duomenų apsaugos teisės tikslais bei schema[499]. ESTT pažymėjo, kad priežiūros institucijos yra su asmens duomenų tvarkymu susijusių teisių „sergėtojos“. Todėl jų įsteigimas valstybėse narėse „yra esminis asmenų apsaugos tvarkant asmens duomenis elementas“[500]. ESTT padarė išvadą, kad „vykdydamos savo funkcijas priežiūros institucijos turi veikti objektyviai ir nešališkai. Šiuo tikslu jų neturi veikti jokia [valdžios institucijų] išorinė įtaka, įskaitant tiesioginę ar netiesioginę, o ne vien kontroliuojamų organizacijų įtaka“[501].

ESTT taip pat nusprendė, kad „visiško nepriklausomumo“ reikšmė turėtų būti aiškinama atsižvelgiant į EDAPP nepriklausomumą, kaip apibrėžta ES institucijų duomenų apsaugos reglamente. Šiame reglamente nepriklausomumo sąvoka reiškia, kad EDAPP neprašo ir nepriima jokių nurodymų iš kitų subjektų.

Todėl ESTT nusprendė, kad Vokietijos priežiūros institucijos, atsižvelgiant į valdžios institucijų vykdomą priežiūrą, nebuvo visiškai nepriklausomos, kaip apibrėžta ES duomenų apsaugos teisėje.

Pavyzdys. Byloje *Europos Komisija prieš Austrijos Respubliką*[502] ESTT atkreipė dėmesį į panašias problemas, susijusias su tam tikrų Austrijos duomenų apsaugos institucijos (Duomenų apsaugos komisija, DSK) narių ir darbuotojų

498 ESTT, C-518/07, *Europos Komisija prieš Vokietijos Federacinę Respubliką* (DK), 2010 m. kovo 9 d., 27 punktas.

499 *Ten pat*, 17 ir 29 punktai.

500 *Ten pat*, 23 punktas.

501 *Ten pat*, 25 punktas.

502 ESTT, C-614/10, *Europos Komisija prieš Austrijos Respubliką* (DK), 2012 m. spalio 16 d., 59 ir 63 punktai.

nepriklausomumu. ESTT padarė išvadą, kad tai, jog Federalinė kanceliarija priežiūros institucijai skyrė darbuotojų, pažeidžia ES duomenų apsaugos teisės aktuose nustatytą nepriklausomumo reikalavimą. ESTT taip pat nusprendė, kad reikalavimas nuolat informuoti kanceliariją apie savo darbą prieštaravo visiškam priežiūros institucijos nepriklausomumui.

Pavyzdys. Byloje *Europos Komisija prieš Vengriją*[503] buvo uždrausta panaši nacionalinė praktika, daranti poveikį darbuotojų nepriklausomumui. ESTT atkreipė dėmesį į tai, kad „reikalavimas užtikrinti, kad priežiūros institucijos joms pavestas funkcijas galėtų vykdyti visiškai nepriklausomai, reiškia, kad valstybės narės privalo nekeisti šios institucijos kadencijos trukmės iki iš pradžių numatytos jos pabaigos“. ESTT taip pat konstatavo, kad „pirma laiko nutraukusi asmens duomenų apsaugos priežiūros institucijos kadenciją Vengrija neįvykdė įsipareigojimų pagal Direktyvą 95/46/EB“.

„Visiško nepriklausomumo“ sąvoka ir kriterijai dabar aiškiai nustatyti BDAR, kuriame įtvirtinti aprašytuose ESTT sprendimuose suformuoti principai. Pagal reglamentą visiškas jų užduočių ir įgaliojimų vykdymo nepriklausomumas reiškia, kad[504]:

- kiekvienos priežiūros institucijos nariai privalo išlikti nepriklausomi nuo tiesioginės arba netiesioginės išorės įtakos ir neprivalo priimti kitų asmenų nurodymų;
- kiekvienos priežiūros institucijos nariai privalo susilaikyti nuo bet kokių veiksmų, kurie yra nesuderinami su jų pareigomis, kad užkirstų kelią interesų konfliktui;
- valstybės narės privalo kiekvieną priežiūros instituciją aprūpinti būtinais žmogiškaisiais, techniniais ir finansiniais ištekliais ir infrastruktūra, kad ji galėtų veiksmingai vykdyti savo užduotis;
- valstybės narės privalo užtikrinti, kad kiekviena priežiūros institucija pati pasirinktų savo darbuotojus;
- priežiūros institucijos finansinė kontrolė, kuri vykdoma pagal nacionalinius įstatymus, negali daryti įtakos jos nepriklausomumui. Priežiūros institucijos privalo turėti atskirą ir viešą metinį biudžetą, kuris sudarytų sąlygas tinkamam jų veikimui.

503 ESTT, C-288/12, *Europos Komisija prieš Vengriją* (DK), 2014 m. balandžio 8 d., 50 ir 67 punktai.

504 Bendrojo duomenų apsaugos reglamento 52 straipsnis.

Priežiūros institucijų nepriklausomumas pagal ET teisę taip pat laikomas esminiu reikalavimu. Pagal atnaujintą 108-ąją konvenciją reikalaujama, kad priežiūros institucijos, „vykdydamos savo užduotis ir įgyvendindamos įgaliojimus, veiktų visiškai nepriklausomai ir nešališkai“ ir neprašytų ir nepriimtų nurodymų[505]. Taip Konvencijoje pripažįstama, kad šios institucijos negali veiksmingai apsaugoti asmenų teisių ir laisvių, susijusių su duomenų tvarkymu, išskyrus atvejus, kai jos savo funkcijas vykdo visiškai nepriklausomai. Atnaujintos 108-osios konvencijos aiškinamojoje ataskaitoje aptarti įvairūs aspektai, padedantys užtikrinti nepriklausomumą. Tokie aspektai apima priežiūros institucijų galimybę pačioms samdyti darbuotojus ir priimti sprendimus nepatiriant išorės kišimosi, taip pat veiksnius, susijusius su jų funkcijų įgyvendinimo trukme ir sąlygomis, kuriomis jie gali nustoti vykdyti savo funkcijas[506].

5.2. Kompetencija ir įgaliojimai

Pagal ES teisę BDAR nustatyta priežiūros institucijų kompetencija ir organizacinė struktūra bei įgaliojimai, kad jos turi būti kompetentingos ir turėti įgaliojimus atlikti reglamente nustatytas užduotis.

Priežiūros institucija yra pagrindinė institucija pagal nacionalinę teisę, kuri užtikrina atitiktį ES duomenų apsaugos teisei. Priežiūros institucijos turi išsamų ne tik stebėsenos užduočių ir įgaliojimų sąrašą, kuris apima aktyvią ir prevencinę priežiūros veiklą. Kad vykdytų šias užduotis, priežiūros institucijos privalo turėti tinkamus tyrimo, taisymo ir patariamuosius įgaliojimus, kaip nustatyta BDAR 57 ir 58 straipsniuose, pavyzdžiui[507]:

- patarti duomenų valdytojams ir duomenų subjektams visais duomenų apsaugos klausimais;
- leisti taikyti standartines sutarčių sąlygas, įmonei privalomas taisykles ar administracinius susitarimus;
- tirti duomenų tvarkymo operacijas ir prireikus į jas įsikišti;

505 Atnaujintos 108-osios konvencijos 15 straipsnio 5 dalis.

506 Atnaujintos 108-osios konvencijos aiškinamoji ataskaita.

507 Bendrojo duomenų apsaugos reglamento 57 ir 58 straipsniai. Taip pat žr. 108-osios konvencijos Papildomo protokolo 1 straipsnį.

- reikalauti pateikti visą informaciją, susijusią su duomenų valdytojo veiklos priežiūra;
- įspėti arba papeikti duomenų valdytojus ir nurodyti, kad pranešimai apie asmens duomenų saugumo pažeidimus būtų siunčiami duomenų subjektams;
- liepti ištaisyti, užblokuoti, ištrinti arba sunaikinti duomenis;
- laikinai arba visam laikui uždrausti tvarkyti duomenis arba skirti administracines nuobaudas;
- perduoti klausimą spręsti teismui.

Kad įgyvendintų savo funkcijas, priežiūros institucija privalo turėti prieigą prie visų asmens duomenų ir informacijos, kuri yra būtina užklausai, taip pat galimybę patekti į bet kurias patalpas, kuriose duomenų valdytojas laiko atitinkamą informaciją. Pasak ESTT, priežiūros institucijos įgaliojimus privaloma aiškinti plačiai, siekiant ES duomenų subjektų atžvilgiu užtikrinti visapusišką duomenų apsaugos veiksmingumą.

Pavyzdys. Byloje *Schrems* ESTT kėlė klausimą, ar asmens duomenų perdavimas JAV pagal ES ir JAV „saugaus uosto“ susitarimą atitiko ES duomenų apsaugos teisę atsižvelgiant į Edwardo Snowdeno atskleistą informaciją. ESTT argumentuose teigiama, kad nacionalinės priežiūros institucijos, veikdamos kaip nepriklausomos duomenų valdytojų atliekamo duomenų tvarkymo stebėtojos, gali užkirsti kelią asmens duomenų perdavimui į trečiąją šalį, nepaisant to, kad priimtas sprendimas dėl tinkamumo, jei yra pagrįstų įrodymų, kad trečiojoje šalyje nebeužtikrinama tinkama apsauga[508].

Kiekviena priežiūros institucija savo veiklos teritorijoje turi kompetenciją įgyvendinti tyrimo įgaliojimus ir įgaliojimus įsikišti. Tačiau duomenų valdytojų ir duomenų tvarkytojų veikla dažnai yra tarpvalstybinio pobūdžio ir duomenų tvarkymas turi poveikį keliose valstybėse narėse esantiems duomenų subjektams, todėl kyla klausimas dėl kompetencijos padalijimo tarp įvairių priežiūros institucijų. ESTT turėjo galimybę išnagrinėti šį klausimą *Weltimmo* byloje.

508 ESTT, C-362/14, *Maximilian Schrems prieš Data Protection Commissioner* (DK), 2015 m. spalio 6 d., 26–36 ir 40–41 punktai.

Pavyzdys. Byloje *Weltimmo*[509] ESTT nagrinėjo klausimą, ar nacionalinės priežiūros institucijos turėjo kompetenciją nagrinėti klausimus, susijusius su ne jų jurisdikcijoje įsteigtomis organizacijomis. *Weltimmo* buvo Slovakijoje įregistruota įmonė, valdanti interneto svetainę, kurioje talpinami skelbimai apie Vengrijoje esantį nekilnojamąjį turtą. Skelbėjai pateikė skundą Vengrijos duomenų apsaugos priežiūros institucijai dėl Vengrijos duomenų teisės pažeidimo, o institucija baudą skyrė *Weltimmo*. Įmonė ginčijo baudą nacionaliniuose teismuose ir byla buvo perduota ESTT, kad jis nustatytų, ar pagal ES duomenų apsaugos direktyvą valstybės narės priežiūros institucijoms buvo leidžiama taikyti savo nacionalinę duomenų apsaugos teisę kitoje valstybėje narėje įregistruotai įmonei.

ESTT Duomenų apsaugos direktyvos 4 straipsnio 1 dalies a punktą aiškino kaip leidžiantį taikyti kitos valstybės narės nei ta, kurioje įregistruotas duomenų valdytojas, duomenų apsaugos teisę, „jeigu šis valdytojas per nuolatinį vienetą tos valstybės narės teritorijoje veiksmingai ir realiai vykdo bent minimalią veiklą, kurios pagrindu atliekamas šis tvarkymas“. ESTT pažymėjo, kad, remiantis jam pateikta informacija, *Weltimmo* vykdė realią ir veiksmingą veiklą Vengrijoje, nes įmonė Vengrijoje turėjo atstovą, įtrauktą į Slovakijos įmonių registrą su adresu vengrų kalba, taip pat Vengrijos banko sąskaitą ir pašto dėžutę, taip pat Vengrijoje vykdė veiklą vengrų kalba. Iš šios informacijos matyti, kad padalinys egzistuoja, todėl *Weltimmo* veiklai būtų taikomi Vengrijos duomenų apsaugos teisės aktai ir Vengrijos priežiūros institucijos jurisdikcija. Tačiau ESTT paliko nacionaliniam teismui patikrinti informaciją ir nuspręsti, ar *Weltimmo* faktiškai turėjo padalinį Vengrijoje.

Jeigu prašymą priimti prejudicinį sprendimą pateikęs teismas būtų konstatavęs, kad *Weltimmo* turėjo padalinį Vengrijoje, Vengrijos priežiūros institucija būtų turėjusi teisę skirti baudą. Vis dėlto, jei nacionalinis teismas nuspręstų priešingai, t. y. kad *Weltimmo* Vengrijoje neturi padalinio, būtų taikoma valstybės (-ių) narės (-ių), kurioje (-iose) bendrovė buvo įregistruota, teisė. Šiuo atveju, kadangi priežiūros institucijų įgaliojimais turi būti naudojamasi paisant kitų valstybių narių teritorinio suvereniteto, Vengrijos institucija negalėtų skirti sankcijų. Kadangi Duomenų apsaugos direktyvoje numatyta priežiūros

509 ESTT, C-230/14, *Weltimmo s.r. o. prieš Nemzeti Adatvédelmi és Információszabadság Hatóság*, 2015 m. spalio 1 d.

institucijų pareiga bendradarbiauti, Vengrijos institucija vis dėlto galėjo prašyti Slovakijos institucijos išnagrinėti šį klausimą, nustatyti Slovakijos teisės pažeidimą ir skirti Slovakijos teisės aktuose numatytas sankcijas.

Priėmus Bendrąjį duomenų apsaugos reglamentą, dabar nustatytos išsamios taisyklės dėl priežiūros institucijų kompetencijos tarpvalstybiniais atvejais. Reglamentu nustatomas vieno langelio mechanizmas ir į jį įtrauktos nuostatos, kuriose numatytas privalomas skirtingų priežiūros institucijų bendradarbiavimas. Kad bendradarbiavimas tarpvalstybiniais atvejais būtų veiksmingas, pagal Bendrąjį duomenų apsaugos reglamentą reikalaujama įsteigti vadovaujančią priežiūros instituciją, kuri būtų duomenų valdytojo arba duomenų tvarkytojo pagrindinės buveinės arba vienintelės buveinės priežiūros institucija[510]. Vadovaujanti priežiūros institucija yra atsakinga už tarpvalstybinius atvejus, yra vienintelė institucija, su kuria duomenų valdytojas arba duomenų tvarkytojas palaiko ryšius, ir koordinuoja bendradarbiavimą su kitomis priežiūros institucijomis, kad būtų pasiektas bendras sutarimas. Bendradarbiavimas apima keitimąsi informacija, abipusę pagalbą stebint, tiriant ir priimant privalomus sprendimus[511].

Pagal ET teisę priežiūros institucijų kompetencija ir įgaliojimai nustatyti atnaujintos 108-osios konvencijos 15 straipsnyje. Šie įgaliojimai atitinka priežiūros institucijoms pagal ES teisę suteiktus įgaliojimus, įskaitant tyrimo įgaliojimus ir įgaliojimus įsikišti, įgaliojimus priimti sprendimus ir skirti administracines sankcijas, susijusias su Konvencijos nuostatų pažeidimais, ir įgaliojimus dalyvauti teisminiame procese. Nepriklausomos priežiūros institucijos taip pat yra kompetentingos nagrinėti duomenų subjektų pateiktus prašymus ir skundus, didinti visuomenės informuotumą apie duomenų apsaugos teisės aktus ir konsultuoti nacionalinius sprendimus priimančius asmenis dėl bet kokių teisinių ar administracinių priemonių, kuriomis numatomas asmens duomenų tvarkymas.

5.3. Bendradarbiavimas

BDAR nustatyta bendra priežiūros institucijų bendradarbiavimo sistema ir įtvirtintos konkretesnės priežiūros institucijų bendradarbiavimo vykdant tarpvalstybinę duomenų tvarkymo veiklą taisyklės.

510 Bendrojo duomenų apsaugos reglamento 56 straipsnio 1 punktas.

511 *Ten pat*, 60 straipsnis.

Pagal BDAR priežiūros institucijos teikia savitarpio pagalbą ir dalijasi atitinkama informacija, kad galėtų nuosekliai įgyvendinti ir taikyti reglamentą[512]. Tai apima priežiūros instituciją, į kurią kreipiamasi ir kuri vykdo konsultacijas, patikrinimus ir tyrimus. Priežiūros institucijos gali vykdyti bendras operacijas, įskaitant bendrus tyrimus ir bendras vykdymo užtikrinimo priemones, kuriose dalyvauja visų priežiūros institucijų darbuotojai[513].

Europos Sąjungoje duomenų valdytojai ir duomenų tvarkytojai vis dažniau veikia tarpvalstybiniu lygmeniu. Tam reikalingas glaudus valstybių narių kompetentingų priežiūros institucijų bendradarbiavimas siekiant užtikrinti, kad asmens duomenys būtų tvarkomi laikantis BDAR reikalavimų. Pagal reglamente nustatytą vieno langelio mechanizmą, jeigu duomenų valdytojas arba duomenų tvarkytojas turi buveines keliose valstybėse narėse arba jeigu jis turi vieną buveinę, tačiau duomenų tvarkymo operacijos daro didelį poveikį duomenų subjektams daugiau nei vienoje valstybėje narėje, pagrindinės (arba vienos) buveinės priežiūros institucija yra pagrindinė duomenų valdytojo arba duomenų tvarkytojo tarpvalstybinės veiklos priežiūros institucija. Vadovaujančios institucijos turi įgaliojimus imtis vykdymo užtikrinimo veiksmų prieš duomenų valdytoją arba duomenų tvarkytoją. Vieno langelio principu veikiančiu mechanizmu siekiama pagerinti ES duomenų apsaugos teisės aktų suderinimą ir vienodą taikymą įvairiose valstybėse narėse. Tai taip pat naudinga įmonėms, nes jos turi dirbti tik su vadovaujančia institucija, o ne su keliomis priežiūros institucijomis. Tai padidina teisinį tikrumą įmonėms ir praktiškai taip pat turėtų reikšti, kad sprendimai priimami greičiau ir kad įmonės nesusiduria su skirtingomis priežiūros institucijomis, kurios joms nustato prieštaringus reikalavimus.

Nustatant vadovaujančią instituciją reikia išsiaiškinti įmonės pagrindinės buveinės vietą ES. Sąvoka „pagrindinė buveinė“ apibrėžta BDAR. Be to, 29 straipsnio darbo grupė paskelbė duomenų valdytojo arba duomenų tvarkytojo vadovaujančios priežiūros institucijos nustatymo gaires, į kurias įtraukti pagrindinės buveinės nustatymo kriterijai[514].

Siekdama užtikrinti aukštą duomenų apsaugos lygį visoje ES, vadovaujančioji priežiūros institucija veikia ne viena. Ji privalo bendradarbiauti su kitomis suinteresuotomis priežiūros institucijomis, kad priimtų sprendimus dėl duomenų valdytojų ir

512 *Ten pat*, 61 straipsnio 1–3 dalys ir 62 straipsnio 1 dalis.

513 *Ten pat*, 62 straipsnio 1 dalis.

514 29 straipsnio darbo grupė (2016 m.), *Duomenų valdytojo arba duomenų tvarkytojo vadovaujančios priežiūros institucijos nustatymo gairės*, WP 244, Briuselis, 2016 m. gruodžio 13 d., peržiūrėtos 2017 m. balandžio 5 d.

duomenų tvarkytojų vykdomo asmens duomenų tvarkymo ir stengtųsi pasiekti susitarimą ir užtikrinti nuoseklumą. Bendradarbiavimas tarp atitinkamų priežiūros institucijų apima keitimąsi informacija, savitarpio pagalbą viena kitai, bendrų tyrimų atlikimą ir stebėsenos veiklą[515]. Teikdamos tarpusavio paramą viena kitai, priežiūros institucijos privalo atidžiai išnagrinėti kitų priežiūros institucijų prašymus pateikti informaciją ir taikyti priežiūros priemones, pavyzdžiui, išankstinius leidimus ir konsultacijas su duomenų valdytoju dėl jo vykdomos duomenų tvarkymo veiklos, patikrinimų arba tyrimų. Savitarpio pagalba kitų valstybių narių priežiūros institucijoms turi būti teikiama remiantis prašymu ir nepagrįstai nedelsiant, ir ne vėliau kaip per vieną mėnesį nuo prašymo gavimo[516].

Jeigu duomenų valdytojas turi padalinių įvairiose valstybėse narėse, priežiūros institucijos gali atlikti bendras operacijas, įskaitant tyrimo ir vykdymo priemonių taikymą, kuriose dalyvauja kitų valstybių narių priežiūros institucijų darbuotojai[517].

Įvairių priežiūros institucijų bendradarbiavimas yra svarbus reikalavimas ir pagal ET teisę. Atnaujintoje 108-ojoje konvencijoje nustatyta, kad priežiūros institucijos privalo bendradarbiauti viena su kita tiek, kiek tai yra būtina jų užduotims atlikti[518]. Tai, pavyzdžiui, turėtų būti daroma suteikiant viena kitai bet kokią susijusią ir naudingą informaciją ir koordinuojant tyrimus bei vykdant bendrus veiksmus[519].

5.4. Europos duomenų apsaugos valdyba

Nepriklausomų priežiūros institucijų svarba ir pagrindinė kompetencija, suteikta pagal Europos duomenų apsaugos teisę, jau aprašyta šiame skyriuje. Europos duomenų apsaugos valdyba (EDAV) yra kitas svarbus subjektas, kuris užtikrina, kad duomenų apsaugos taisyklės visoje ES būtų taikomos veiksmingai ir nuosekliai.

515 Bendrojo duomenų apsaugos reglamento 60 straipsnio 1–3 dalys.

516 *Ten pat*, 61 straipsnio 1 ir 2 dalys.

517 *Ten pat*, 62 straipsnio 1 punktas.

518 Atnaujintos 108-osios konvencijos 16 ir 17 straipsniai.

519 *Ten pat*, 17 straipsnis.

BDAR nustatyta, kad EDAV yra juridinio asmens teises turinti ES įstaiga[520]. Ji yra 29 straipsnio darbo grupės[521] teisių perėmėja, kuri pagal Duomenų apsaugos direktyvą buvo įsteigta tam, kad patartų Komisijai dėl bet kurios ES priemonės, kuri daro įtaką asmenų teisėms, susijusioms su asmens duomenų tvarkymu ir privatumu, skatintų vienodą direktyvos taikymą ir teiktų Komisijai ekspertų nuomones su duomenų apsauga susijusiais klausimais. 29 straipsnio darbo grupę sudarė ES valstybių narių priežiūros institucijų atstovai, taip pat Komisijos ir EDAPP atstovai.

Panašiai kaip ir darbo grupę, EDAV sudaro kiekvienos valstybės narės priežiūros institucijų vadovai ir EDAPP arba jų atstovai[522]. EDAPP turi vienodas balsavimo teises, išskyrus su ginčų sprendimu susijusius atvejus, kai jis gali balsuoti tik dėl sprendimų, susijusių su ES institucijoms taikomais principais ir taisyklėmis, atitinkančiomis BDAR nustatytų principų ir taisyklių esmę. Komisija turi teisę dalyvauti EDAV veikloje ir posėdžiuose, tačiau neturi balsavimo teisių[523]. EDAV iš savo narių paprasta balsų dauguma penkerių metų kadencijai išrenka pirmininką (kuris veikia kaip jos atstovas) ir du pirmininko pavaduotojus. Be to, EDAV taip pat turi jai pavaldų sekretoriatą, kurio funkcijas atlieka EDAPP, kad EDAV būtų teikiama analitinė, administracinė ir logistinė parama[524].

EDAV užduotys išsamiai aprašytos BDAR 64, 65 ir 70 straipsniuose ir apima išsamias pareigas, kurias galima suskirstyti į trijų pagrindinių rūšių veiklą.

- **Nuoseklumas.** EDAV teisiškai įpareigojančius sprendimus gali priimti trimis atvejais: kai priežiūros institucija pareiškė atitinkamą ir pagrįstą prieštaravimą pagal vieno langelio mechanizmą, kai yra prieštaringų nuomonių dėl to, kuri priežiūros institucija yra vadovaujanti, ir galiausiai kai kompetentinga priežiūros institucija neprašo EDAV nuomonės arba nesivadovauja priimta EDAV nuomone[525]. Pagrindinė EDAV pareiga yra užtikrinti, kad BDAR būtų nuosekliai taikomas visoje ES, be to, ji atlieka pagrindinį vaidmenį taikant nuoseklumo užtikrinimo mechanizmą, kaip aprašyta 5.5 skirsnyje.

520 Bendrojo duomenų apsaugos reglamento 68 straipsnis.

521 Pagal Direktyvą 95/46/EB 29 straipsnio darbo grupė turėjo patarti Komisijai dėl bet kokių ES priemonių, darančių poveikį asmenų teisėms, susijusioms su asmens duomenų tvarkymu ir privatumu, skatinti vienodą direktyvos taikymą ir teikti Komisijai ekspertų nuomonę su duomenų apsauga susijusiais klausimais. 29 straipsnio darbo grupę sudarė ES valstybės narės priežiūros institucijų, Komisijos ir EDAPP atstovai.

522 Bendrojo duomenų apsaugos reglamento 68 straipsnio 3 dalis.

523 *Ten pat*, 68 straipsnio 4 ir 5 dalys.

524 *Ten pat*, 73 ir 75 straipsniai.

525 *Ten pat*, 65 straipsnis.

- **Konsultacijos.** Be to, EDAV pavesta konsultuoti Komisiją visais su asmens duomenų apsauga Sąjungoje susijusiais klausimais, pavyzdžiui, dėl Bendrojo duomenų apsaugos reglamento pakeitimų, ES teisės aktų, susijusių su duomenų tvarkymu ir galinčių prieštarauti ES duomenų apsaugos taisyklėms, peržiūros arba Komisijos sprendimų dėl tinkamumo, kuriais sudaromos sąlygos perduoti asmens duomenis į trečiąją šalį arba tarptautinei organizacijai, priėmimo.

- **Rekomendacijos.** Valdyba taip pat skelbia gaires, rekomendacijas ir geriausią patirtį, kad skatintų nuoseklų reglamento taikymą, ir remia priežiūros institucijų bendradarbiavimą ir keitimąsi žiniomis. Be to, ji privalo skatinti duomenų valdytojų arba duomenų tvarkytojų asociacijas parengti elgesio kodeksus, taip pat nustatyti duomenų apsaugos sertifikavimo mechanizmus ir antspaudus.

EDAV sprendimai gali būti ginčijami ESTT.

5.5. BDAR nuoseklumo užtikrinimo mechanizmas

BDAR nustatytas nuoseklumo užtikrinimo mechanizmas, kuriuo užtikrinama, kad reglamentas būtų nuosekliai taikomas visose valstybėse narėse, ir pagal šį mechanizmą priežiūros institucijos bendradarbiauja tarpusavyje ir prireikus su Komisija. Nuoseklumo užtikrinimo mechanizmas naudojamas dviem atvejais. Pirmasis atvejis yra susijęs su EDAV nuomonėmis, kurios pateikiamos tais atvejais, kai kompetentinga valdžios institucija ketina patvirtinti priemones, pavyzdžiui, duomenų tvarkymo operacijų, dėl kurių reikia atlikti poveikio duomenų apsaugai vertinimą (PDAV), sąrašu, arba nustatyti standartines sutarčių sąlygas. Antrasis atvejis yra susijęs su priežiūros institucijoms privalomais EDAV sprendimais, priimtais pagal vieno langelio mechanizmą, ir atvejais, kai priežiūros institucija neprašo EDAV nuomonės arba nesivadovauja priimta EDAV nuomone.

6

Duomenų subjektų teisės ir jų užtikrinimas

ES	Reglamentuojami klausimai	ET
Teisė būti informuotam		
Bendrojo duomenų apsaugos reglamento 12 straipsnis ESTT, C-473/12, *Institut professionnel des agents immobiliers (IPI) prieš Englebert*, 2013 m. ESTT, C-201/14, *Smaranda Bara ir kt. prieš Casa Națională de Asigurări de Sănătate ir kt.*, 2015 m.	**Informacijos skaidrumas**	Atnaujintos 108-osios konvencijos 8 straipsnis
Bendrojo duomenų apsaugos reglamento 13 straipsnio 1 ir 2 dalys ir 14 straipsnio 1 ir 2 dalys	**Informacijos turinys**	Atnaujintos 108-osios konvencijos 8 straipsnio 1 dalis
Bendrojo duomenų apsaugos reglamento 13 straipsnio 1 dalis ir 14 straipsnio 3 dalis	**Informacijos pateikimo laikas**	Atnaujintos 108-osios konvencijos 9 straipsnio 1 dalies b punktas
Bendrojo duomenų apsaugos reglamento 12 straipsnio 1, 5 ir 7 dalys	**Informacijos pateikimo priemonės**	Atnaujintos 108-osios konvencijos 9 straipsnio 1 dalies b punktas
Bendrojo duomenų apsaugos reglamento 13 straipsnio 2 dalies d punktas ir 14 straipsnio 2 dalies e punktas, 77, 78 ir 79 straipsniai	**Teisė pateikti skundą**	Atnaujintos 108-osios konvencijos 9 straipsnio 1 dalies f punktas

ES	Reglamentuojami klausimai	ET
Teisė susipažinti su duomenimis		
Bendrojo duomenų apsaugos reglamento 15 straipsnio 1 dalis ESTT, C-553/07, *College van burgemeester en wethouders van Rotterdam prieš M. E. E. Rijkeboer*, 2009 m. ESTT, sujungtos bylos C-141/12 ir C-372/12, *YS prieš Minister voor Immigratie, Integratie en Asiel* ir *Minister voor Immigratie, Integratie en Asiel prieš M ir S*, 2014 m. ESTT, C-434/16, *Peter Nowak prieš Data Protection Commissioner*, 2017 m.	**Teisė susipažinti su savo duomenimis**	Atnaujintos 108-osios konvencijos 9 straipsnio 1 dalies b punktas EŽTT, *Leander prieš Švediją*, Nr. 9248/81, 1987 m.
Teisė ištaisyti duomenis		
Bendrojo duomenų apsaugos reglamento 16 straipsnis	**Netikslių asmens duomenų ištaisymas**	Atnaujintos 108-osios konvencijos 9 straipsnio 1 dalies e punktas EŽTT, *Cemalettin Canli prieš Turkiją*, Nr. 22427/04, 2008 m. EŽTT, *Ciubotaru prieš Moldovą*, Nr. 27138/04, 2010 m.
Teisė reikalauti ištrinti duomenis		
Bendrojo duomenų apsaugos reglamento 17 straipsnio 1 dalis	**Asmens duomenų ištrynimas**	Atnaujintos 108-osios konvencijos 9 straipsnio 1 dalies e punktas EŽTT, *Segerstedt-Wiberg ir kiti prieš Švediją*, Nr. 62332/00, 2006 m.
ESTT, C-131/12, *Google Spain SL, Google Inc. prieš Agencia Española de Protección de Datos (AEPD), Mario Costeja González* (DK), 2014 m. ESTT, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce prieš Salvatore Manni*, 2017 m.	**Teisė būti pamirštam**	
Teisė apriboti duomenų tvarkymą		
Bendrojo duomenų apsaugos reglamento 18 straipsnio 1 dalis	**Teisė apriboti asmens duomenų naudojimą**	

ES	Reglamentuojami klausimai	ET
Bendrojo duomenų apsaugos reglamento 19 straipsnis	Prievolė pranešti	
Teisė į duomenų perkeliamumą		
Bendrojo duomenų apsaugos reglamento 20 straipsnis	Teisė į duomenų perkeliamumą	
Teisė nesutikti		
Bendrojo duomenų apsaugos reglamento 21 straipsnio 1 dalis ESTT, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce prieš Salvatore Manni*, 2017 m.	Teisė nesutikti dėl duomenų subjekto konkrečios padėties	Rekomendacijos dėl profiliavimo 5.3 straipsnis Atnaujintos 108-osios konvencijos 9 straipsnio 1 dalies d punktas
Bendrojo duomenų apsaugos reglamento 21 straipsnio 2 dalis	Teisė nesutikti, kad duomenys būtų naudojami rinkodaros tikslais	Rekomendacijos dėl tiesioginės rinkodaros 4.1 straipsnis
Bendrojo duomenų apsaugos reglamento 21 straipsnio 5 dalis	Teisė nesutikti automatizuotomis priemonėmis	
Teisės, susijusios su automatizuotu sprendimų priėmimu ir profiliavimu		
Bendrojo duomenų apsaugos reglamento 22 straipsnis	Teisės, susijusios su automatizuotu sprendimų priėmimu ir profiliavimu	Atnaujintos 108-osios konvencijos 9 straipsnio 1 dalies a punktas
Bendrojo duomenų apsaugos reglamento 21 straipsnis	Teisė nesutikti su automatizuotu sprendimų priėmimu	
Bendrojo duomenų apsaugos reglamento 13 straipsnio 2 dalies f punktas	Teisė į prasmingą paaiškinimą	Atnaujintos 108-osios konvencijos 9 straipsnio 1 dalies c punktas
Teisių gynimo priemonės, atsakomybė, sankcijos ir kompensacija		
Chartijos 47 straipsnis ESTT, C-362/14, *Maximilian Schrems prieš Data Protection Commissioner* (DK), 2015 m. Bendrojo duomenų apsaugos reglamento 77–84 straipsniai	Už nacionalinės duomenų apsaugos teisės pažeidimus	EŽTK 13 straipsnis (taikoma tik ET valstybėms narėms) Atnaujintos 108-osios konvencijos 9 straipsnio 1 dalies f punktas, 12, 15, 16–21 straipsniai EŽTT, *K. U. prieš Suomiją*, Nr. 2872/02, 2008 m. EŽTT, *Biriuk prieš Lietuvą*, Nr. 23373/03, 2008 m.

ES	Reglamentuojami klausimai	ET
ES institucijų duomenų apsaugos reglamento 34 ir 49 straipsniai ESTT, C-28/08 P, *Europos Komisija prieš The Bavarian Lager Co. Ltd* (DK), 2010 m.	Už ES institucijų ir įstaigų padarytus ES teisės pažeidimus	

Apskritai teisinių taisyklių, ypač duomenų subjektų teisių apsauga, iš esmės priklauso nuo tinkamo jų užtikrinimo mechanizmo buvimo. Skaitmeniniame amžiuje duomenų tvarkymo mastas tapo labai didelis ir asmenims jį vis sunkiau suprasti. Siekiant sumažinti duomenų subjektų ir duomenų valdytojų galios pusiausvyros nebuvimą, asmenims suteiktos tam tikros teisės labiau kontroliuoti savo asmens duomenų tvarkymą. Teisė susipažinti su savo asmens duomenimis ir teisė juos ištaisyti numatyta ES pagrindinių teisių chartijos, kuri yra pirminės ES teisės dokumentas, turintis pagrindinę vertę ES teisinėje sistemoje, 8 straipsnio 2 dalyje. Antrinėje ES teisėje, visų pirma Bendrajame duomenų apsaugos reglamente, nustatyta išsami teisinė sistema, kurioje duomenų subjektams suteikiami įgaliojimai nustatant jiems teises duomenų valdytojų atžvilgiu. BDAR pripažįstama ne tik teisė susipažinti su duomenimis ir teisė ištaisyti duomenis, bet ir įvairios kitos teisės, pavyzdžiui, teisė ištrinti duomenis (teisė būti pamirštam), teisė nesutikti su duomenų tvarkymu arba teisė apriboti duomenų tvarkymą, ir su automatizuotu sprendimų priėmimu ir profiliavimu susijusios teisės. Atnaujintoje 108-ojoje konvencijoje taip pat numatytos panašios apsaugos priemonės, sudarančios sąlygas duomenų subjektams veiksmingai kontroliuoti savo duomenis. 9 straipsnyje išvardytos teisės, susijusios su jų asmens duomenų tvarkymu, kurias asmenys turėtų turėti galimybę įgyvendinti. Susitariančiosios šalys privalo užtikrinti, kad jų jurisdikcijoje šiomis teisėmis galėtų pasinaudoti kiekvienas duomenų subjektas, be to, kartu su jomis nustatomos veiksmingos teisinės ir praktinės priemonės, padedančios duomenų subjektams jas įgyvendinti.

Asmenims svarbu ne tik suteikti teises, lygiai taip pat svarbu nustatyti mechanizmus, kurie sudarytų sąlygas duomenų subjektams ginčyti jų teisių pažeidimus, patraukti duomenų valdytojus atsakomybėn ir reikalauti kompensacijos. Pagal EŽTK ir Chartijoje garantuojamą teisę į veiksmingą teisių gynimą reikalaujama, kad kiekvienam asmeniui būtų sudaryta galimybė pasinaudoti teisminėmis teisių gynimo priemonėmis.

6.1. Duomenų subjektų teisės

Pagrindiniai faktai

- Kiekvienas duomenų subjektas turi teisę gauti informaciją apie bet kurio duomenų valdytojo vykdomą jo asmens duomenų tvarkymo veiklą, išskyrus tam tikras išimtis.
- Duomenų subjektai turi teisę:
  - susipažinti su savo duomenimis ir gauti tam tikrą informaciją apie duomenų tvarkymą;
  - kad jų duomenis tvarkantis duomenų valdytojas ištaisytų jų duomenis, jeigu duomenys yra netikslūs;
  - kad duomenų valdytojas, kai tinkama, ištrintų jų duomenis, jeigu duomenų valdytojas jų duomenis tvarko neteisėtai;
  - laikinai apriboti duomenų tvarkymą;
  - kad jų duomenys tam tikromis sąlygomis būtų perduoti kitam duomenų valdytojui.
- Be to, duomenų subjektai turi teisę nesutikti, kad duomenys būtų tvarkomi, remdamiesi:
  - su jų konkrečia padėtimi susijusiais pagrindais;
  - tuo, kad jų duomenys naudojami tiesioginės rinkodaros tikslais.
- Duomenų subjektai turi teisę, kad jiems nebūtų taikomi tik automatizuotu duomenų tvarkymu, įskaitant profiliavimą, grindžiami sprendimai, kurie turi teisinį poveikį arba daro jiems didelį poveikį. Duomenų subjektai taip pat turi teisę:
  - iš duomenų valdytojo reikalauti žmogaus įsikišimo;
  - išreikšti savo nuomonę ir ginčyti automatizuotu duomenų tvarkymu pagrįstą sprendimą.

6.1.1. Teisė būti informuotam

Pagal **ET teisę** ir **ES teisę** duomenų tvarkymo operacijas vykdantys duomenų valdytojai yra įpareigoti asmens duomenų rinkimo metu informuoti duomenų subjektą apie numatomą jo duomenų tvarkymo tikslą. Ši prievolė nepriklauso nuo duomenų subjekto prašymo, tai veikiau reiškia, kad duomenų valdytojas privalo aktyviai laikytis pareigos, nepaisant to, ar duomenų subjektas rodo susidomėjimą gauti informaciją.

Pagal ET teisę, t. y. atnaujintos 108-osios konvencijos 8 straipsnį, susitariančiosios šalys privalo nustatyti duomenų valdytojų prievolę informuoti duomenų subjektus apie savo tapatybę ir įprastinę buveinę, duomenų tvarkymo teisinį pagrindą ir tikslą, tvarkomų asmens duomenų kategorijas, jų asmens duomenų gavėjus (jeigu tokių yra) ir kaip jie gali įgyvendinti 9 straipsnyje nustatytas teises, kurios apima teisę susipažinti su duomenimis, teisę ištaisyti duomenis ir teisę į teisių gynimo priemones. Bet kuri kita informacija, kuri laikoma būtina siekiant užtikrinti sąžiningą ir skaidrų asmens duomenų tvarkymą, duomenų subjektams taip pat turėtų būti pateikta. Atnaujintos 108-osios konvencijos aiškinamojoje ataskaitoje paaiškinta, kad duomenų subjektams pateikta informacija „turėtų būti prieinama, įskaitoma, suprantama ir pritaikyta prie atitinkamų duomenų subjektų“[526].

Pagal ES teisėje nustatytą skaidrumo principą reikalaujama, kad bet kokia duomenų tvarkymo veikla asmenų atžvilgiu turėtų būti skaidri. Asmenys turi teisę žinoti, kaip ir kokie asmens duomenys renkami, naudojami ar kitaip tvarkomi, taip pat žinoti apie riziką, apsaugos priemones ir savo teises, susijusias su duomenų tvarkymu[527]. Todėl BDAR 12 straipsnyje nustatyta plataus masto išsami duomenų valdytojų prievolė skaidriai teikti informaciją ir (arba) informuoti, kaip duomenų subjektai gali įgyvendinti savo teises[528]. Informacija turi būti glausta, skaidri, suprantama ir lengvai prieinama, pateikiama aiškia ir paprasta kalba. Kai tinkama, ją būtina pateikti rašytine forma, be to, ji, duomenų subjektui paprašius, gali būti pateikta net žodžiu, jeigu nekyla abejonių dėl jo tapatybės. Informacija pateikiama be pernelyg didelio delsimo ar išlaidų[529].

BDAR 13 ir 14 straipsniuose reglamentuojama duomenų subjektų teisė būti informuotiems atitinkamai tais atvejais, kai asmens duomenys buvo surinkti tiesiai iš jų arba kai duomenys iš jų nebuvo gauti.

Teisė gauti informaciją ir jos ribos pagal ES teisę išaiškintos ESTT jurisprudencijoje.

526 Atnaujintos 108-osios konvencijos aiškinamosios ataskaitos 68 punktas.

527 Bendrojo duomenų apsaugos reglamento 39 konstatuojamoji dalis.

528 *Ten pat*, 13 ir 14 straipsniai; atnaujintos 108-osios konvencijos 8 straipsnio 1 dalies b punktas.

529 Bendrojo duomenų apsaugos reglamento 12 straipsnio 5 dalis; atnaujintos 108-osios konvencijos 9 straipsnio 1 dalies b punktas.

Pavyzdys. Byloje *Institut professionnel des agents immobiliers (IPI) prieš Englebert*[530] ESTT buvo prašoma išaiškinti Direktyvos 95/46/EB 13 straipsnio 1 dalį. Pagal šį straipsnį valstybėms narėms suteikta teisė pasirinkti, ar priimti teisėkūros priemones, kuriomis ribojama duomenų subjekto teisė būti informuotam tais atvejais, kai tai yra būtina, be kita ko, siekiant apsaugoti kitų asmenų teises ir laisves ir užkirsti kelią nusikaltimams arba reglamentuojamų profesijų etikos pažeidimams ir juos ištirti. IPI yra Belgijos nekilnojamojo turto agentų profesinė organizacija, atsakinga už tai, kad būtų laikomasi nekilnojamojo turto agento profesinės veiklos reikalavimų. Ji paprašė nacionalinio teismo pripažinti, kad atsakovai pažeidė profesines taisykles, ir nurodyti jiems nutraukti įvairią nekilnojamojo turto agentūrų veiklą. Ieškinys buvo pagrįstas privačių detektyvų pateiktais įrodymais, kuriais rėmėsi IPI.

Prašymą priimti prejudicinį sprendimą pateikusiam teismui kilo abejonių dėl detektyvų surinktų įrodymų įrodomosios galios, nes jie galėjo būti gauti nesilaikant Belgijos teisės aktuose nustatytų duomenų apsaugos reikalavimų, visų pirma prievolės informuoti duomenų subjektus apie jų asmens duomenų tvarkymą prieš juos renkant. ESTT pažymėjo, kad 13 straipsnio 1 dalyje nurodyta, jog valstybės narės „gali“, bet neprivalo savo nacionalinėje teisėje numatyti įpareigojimo informuoti duomenų subjektus apie jų duomenų tvarkymą išimčių. Kadangi 13 straipsnio 1 dalyje nusikalstamų veikų ar etikos pažeidimų prevencija, tyrimas ir baudžiamasis persekiojimas už juos numatytas kaip pagrindas, kuriuo remdamosi valstybės narės gali apriboti asmenų teises, įstaigos, pavyzdžiui, IPI, ir jos vardu veikiančių detektyvų veikla galėtų būti grindžiama tokia nuostata. Tačiau jeigu valstybė narė nenumatė tokios išimties, duomenų subjektus informuoti būtina.

Pavyzdys. Byloje *Smaranda Bara ir kt. prieš Casa Națională de Asigurări de Sănătate ir kt.*[531] ESTT paaiškino, ar pagal ES teisę nacionalinei valstybinei administravimo įstaigai draudžiama perduoti asmens duomenis kitai valstybinei administravimo įstaigai vėlesnio tvarkymo tikslais neinformavus duomenų subjektų apie tokį perdavimą ir duomenų tvarkymą. Toje byloje Nacionalinė administravimo agentūra iš anksto neinformavo pareiškėjų, kad perdavė jų duomenis Nacionaliniam sveikatos draudimo fondui.

530 ESTT, C-473/12, *Institut professionnel des agents immobiliers (IPI) prieš Geoffrey Englebert ir kt.*, 2013 m. lapkričio 7 d.

531 ESTT, C-201/14, *Smaranda Bara ir kt. prieš Casa Națională de Asigurări de Sănătate ir kt.*, 2015 m. spalio 1 d.

ESTT manė, kad ES teisėje nustatytas reikalavimas informuoti duomenų subjektus apie jų asmens duomenų tvarkymą yra „svarbus tuo, kad jis yra viena iš sąlygų, būtinų tam, kad šie asmenys pasinaudotų <...> teise gauti informaciją apie tvarkomus duomenis ir teise juos ištaisyti, taip pat <...> teise pateikti prieštaravimą dėl minėtų duomenų tvarkymo“. Pagal sąžiningo duomenų tvarkymo principą reikalaujama informuoti duomenų subjektus apie jų duomenų perdavimą kitai valdžios institucijai, kad pastaroji galėtų juos toliau tvarkyti. Pagal Direktyvos 95/46/EB 13 straipsnio 1 dalį valstybės narės gali apriboti teisę būti informuotam, jeigu manoma, kad tai yra būtina siekiant apsaugoti svarbius valstybės ekonominius interesus, įskaitant mokesčių klausimus. Tačiau tokie apribojimai turi būti nustatyti priimant teisėkūros priemones. Kadangi nei perduotinų duomenų apibrėžtis, nei išsami jų perdavimo tvarka nebuvo nustatyta teisėkūros priemonėje, o tik dviejų valdžios institucijų protokole, ES teisėje nustatytos leidžiančios nukrypti nuostatos sąlygos nebuvo įvykdytos. Pareiškėjai turėjo būti iš anksto informuoti apie jų duomenų perdavimą Nacionaliniam sveikatos draudimo fondui ir tolesnį šių duomenų tvarkymą.

Informacijos turinys

Pagal atnaujintos 108-osios konvencijos 8 straipsnio 1 dalį duomenų valdytojas privalo pateikti duomenų subjektui visą informaciją, kuria užtikrinamas sąžiningas ir skaidrus asmens duomenų tvarkymas, įskaitant:

- duomenų valdytojo tapatybę ir įprastą gyvenamąją vietą arba buveinę;
- numatomo duomenų tvarkymo teisinį pagrindą ir tikslus;
- tvarkomų asmens duomenų kategorijas;
- kai taikytina, asmens duomenų gavėjus arba gavėjų kategorijas;
- būdus, kuriais duomenų subjektai gali įgyvendinti savo teises.

Pagal BDAR tais atvejais, kai iš duomenų subjekto renkami asmens duomenys, duomenų valdytojas privalo duomenų subjektui tuo metu, kai gaunami asmens duomenys, pateikti šią informaciją[532]:

- duomenų valdytojo ir, jei taikytina, DAP vardą bei pavardę (pavadinimą) ir kontaktinius duomenis;
- duomenų tvarkymo tikslą ir teisinį pagrindą, t. y. sutartį arba teisinę prievolę;
- teisėtą duomenų valdytojo interesą, jeigu tai yra duomenų tvarkymo pagrindas;
- galimus asmens duomenų gavėjus arba gavėjų kategorijas;
- ar duomenys bus perduoti trečiajai šaliai ar tarptautinei organizacijai ir ar šis perdavimas grindžiamas sprendimu dėl tinkamumo ir ar taikomos tinkamos apsaugos priemonės;
- asmens duomenų saugojimo laikotarpį ir, jeigu to laikotarpio neįmanoma nustatyti, kriterijus, kuriais remiantis nustatomas duomenų saugojimo laikotarpis;
- duomenų subjektų teises, susijusias su duomenų tvarkymu, pavyzdžiui, teisę susipažinti su duomenimis, ištaisyti duomenis, juos ištrinti ir apriboti duomenų tvarkymą arba su juo nesutikti;
- ar asmens duomenis reikalaujama pateikti pagal įstatymą, ar sutartį, ar duomenų subjektas privalo pateikti savo asmens duomenis, taip pat informaciją apie pasekmes, jeigu asmens duomenys nepateikiami;
- automatizuotą sprendimų priėmimą, įskaitant profiliavimą;
- teisę pateikti skundą priežiūros institucijai;
- teisės atšaukti sutikimą buvimą.

Automatizuoto sprendimų priėmimo, įskaitant profiliavimą, atvejais duomenų subjektai turi gauti prasmingą informaciją apie profiliavimo logiką, jo svarbą ir numatomas tvarkymo pasekmes.

532 Bendrojo duomenų apsaugos reglamento 13 straipsnio 1 punktas.

Tais atvejais, kai asmens duomenys gaunami ne tiesiogiai iš duomenų subjekto, duomenų valdytojas privalo pranešti asmeniui apie asmens duomenų kilmę. Bet kuriuo atveju duomenų valdytojas, be kita ko, privalo informuoti duomenų subjektus apie automatizuotą sprendimų priėmimą, įskaitant profiliavimą[533]. Galiausiai, jei duomenų valdytojas ketina tvarkyti asmens duomenis kitu tikslu nei tas, kuris iš pradžių buvo nurodytas duomenų subjektui, pagal tikslų apribojimo ir skaidrumo principus reikalaujama, kad duomenų valdytojas pateiktų duomenų subjektui informaciją apie šį naują tikslą. Duomenų valdytojai privalo pateikti informaciją prieš bet kokį tolesnį duomenų tvarkymą. Kitaip tariant, jeigu duomenų subjektas davė sutikimą tvarkyti asmens duomenis, duomenų valdytojas privalo gauti atnaujintą duomenų subjekto sutikimą, jeigu pasikeičia duomenų tvarkymo tikslas arba jeigu nustatomi papildomi duomenų tvarkymo tikslai.

Informacijos pateikimo laikas

BDAR išskiriami du scenarijai ir du momentai, kai duomenų valdytojas turi pateikti informaciją duomenų subjektui.

- Jeigu asmens duomenys gaunami tiesiogiai iš duomenų subjekto, duomenų valdytojas duomenų gavimo momentu privalo informuoti duomenų subjektą apie visą su juo susijusią informaciją ir teises pagal BDAR[534].

- Jeigu duomenų valdytojas ketina toliau tvarkyti asmens duomenis kitu tikslu, jis visą susijusią informaciją pateikia prieš pradėdamas tvarkyti duomenis.

Jeigu asmens duomenys iš duomenų subjekto nebuvo gauti tiesiogiai, duomenų valdytojas privalo duomenų subjektui pateikti informaciją apie duomenų tvarkymą „per pagrįstą laikotarpį nuo asmens duomenų gavimo, bet ne vėliau kaip per vieną mėnesį“ arba prieš atskleisdamas duomenis trečiajai šaliai[535].

Atnaujintos 108-osios konvencijos aiškinamojoje ataskaitoje nustatyta, kad jeigu duomenų subjektų neįmanoma informuoti pradedant tvarkyti duomenis, tai galima

533 Bendrojo duomenų apsaugos reglamento 13 straipsnio 2 dalis ir 14 straipsnio 2 dalies f punktas.

534 *Ten pat*, 13 straipsnio 1 ir 2 dalys, įvadiniai žodžiai, kuriais Bendrojo duomenų apsaugos reglamento nuostatose daroma nuoroda į informaciją apie prievolę taikyti „asmens duomenų gavimo metu“.

535 *Ten pat*, 13 straipsnio 3 dalis ir 14 straipsnio 3 dalis; taip pat žr. nuorodą į pagrįstus intervalus ir nepagrįstai nedelsiant pagal atnaujintos 108-osios konvencijos 8 straipsnio 1 dalies b punktą.

padaryti vėlesniame etape, pavyzdžiui, kai duomenų valdytojas dėl kokios nors priežasties susisiekia su duomenų subjektu[536].

Įvairūs informacijos pateikimo būdai

Pagal ET ir ES teisę duomenų valdytojas duomenų subjektams privalo pateikti nuoseklią, skaidrią, suprantamą ir lengvai prieinamą informaciją. Ji turi būti pateikta raštu arba kitomis priemonėmis, įskaitant elektronines priemones, aiškia, paprasta ir lengvai suprantama kalba. Teikdamas informaciją, duomenų valdytojas gali naudoti standartizuotas piktogramas, kad pateiktų informaciją lengvai matomu ir suprantamu būdu[537]. Pavyzdžiui, spyną vaizduojanti piktograma gali būti naudojama norint parodyti, kad duomenys renkami ir (arba) užšifruojami saugiai. Duomenų subjektai gali prašyti pateikti informaciją žodžiu. Informacija turi būti nemokama, išskyrus atvejus, kai duomenų subjekto prašymai yra akivaizdžiai nepagrįsti arba pertekliniai (t. y. pasikartojančio pobūdžio)[538]. Galimybė lengvai susipažinti su pateikta informacija yra itin svarbi, kad duomenų subjektas galėtų pasinaudoti savo teisėmis pagal ES duomenų apsaugos teisę.

Pagal sąžiningo duomenų tvarkymo principą reikalaujama, kad duomenų subjektai lengvai suprastų informaciją. Vartojama kalba turi būti pritaikyta tikslinei grupei. Kalbos lygis ir rūšis turėtų skirtis priklausomai nuo to, ar tikslinė auditorija yra, pavyzdžiui, suaugęs asmuo, vaikas, plačioji visuomenė ar akademinis ekspertas. Klausimas, kaip suderinti šį suprantamos informacijos aspektą, nagrinėjamas 29 straipsnio darbo grupės nuomonėje dėl labiau suderintos informacijos nuostatų. Taip skatinama vadinamųjų kelių sluoksnių pranešimų idėja[539] sudarant sąlygas duomenų subjektui nuspręsti, kiek išsamią informaciją jis pageidauja gauti. Tačiau toks informacijos pateikimo būdas neatleidžia duomenų valdytojo nuo prievolės pagal BDAR 6 ir 14 straipsnius. Duomenų valdytojas vis tiek privalo pateikti visą informaciją duomenų subjektui.

536 Atnaujintos 108-osios konvencijos aiškinamosios ataskaitos 70 punktas.

537 Europos Komisija, priimdama deleguotuosius aktus, toliau plėtos informaciją, kuri turi būti pateikta naudojant piktogramas, ir standartizuotų piktogramų pateikimo procedūras; žr. Bendrojo duomenų apsaugos reglamento 12 straipsnio 8 dalį.

538 Bendrojo duomenų apsaugos reglamento 12 straipsnio 1, 5 ir 7 dalys ir atnaujintos 108-osios konvencijos 9 straipsnio 1 dalies b punktas.

539 29 straipsnio darbo grupė (2004 m.), *Nuomonė Nr. 10/2004 dėl labiau suderintos informacijos nuostatų*, WP 100, Briuselis, 2004 m. lapkričio 25 d.

Vienas iš veiksmingiausių būdų teikti informaciją – duomenų valdytojo pradžios tinklalapyje pateikti atitinkamas nuostatas dėl informacijos, pavyzdžiui, interneto svetainės privatumo politiką. Vis dėlto nemažai gyventojų nesinaudoja internetu, todėl į tai reikėtų atsižvelgti rengiant įmonės arba valdžios institucijos informacijos politiką.

Svetainėje pateikiamas pranešimas apie tvarkomų asmens duomenų privatumą galėtų atrodyti taip:

Kas mes esame?

Duomenis tvarkantis duomenų valdytojas yra *Bed and Breakfast C&U*, įsteigtas [nurodomas adresas], tel. xxx; faks. xxx; e. pašto adresas info@c&u.com; duomenų apsaugos pareigūno kontaktiniai duomenys [xxx].

Informacinis pranešimas apie asmens duomenis yra mūsų viešbučio paslaugas reglamentuojančių nuostatų ir sąlygų sudedamoji dalis.

Kokius jūsų duomenis renkame?

Renkame šiuos jūsų asmens duomenis: jūsų vardas, pavardė, pašto adresas, telefono numeris, e. pašto adresas, informacija apie buvimą šalyje, kredito ir debeto kortelės numeris ir kompiuterių, kuriuos naudojote prisijungdami prie mūsų tinklapio, IP adresai arba domenų vardai.

Kodėl renkame jūsų asmens duomenis?

Jūsų duomenis tvarkome remdamiesi jūsų sutikimu ir rezervacijos tikslais, siekdami sudaryti ir vykdyti su jums siūlomomis paslaugomis susijusias sutartis ir laikytis reikalavimų, nustatytų teisės aktuose, pavyzdžiui, vietos mokesčių įstatyme, pagal kurį reikalaujama rinkti jūsų asmens duomenis, kad būtų galima sumokėti miesto apgyvendinimo mokestį.

Kaip tvarkome jūsų duomenis?

Jūsų asmens duomenys bus saugomi tris mėnesius. Jūsų duomenims nebus taikomos automatizuoto sprendimų priėmimo procedūros.

Mūsų įmonė *Bed and Breakfast C&U* griežtai laikosi saugumo procedūrų siekdama užtikrinti, kad jūsų asmens duomenims nebūtų pakenkta, jie nebūtų sunaikinti arba atskleisti trečiajai šaliai be jūsų leidimo ir kad būtų užkirstas kelias neteisėtai prieigai prie jų. Kompiuteriai, kuriuose saugoma informacija, laikomi saugioje aplinkoje, prie kurios ribojama fizinė prieiga. Naudojame saugias ugniasienes ir kitas priemones elektroninei prieigai apriboti. Jei duomenys turi būti perduoti trečiajai šaliai, reikalaujame, kad ji taikytų panašias jūsų asmens duomenų apsaugos priemones.

Visa mūsų renkama ir registruojama informacija skirta tik mūsų biurams. Prieiga prie asmens duomenų suteikiama tik tiems asmenims, kuriems reikalinga informacija, kad jie galėtų vykdyti savo pareigas pagal šią sutartį. Jūsų bus aiškiai paklausta, kada mums reikia informacijos jūsų tapatybei nustatyti. Prieš atskleisdami jums informaciją, galime paprašyti jūsų bendradarbiauti atliekant saugumo patikrinimus. Asmens duomenis, kuriuos mums pateikiate, galite bet kuriuo metu atnaujinti tiesiogiai susisiekę su mumis.

Kokios yra jūsų teisės?

Jūs turite teisę susipažinti su savo duomenimis, gauti savo duomenų kopiją, prašyti juos ištrinti ar ištaisyti arba prašyti, kad jūsų duomenys būtų persiųsti kitam duomenų valdytojui.

Su mumis galite susisiekti e. pašto adresu info@c&u.com ir pateikti prašymus. Į jūsų prašymą atsakysime per vieną mėnesį, tačiau jeigu jūsų prašymas yra pernelyg sudėtingas arba jeigu gauname per daug kitų prašymų, informuosime jus, kad šis terminas gali būti pratęstas dar dviem mėnesiams.

Galimybė susipažinti su savo asmens duomenimis

Turite teisę susipažinti su savo duomenimis ir, pateikę prašymą, gauti informaciją apie priežastis, kuriomis grindžiamas duomenų tvarkymas, prašyti juos ištrinti arba ištaisyti, taip pat teisę prieštarauti, kad būtų priimtas visiškai automatinis sprendimas neatsižvelgus į jūsų nuomonę. Su mumis galite susisiekti e. pašto adresu info@c&u.com ir pateikti prašymus. Taip pat turite teisę nesutikti, kad duomenys būtų tvarkomi, atsisakyti savo sutikimo ir pateikti skundą nacionalinei priežiūros institucijai, jei manote, kad šiuo duomenų tvarkymu pažeidžiama teisė, ir reikalauti sumokėti kompensaciją už žalą, padarytą dėl neteisėto duomenų tvarkymo.

Teisė pateikti skundą

Pagal BDAR reikalaujama, kad duomenų valdytojas informuotų duomenų subjektus apie vykdymo užtikrinimo mechanizmus pagal nacionalinę ir ES teisę tais atvejais, kai padaromi asmens duomenų saugumo pažeidimai. Duomenų valdytojas privalo informuoti duomenų subjektus apie jų teisę kreiptis į priežiūros instituciją ir prireikus nacionaliniam teismui pateikti skundą apie asmens duomenų saugumo pažeidimą[540]. ET teisėje taip pat numatyta duomenų subjektų teisė būti informuotiems apie jų teisių įgyvendinimo priemones, įskaitant teisę pasinaudoti 9 straipsnio 1 dalies f punkte nustatyta teisių gynimo priemone.

Prievolės informuoti išimtys

BDAR nustatyta prievolės informuoti išimtis. Pagal BDAR 13 straipsnio 4 dalį ir 14 straipsnio 5 dalį prievolė informuoti duomenų subjektus netaikoma, jeigu duomenų subjektas jau turi visą susijusią informaciją[541]. Be to, tais atvejais, kai asmens duomenys buvo gauti ne iš duomenų subjekto, prievolė informuoti netaikoma, jei informacijos pateikti neįmanoma arba neproporcinga, visų pirma tais atvejais, kai asmens duomenys tvarkomi archyvavimo tikslais viešojo intereso labui, mokslinių ar istorinių tyrimų tikslais arba statistiniais tikslais[542].

Be to, pagal BDAR valstybės narės turi tam tikrą veiksmų laisvę apriboti pagal reglamentą asmenims nustatytas pareigas ir suteiktas teises, jei tai yra būtina ir proporcinga priemonė demokratinėje visuomenėje, pavyzdžiui, siekiant užtikrinti nacionalinį ir visuomenės saugumą, gynybą, teisminių tyrimų ir procesų apsaugą arba ekonominių ir finansinių interesų, taip pat privačių interesų, kurie yra svarbesni nei duomenų apsaugos interesai, apsaugą[543].

Bet kokios išimtys arba apribojimai turi būti būtini demokratinėje visuomenėje ir proporcingi siekiamam tikslui. Itin išskirtiniais atvejais, pavyzdžiui, dėl medicininių diagnozių, siekiant užtikrinti duomenų subjekto apsaugą gali prireikti apriboti skaidrumą; tai visų pirma yra susiję su kiekvieno duomenų subjekto teisės susipažinti su duomenimis apribojimu[544]. Tačiau atsižvelgiant į minimalų duomenų apsaugos lygį,

540 Bendrojo duomenų apsaugos reglamento 13 straipsnio 2 dalies d punktas ir 14 straipsnio 2 dalies e punktas; atnaujintos 108-osios konvencijos 8 straipsnio 1 dalies f punktas.

541 *Ten pat*, 13 straipsnio 4 dalis ir 14 straipsnio 5 dalies a punktas.

542 *Ten pat*, 14 straipsnio 5 dalies b–e punktai.

543 Bendrojo duomenų apsaugos reglamento 23 straipsnio 1 dalis.

544 Bendrojo duomenų apsaugos reglamento 15 straipsnis.

nacionalinėje teisėje turi būti paisoma ES teisėje nustatytų pagrindinių teisių ir laisvių esmės[545]. Šiuo tikslu reikia, kad nacionalinėje teisėje būtų įtvirtintos konkrečios nuostatos, kuriose paaiškinamas duomenų tvarkymo tikslas, tvarkomų asmens duomenų kategorijos, apsaugos priemonės ir kiti procedūriniai reikalavimai[546].

Jeigu duomenys renkami mokslinių arba istorinių tyrimų tikslais, statistiniais tikslais arba archyvavimo tikslais viešojo intereso labui, Sąjungos ar valstybių narių teisėje gali būti numatytos nuo prievolės pranešti nukrypti leidžiančios nuostatos, jei dėl to gali tapti neįmanoma arba gali būti labai trukdoma siekti konkrečių tikslų[547].

ET teisėje yra panašių apribojimų, pagal kuriuos atnaujintos 108-osios konvencijos 9 straipsnyje duomenų subjektams suteikiamos teisės, laikantis griežtų sąlygų, gali būti apribojamos pagal atnaujintos 108-osios konvencijos 11 straipsnį. Be to, pagal atnaujintos 108-osios konvencijos 8 straipsnio 2 dalį duomenų valdytojams nustatyta prievolė skaidriai tvarkyti duomenis netaikoma tais atvejais, kai duomenų subjektas jau turi informacijos.

Teisė susipažinti su savo duomenimis

Pagal ET teisę asmens teisė susipažinti su savo duomenimis yra aiškiai pripažinta atnaujintos 108-osios konvencijos 9 straipsnyje. Jame nustatyta, kad kiekvienas asmuo turi teisę paprašęs gauti informaciją apie jo asmens duomenų tvarkymą, kuri perduodama suprantamu būdu. Teisė susipažinti su duomenimis pripažinta ne tik atnaujintos 108-osios konvencijos nuostatose, bet ir EŽTT praktikoje. EŽTT ne kartą konstatavo, kad asmenys turi teisę susipažinti su informacija apie savo asmens duomenis ir kad ši teisė kildinama iš poreikio gerbti privatų gyvenimą[548]. Tačiau teisė susipažinti su viešų arba privačių organizacijų saugomais asmens duomenimis tam tikromis aplinkybėmis gali būti ribojama[549].

Pagal ES teisę teisė susipažinti su savo duomenimis aiškiai pripažįstama BDAR 15 straipsnyje, be to, ES pagrindinių teisių chartijos 8 straipsnio 2 dalyje ji įvardijama

545 Bendrojo duomenų apsaugos reglamento 23 straipsnio 1 punktas.

546 *Ten pat*, 23 straipsnio 2 punktas.

547 *Ten pat*, 89 straipsnio 2 ir 3 dalys.

548 EŽTT, *Gaskin prieš Jungtinę Karalystę*, Nr. 10454/83, 1989 m. liepos 7 d.; EŽTT, *Odièvre prieš Prancūziją* (DK), Nr. 42326/98, 2003 m. vasario 13 d.; EŽTT, *K. H. ir kiti prieš Slovakiją*, Nr. 32881/04, 2009 m. balandžio 28 d.; EŽTT, *Godelli prieš Italiją*, Nr. 33783/09, 2012 m. rugsėjo 25 d.

549 EŽTT, *Leander prieš Švediją*, Nr. 9248/81, 1987 m. kovo 26 d.

kaip pagrindinės teisės į asmens duomenų apsaugą sudedamoji dalis[550]. Asmens teisė gauti prieigą prie savo asmens duomenų yra pagrindinis Europos duomenų apsaugos teisės aspektas[551].

BDAR nustatyta, kad kiekvienas duomenų subjektas turi teisę susipažinti su savo asmens duomenimis ir su tam tikra informacija apie duomenų tvarkymą, kurią duomenų valdytojai privalo pateikti[552]. Visų pirma kiekvienas duomenų subjektas turi teisę gauti (iš duomenų valdytojo) patvirtinimą, ar su juo susiję duomenys yra tvarkomi, ir informaciją bent apie:

- duomenų tvarkymo tikslus;
- atitinkamų duomenų kategorijas;
- gavėjus, kuriems atskleidžiami duomenys, arba tokių gavėjų kategorijas;
- laikotarpį, kurį duomenis ketinama saugoti, arba, jei tai neįmanoma, kriterijus, kuriais remiantis nustatomas toks laikotarpis;
- teisių ištaisyti ar ištrinti asmens duomenis arba apriboti asmens duomenų tvarkymą buvimą;
- teisę pateikti skundą priežiūros institucijai;
- visą turimą informaciją apie tvarkomų duomenų šaltinį, jei duomenys renkami ne iš duomenų subjekto;
- automatizuoto sprendimų priėmimo atveju – bet kokio automatizuoto duomenų tvarkymo logiką.

Duomenų valdytojas privalo pateikti duomenų subjektui tvarkomų asmens duomenų kopiją. Bet kokia duomenų subjektui perduodama informacija turi būti

550 Taip pat žr. ESTT sujungtas bylas C-141/12 ir C-372/12, *YS prieš Minister voor Immigratie, Integratie en Asiel* ir *Minister voor Immigratie, Integratie en Asiel prieš M ir S*, 2014 m. liepos 17 d.; ESTT, C-615/13 P, *ClientEarth, Pesticide Action Network Europe (PAN Europe) prieš Europos maisto saugos tarnybą (EFSA), Europos Komisiją*, 2015 m. liepos 16 d.

551 ESTT, sujungtos bylos C-141/12 ir C-372/12, *YS prieš Minister voor Immigratie, Integratie en Asiel* ir *Minister voor Immigratie, Integratie en Asiel prieš M ir S*, 2014 m. liepos 17 d.

552 Bendrojo duomenų apsaugos reglamento 15 straipsnio 1 punktas.

pateikta suprantama forma ir tai reiškia, kad duomenų valdytojas privalo užtikrinti, kad duomenų subjektas galėtų suprasti pateikiamą informaciją. Pavyzdžiui, paprastai nepakanka techninių santrumpų, koduotų terminų ar akronimų atsakant į prašymą leisti susipažinti su duomenimis, nebent būtų paaiškinta šių terminų reikšmė. Jeigu sprendimai priimami automatizuotai, įskaitant profiliavimą, reikia paaiškinti bendruosius automatizuoto sprendimų priėmimo loginius principus, įskaitant kriterijus, pagal kuriuos buvo vertinamas duomenų subjektas. Panašūs reikalavimai galioja ir **ET teisėje**[553].

Pavyzdys. Galimybė susipažinti su savo asmens duomenimis padeda duomenų subjektui nustatyti, ar duomenys yra tikslūs. Todėl labai svarbu duomenų subjektą suprantama forma informuoti ne tik apie faktiškai tvarkomus asmens duomenis, bet ir apie kategorijas, kuriomis remiantis tvarkomi šie asmens duomenys, pavyzdžiui, vardas ir pavardė, IP adresas, geografinės vietos nustatymo koordinatės, kreditinės kortelės numeris ir pan.

Informacija apie duomenų šaltinį, t. y. kai duomenys nerenkami iš duomenų subjekto, turi būti pateikta atsakant į prašymą leisti susipažinti su duomenimis, jeigu tokia informacija yra prieinama. Ši nuostata turi būti suprantama atsižvelgiant į sąžiningumo, skaidrumo ir atskaitomybės principus. Duomenų valdytojas negali sunaikinti informacijos apie duomenų šaltinį, kad būtų atleistas nuo informacijos atskleidimo, išskyrus atvejus, kai ji būtų pašalinta nepaisant to, kad buvo gautas prašymas leisti susipažinti su duomenimis, ir jis vis tiek turi laikytis savo bendrųjų atskaitomybės reikalavimų.

Kaip nustatyta ESTT jurisprudencijoje, teisė susipažinti su asmens duomenimis negali būti nepagrįstai ribojama nustatant terminus. Duomenų subjektams taip pat būtina suteikti galimybę gauti informacijos apie anksčiau vykdytas duomenų tvarkymo operacijas.

Pavyzdys. Byloje *Rijkeboer*[554] ESTT buvo prašoma nustatyti, ar asmens teisė susipažinti su informacija apie asmens duomenų gavėjus arba tokių gavėjų kategorijas ir duomenų turiniu galėjo būti ribojama nustatant vienų metų terminą tokiam prašymui pateikti.

553 Žr. atnaujintos 108-osios konvencijos 8 straipsnio 1 dalies c punktą.

554 ESTT, C-553/07, *College van burgemeester en wethouders van Rotterdam prieš M. E. E. Rijkeboer*, 2009 m. gegužės 7 d.

Siekdamas nustatyti, ar ES teisės aktais leidžiama nustatyti tokį terminą, ESTT nusprendė 12 straipsnį aiškinti atsižvelgdamas į direktyvos tikslus. Pirmiausia ESTT nurodė, kad teisė susipažinti su duomenimis yra būtina, kad duomenų subjektas galėtų pasinaudoti teise reikalauti, kad duomenų valdytojas ištaisytų, ištrintų ar blokuotų savo duomenis, arba pranešti trečiosioms šalims, kurioms duomenys buvo atskleisti, apie tokį ištaisymą, ištrynimą ar blokavimą. Veiksminga teisė susipažinti su duomenimis taip pat yra būtina, kad duomenų subjektas galėtų įgyvendinti savo teisę nesutikti, kad būtų tvarkomi jo duomenys, arba savo teisę pateikti skundą ir reikalauti atlyginti žalą[555].

Siekdamas užtikrinti duomenų subjektams suteiktų teisių praktinį poveikį, ESTT nusprendė, kad „ta teisė būtinai turi būti susijusi su praeitimi. Kitu atveju suinteresuotas asmuo negalėtų veiksmingai pasinaudoti turima teise pasiekti, kad neteisėtais arba neteisingais laikomi duomenys būtų ištaisyti, ištrinti arba užblokuoti, bei pareikšti ieškinį teisme ir prisiteisti patirtos žalos atlyginimą."

6.1.2. Teisė ištaisyti duomenis

Pagal ES ir **ET teisę** duomenų subjektai turi teisę ištaisyti savo asmens duomenis. Asmens duomenų tikslumas yra labai svarbus siekiant užtikrinti aukšto lygio duomenų subjektų duomenų apsaugą[556].

Pavyzdys. Byloje *Ciubotaru prieš Moldovą*[557] pareiškėjas negalėjo pakeisti savo etninės kilmės registracijos oficialiuose įrašuose iš moldavo į rumuną, nes nepagrindė savo prašymo. EŽTT manė, kad valstybės, registruodamos asmenų kilmę, galėjo reikalauti pateikti objektyvius įrodymus. Institucijos galėjo atsisakyti registruoti etninę kilmę, jeigu toks prašymas buvo subjektyvus ir nepagrįstas tvirtais įrodymais. Tačiau pareiškėjo reikalavimas buvo pagrįstas ne tik subjektyviu savo etninės kilmės suvokimu; jis sugebėjo pateikti objektyviai patikrinamus ryšius su rumunų etnine grupe, pavyzdžiui, kalba, vardas ir pavardė, bendrumas ir kt. Vis dėlto pagal nacionalinę teisę pareiškėjo buvo prašoma pateikti įrodymus, kad jo tėvai priklauso rumunų etninei grupei. Atsižvelgiant į istorines Moldovos realijas, dėl tokio

555 Bendrojo duomenų apsaugos reglamento 15 straipsnio 1 dalies c ir f punktai, 16 straipsnis, 17 straipsnio 2 dalis, 21 straipsnis ir VIII skyrius.

556 *Ten pat*, 16 straipsnis ir 65 konstatuojamoji dalis; atnaujintos 108-osios konvencijos 9 straipsnio 1 dalies e punktas.

557 EŽTT, *Ciubotaru prieš Moldovą*, Nr. 27138/04, 2010 m. balandžio 27 d., 51 ir 59 punktai.

reikalavimo atsirado neįveikiama kliūtis registruoti kitą etninę tapatybę nei ta, kurią Sovietų valdžios institucijos užregistravo dėl pareiškėjo tėvų. Kadangi pareiškėjo prašymas nebuvo nagrinėjamas atsižvelgiant į objektyviai patikrinamus įrodymus, valstybė nesilaikė teigiamos prievolės užtikrinti tinkamos pagarbos pareiškėjo privačiam gyvenimui. Teismas padarė išvadą, kad buvo pažeistas EŽTK 8 straipsnis.

Tam tikrais atvejais duomenų subjektui pakanka paprasčiausiai paprašyti ištaisyti duomenis, pavyzdžiui, vardo ar pavardės rašybą, pakeisti adresą arba telefono numerį. Pagal **ES teisę** ir **ET teisę** netikslūs asmens duomenys turi būti ištaisyti nepagrįstai arba pernelyg nedelsiant[558]. Tačiau jei tokie prašymai yra susiję su teisiškai svarbiais klausimais, pavyzdžiui, duomenų subjekto teisine tapatybe arba tinkama teisinių dokumentų pristatymo vieta, gali nepakakti prašymų ištaisyti duomenis ir duomenų valdytojas gali turėti teisę reikalauti pateikti tariamo netikslumo įrodymus. Dėl tokių reikalavimų duomenų subjektui neturi atsirasti nepagrįsta prievolė įrodyti, dėl kurios duomenų subjektai negalėtų ištaisyti savo asmens duomenų. EŽTT nustatė EŽTK 8 straipsnio pažeidimus keliose bylose, kuriose pareiškėjas negalėjo ginčyti slaptuose registruose saugomos informacijos tikslumo[559].

Pavyzdys. Byloje *Cemalettin Canli prieš Turkiją*[560] EŽTT nustatė EŽTK 8 straipsnio pažeidimą dėl neteisingo policijos pranešimo baudžiamajame procese.

Pareiškėjas du kartus dalyvavo baudžiamajame procese dėl tariamo dalyvavimo neteisėtose organizacijose, tačiau nebuvo nuteistas. Kai pareiškėjas buvo dar kartą areštuotas ir jam buvo pareikšti kaltinimai dėl kitos nusikalstamos veikos, policija baudžiamajam teismui pateikė pranešimą, pavadintą *informacija apie papildomas nusikalstamas veikas*, kuriame buvo nurodyta, kad pareiškėjas priklauso dviem neteisėtoms organizacijoms. Pareiškėjo prašymas pakeisti pranešimą ir policijos įrašus nebuvo patenkintas. EŽTT nusprendė, kad policijos ataskaitoje pateikta informacija patenka į EŽTK 8 straipsnio taikymo sritį, nes sistemingai renkama vieša informacija, saugoma valdžios institucijų turimose bylose, taip pat gali patekti į „privataus

558 Bendrojo duomenų apsaugos reglamento 16 straipsnis; atnaujintos 108-osios konvencijos 9 straipsnio 1 dalis.

559 EŽTT, *Rotaru prieš Rumuniją* (DK), Nr. 28341/95, 2000 m. gegužės 4 d.

560 EŽTT, *Cemalettin Canli prieš Turkiją*, Nr. 22427/04, 2008 m. lapkričio 18 d., 33 ir 42–43 punktai; EŽTT, *Dalea prieš Prancūziją*, Nr. 964/07, 2010 m. vasario 2 d.

gyvenimo“ sąvoką. Be to, policijos pranešimas buvo neteisingai parengtas ir jis baudžiamajam teismui buvo pateiktas nesilaikant nacionalinės teisės. EŽTT padarė išvadą, kad buvo pažeistas EŽTK 8 straipsnis.

Vykstant civiliniam procesui arba procesui valdžios institucijoje, siekiant nuspręsti, ar duomenys yra teisingi, duomenų subjektas gali prašyti, kad prie jo duomenų bylos būtų pridėtas įrašas arba pastaba, kuriuose būtų nurodyta, kad tikslumas yra ginčijamas ir kad dar nepriimtas oficialus sprendimas[561]. Šiuo laikotarpiu duomenų valdytojas neturi pateikti duomenų kaip teisingų arba jų keisti, ypač trečiosioms šalims.

6.1.3. Teisė reikalauti ištrinti duomenis (teisė būti pamirštam)

Labai svarbu duomenų subjektams suteikti teisę reikalauti ištrinti jų duomenis, kad būtų veiksmingai taikomi duomenų apsaugos principai, visų pirma duomenų kiekio mažinimo principas (asmens duomenys turi apimti tik tuos duomenis, kurie yra būtini siekiant tikslų, kuriais jie yra tvarkomi). Todėl teisę reikalauti ištrinti duomenis galima rasti ET ir ES teisės aktuose[562].

Pavyzdys. Byloje *Segerstedt-Wiberg ir kiti prieš Švediją*[563] pareiškėjai buvo susiję su tam tikromis liberalų ir komunistų politinėmis partijomis. Jie įtarė, kad informacija apie juos buvo įtraukta į saugumo policijos įrašus, ir paprašė ją ištrinti. EŽTT teigiamai įvertino tai, kad aptariami duomenys buvo saugomi remiantis teisiniu pagrindu ir buvo tvarkomi teisėtu tikslu. Vis dėlto, kiek tai susiję su kai kuriais pareiškėjais, EŽTT nusprendė, kad tolesnis duomenų saugojimas buvo neproporcingas jų privataus gyvenimo apribojimas. Pavyzdžiui, vieno pareiškėjo atveju valdžios institucijos išsaugojo informaciją, kad 1969 m. jis tariamai palaikė smurtinį pasipriešinimą policijai bandant kontroliuoti demonstracijas. EŽTT nustatė, kad ši informacija negalėjo būti susijusi su kokiu nors svarbiu nacionalinio saugumo interesu, ypač atsižvelgiant į jos istorinį pobūdį. EŽTT nustatė, kad buvo pažeistas EŽTK 8 straipsnis dėl keturių iš penkių pareiškėjų, nes, atsižvelgiant į tai, kad nuo tariamų pareiškėjų veiksmų praėjo daug laiko, tolesnis jų duomenų saugojimas neturėjo reikšmės.

561 Bendrojo duomenų apsaugos reglamento 18 straipsnis ir 67 konstatuojamoji dalis.

562 *Ten pat*, 17 straipsnis.

563 EŽTT, *Segerstedt-Wiberg ir kiti prieš Švediją*, Nr. 62332/00, 2006 m. birželio 6 d., 89 ir 90 punktai; taip pat žr., pvz., EŽTT, *M. K. prieš Prancūziją*, Nr. 19522/09, 2013 m. balandžio 18 d.

Pavyzdys. Byloje *Brunet prieš Prancūziją*[564] pareiškėjas nepalankiai vertino jo asmens duomenų saugojimą policijos duomenų bazėje, kurioje buvo informacija apie nuteistus asmenis, kaltinamuosius ir aukas. Nors baudžiamoji byla pareiškėjui buvo nutraukta, jo duomenys buvo įtraukti į duomenų bazę. EŽTT nusprendė, kad buvo pažeistas EŽTK 8 straipsnis. Prieidamas prie išvados, EŽTT laikėsi nuomonės, kad pareiškėjas praktiškai neturėjo jokios galimybės duomenų bazėje ištrinti savo asmens duomenis. EŽTT taip pat išnagrinėjo duomenų bazėje esančios informacijos pobūdį ir manė, kad taip pažeidžiamas pareiškėjo privatumas, nes jie apėmė informaciją apie jo tapatybę ir asmenybę. Be to, jis nustatė, kad asmens duomenų saugojimo duomenų bazėje laikotarpis, kuris truko 20 metų, buvo pernelyg ilgas, ypač dėl to, kad nė vienas teismas niekada nebuvo nuteisęs pareiškėjo.

Atnaujintoje 108-ojoje konvencijoje aiškiai pripažįstama, kad kiekvienas asmuo turi teisę reikalauti ištrinti netikslius, neteisingus arba neteisėtai tvarkomus duomenis[565].

ES teisėje duomenų subjektų prašymų ištrinti duomenis teisinis reglamentavimas nustatytas BDAR 17 straipsnyje. Teisė reikalauti, kad asmens duomenys būtų nedelsiant ištrinti, taikoma, kai:

- asmens duomenų nebereikia tais tikslais, kuriais jie buvo surinkti ar kitaip tvarkomi;
- duomenų subjektas atšaukia sutikimą, kuriuo grindžiamas duomenų tvarkymas, ir nėra jokio kito teisinio pagrindo tvarkyti duomenis;
- duomenų subjektas nesutinka, kad būtų tvarkomi duomenys, ir nėra jokių viršesnių teisėtų duomenų tvarkymo pagrindų;
- asmens duomenys buvo tvarkomi neteisėtai;
- asmens duomenys turi būti ištrinti laikantis Sąjungos arba valstybės narės teisėje, kuri taikoma duomenų valdytojui, nustatytos teisinės prievolės;

564 EŽTT, *Brunet prieš Prancūziją*, Nr. 21010/10, 2014 m. rugsėjo 18 d.

565 Atnaujintos 108-osios konvencijos 9 straipsnio 1 dalies e punktas.

- buvo surinkti asmens duomenys, susiję su informacinės visuomenės paslaugų siūlymu vaikams pagal BDAR 8 straipsnį[566].

Prievolė įrodyti, kad duomenys tvarkomi teisėtai, tenka duomenų valdytojams, nes jie atsako už duomenų tvarkymo teisėtumą[567]. Pagal atskaitomybės principą duomenų valdytojas privalo bet kuriuo metu sugebėti įrodyti, kad jis duomenis tvarko remdamasis patikimu teisėtu pagrindu, nes kitu atveju duomenų tvarkymą būtina sustabdyti[568]. BDAR nustatytos teisės būti pamirštam išimtys, įskaitant atvejus, kai asmens duomenų tvarkymas būtinas:

- siekiant pasinaudoti teise į saviraiškos ir informacijos laisvę;
- siekiant laikytis Sąjungos ar valstybės narės teisėje, kuri taikoma duomenų valdytojui, nustatytos teisinės prievolės, pagal kurią reikalaujama tvarkyti duomenis, arba siekiant atlikti užduotį, vykdomą viešojo intereso labui, arba vykdant duomenų valdytojui pavestas viešosios valdžios funkcijas;
- dėl viešojo intereso priežasčių visuomenės sveikatos srityje;
- archyvavimo tikslais viešojo intereso labui, mokslinių ar istorinių tyrimų tikslais arba statistiniais tikslais;
- siekiant pareikšti, vykdyti arba apginti teisinius reikalavimus[569].

ES patvirtino teisės reikalauti ištrinti duomenis svarbą siekiant užtikrinti aukšto lygio duomenų apsaugą.

Pavyzdys. Byloje *Google Spain*[570] ESTT nagrinėjo, ar *Google* privalėjo iš paieškos sąrašo rezultatų pašalinti pasenusią informaciją apie pareiškėjo finansinius sunkumus. Be kita ko, *Google* ginčijo atsakomybę, teigdama, kad ji tik pateikia saitą į leidėjo tinklalapį, kuriame yra informacija, šiuo

566 Bendrojo duomenų apsaugos reglamento 17 straipsnio 1 punktas.

567 *Ten pat*.

568 *Ten pat*, 5 straipsnio 2 punktas.

569 *Ten pat*, 17 straipsnio 3 punktas.

570 ESTT, C-131/12, *Google Spain SL, Google Inc. prieš Agencia Española de Protección de Datos (AEPD), Mario Costeja González* (DK), 2014 m. gegužės 13 d., 55–58 punktai.

atveju – laikraštį, kuriame pranešama apie pareiškėjo nemokumo problemas[571]. *Google* teigė, kad prašymas ištrinti svetainėje pasenusią informaciją turėtų būti pateikiamas svetainės prieglobos paslaugų teikėjui, o ne *Google*, kuris paprasčiausiai pateikia saitą į originalų tinklalapį. ESTT nusprendė, kad *Google*, atlikdama informacijos paiešką internete ir tinklalapių paiešką ir indeksuodama turinį, kad pateiktų paieškos rezultatus, tampa duomenų valdytoja, kuriai taikomos ES teisėje nustatytos pareigos ir prievolės.

ESTT paaiškino, kad internetinės paieškos sistemos ir paieškos rezultatai, kuriuose pateikiami asmens duomenys, gali padėti nustatyti išsamų asmens profilį[572]. Paieškos sistemos padeda užtikrinti, kad tokiame rezultatų sąraše esanti informacija būtų visur prieinama. Atsižvelgiant į tai, kad apribojimas gali būti rimtas, jo negalima pateisinti paprasčiausiu tokios paieškos sistemos operatoriaus ekonominiu interesu, susijusiu su tokiu duomenų tvarkymu. Būtina ieškoti tinkamos pusiausvyros, visų pirma tarp interneto naudotojų teisėto intereso susipažinti su informacija ir duomenų subjekto pagrindinių teisių pagal ES pagrindinių teisių chartijos 7 ir 8 straipsnius. Atsižvelgiant į vis didesnį visuomenės skaitmeninimą, reikalavimas, kad asmens duomenys būtų tikslūs ir kad jų nebūtų daugiau nei būtina (t. y. teikti informaciją visuomenei), yra labai svarbūs siekiant užtikrinti aukštą asmens duomenų apsaugos lygį. „Duomenų valdytojas, kiek tai susiję su tuo duomenų tvarkymu, neviršydamas savo pareigų, įgaliojimų ir gebėjimų, turi užtikrinti, kad tas duomenų tvarkymas atitiktų ES teisės reikalavimus“, kad nustatytos teisinės garantijos būtų visiškai veiksmingos[573]. Tai reiškia, kad teisė reikalauti ištrinti asmens duomenis, kai duomenų tvarkymas yra pasenęs arba nebereikalingas, taip pat taikomas duomenų valdytojams, kurie pakartotinai skelbia informaciją[574].

---

571 *Google* taip pat ginčijo ES duomenų apsaugos taisyklių taikymą dėl to, kad *Google Inc.* yra įsisteigusi JAV, o šioje byloje nagrinėjami asmens duomenys taip pat buvo tvarkomi JAV. Antrasis argumentas dėl ES duomenų apsaugos teisės netaikymo susijęs su teiginiu, kad paieškos sistemos negali būti laikomos „valdytojomis“, kiek tai susiję su jų rezultatuose pateikiamais duomenimis, nes jos nežino apie šiuos duomenis ir jų nekontroliuoja. ESTT atmetė abu argumentus, nurodydamas, kad tuo atveju taikoma Direktyva 95/46/EB, ir toliau nagrinėjo joje garantuojamų teisių, visų pirma teisės reikalauti ištrinti asmens duomenis, apimtį.

572 *Ten pat*, 36, 38, 80–81 ir 97 punktai.

573 *Ten pat*, 81–83 punktai.

574 ESTT, C-131/12, *Google Spain SL, Google Inc. prieš Agencia Española de Protección de Datos (AEPD), Mario Costeja González* (DK), 2014 d. gegužės 13 d., 88 punktas. Taip pat žr. 29 straipsnio duomenų apsaugos darbo grupės (2014 m.), *ESTT sprendimo „Google Spain and Inc prieš Agencia Española de Protección de Datos (AEPD) ir Mario Costeja González“ (C-131/12) įgyvendinimo rekomendacijas*, WP 225, Briuselis, 2014 m. lapkričio 26 d., ir Ministrų Komiteto rekomendaciją CM/Rec 2012(3) valstybėms narėms dėl žmogaus teisių apsaugos atsižvelgiant į paieškos sistemas, 2012 m. balandžio 4 d.

Nagrinėdamas, ar *Google* turėjo pašalinti su pareiškėju susijusias nuorodas, ESTT nusprendė, kad tam tikromis sąlygomis asmenys turi teisę reikalauti, kad jų asmens duomenys būtų ištrinti. Šia teise galima pasinaudoti tais atvejais, kai su asmeniu susijusi informacija yra netiksli, netinkama, nereikšminga arba perteklinė duomenų tvarkymo tikslais. ESTT pripažino, kad ši teisė nėra absoliuti; ją būtina suderinti su kitomis teisėmis ir interesais, visų pirma su plačiosios visuomenės interesu ir teise susipažinti su tam tikra informacija. Kiekvieną prašymą ištrinti duomenis būtina įvertinti atskirai, kad būtų užtikrinta pusiausvyra tarp, viena vertus, duomenų subjekto pagrindinių teisių į asmens duomenų apsaugą ir privatų gyvenimą ir, kita vertus, visų interneto naudotojų, įskaitant leidėjus, teisėtų interesų. ESTT pateikė rekomendacijas dėl veiksnių, į kuriuos reikia atsižvelgti nustatant teisių pusiausvyrą. Nagrinėjamos informacijos pobūdis yra ypač svarbus veiksnys. Jeigu informacija yra neskelbtina atsižvelgiant į asmens privatų gyvenimą ir jeigu nėra viešojo intereso, kad informacija būtų prieinama, duomenų apsauga ir privatumas būtų viršesnis už plačiosios visuomenės teisę susipažinti su informacija. Priešingai, jeigu paaiškėja, kad duomenų subjektas yra visuomenės veikėjas arba kad informacija yra tokio pobūdžio, kad galima pateisinti galimybę plačiajai visuomenei leisti susipažinti su tokia informacija, tuomet remiantis plačiosios visuomenės viršesniu interesu susipažinti su informacija gali būti pateisinamas duomenų subjekto pagrindinių teisių į duomenų apsaugą ir privatumą apribojimas.

Remdamasi sprendimu, 29 straipsnio darbo grupė priėmė ESTT sprendimo įgyvendinimo rekomendacijas[575]. Rekomendacijose pateikiamas bendrų kriterijų sąrašas, kuriuos turi naudoti priežiūros institucijos nagrinėdamos skundus, susijusius su asmenų prašymais ištrinti duomenis, paaiškinant teisės reikalauti ištrinti duomenis turinį, ir jie turi padėti šioms institucijoms nustatyti šių teisių įgyvendinimo pusiausvyrą. Rekomendacijose pakartojama, kad vertinimą reikia atlikti kiekvienu konkrečiu atveju. Kadangi teisė būti pamirštam nėra absoliuti, prašymo rezultatas gali skirtis priklausimai nuo nagrinėjamos bylos. Tai taip pat atsispindi ESTT jurisprudencijoje po sprendimo *Google* byloje.

575 29 straipsnio darbo grupė (2014 m.), *ESTT sprendimo „Google Spain and Inc prieš Agencia Española de Protección de Datos (AEPD) ir Mario Costeja González“ (C-131/12) įgyvendinimo rekomendacijos*, WP 225, Briuselis, 2014 m. lapkričio 26 d.

Pavyzdys. Byloje *Camera di Commercio di Lecce prieš Manni*[576] ESTT privalėjo nagrinėti, ar asmuo turėjo teisę ištrinti savo asmens duomenis, kurie buvo paskelbti viešame įmonių registre, kai jo įmonė nutraukė veiklą. S. Manni prašė Lečės prekybos rūmų ištrinti jo asmens duomenis iš to registro, kai išsiaiškino, kad potencialūs klientai ieškojo informacijos registre ir matė, kad jis anksčiau buvo įmonės, kurios bankrotas buvo paskelbtas daugiau nei prieš dešimt metų, administratorius. Pareiškėjas manė, kad ši informacija galėjo atgrasyti potencialius klientus.

Nustatydamas S. Manni teisės į jo duomenų apsaugą ir plačiosios visuomenės interesą susipažinti su informacija pusiausvyrą, ESTT pirmiausia nagrinėjo viešo registro paskirtį. Jis nurodė, kad pareiga atskleisti informaciją buvo nustatyta įstatyme, visų pirma ES direktyvoje, siekiant sudaryti sąlygas trečiosioms šalims lengviau susipažinti su informacija apie įmonę. Todėl trečiosioms šalims turėtų būti suteikta galimybė susipažinti su pagrindiniais įmonės dokumentais ir kita su įmone susijusia informacija, „ypač duomeni[mi]s apie asmenis, kurie yra įgalioti prisiimti įsipareigojimus bendrovės vardu“, be to, joms turėtų būti suteikta galimybė patikrinti tokius duomenis. Informacijos atskleidimo tikslas taip pat buvo užtikrinti teisinį tikrumą atsižvelgiant į intensyvesnę prekybą tarp valstybių narių, užtikrinant, kad trečiosios šalys galėtų susipažinti su visa svarbia informacija apie įmones visoje ES.

ESTT taip pat pažymėjo, kad net praėjus tam tikram laikui ir net likvidavus įmonę, su ja susijusios teisės ir teisinės prievolės dažnai išlieka. Ginčai, susiję su likvidavimu, gali būti ilgi, o klausimai, susiję su įmone, jos vadovais ir likvidatoriais, gali kilti praėjus daugybei metų po bendrovės veiklos nutraukimo. ESTT nusprendė, kad, atsižvelgiant į galimų scenarijų įvairovę ir kiekvienoje valstybėje narėje nustatytų senaties terminų skirtumus, „dabartinėmis aplinkybėmis neįmanoma nustatyti vieno termino, skaičiuojamo nuo bendrovės likvidavimo, kuriam pasibaigus nebūtų būtina įrašyti minėtų duomenų į registrą ir juos skelbti“. Atsižvelgdamas į teisėtą informacijos atskleidimo tikslą ir į sunkumus nustatant laikotarpį, kuriam pasibaigus asmens duomenys galėtų būti ištrinti iš registro nedarant žalos trečiųjų šalių interesams, ESTT nustatė, kad ES duomenų apsaugos taisyklėmis neužtikrinama asmenų, esančių tokioje padėtyje kaip S. Manni, teisė reikalauti ištrinti asmens duomenis.

576 ESTT, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce prieš Salvatore Manni*, 2017 m. kovo 9 d.

Jeigu duomenų valdytojas paskelbė asmens duomenis ir reikalaujama, kad jis ištrintų informaciją, duomenų valdytojas įpareigojamas ir privalo imtis „reikalingų“ priemonių, kad informuotų kitus duomenų valdytojus, kurie tvarko tokius pat duomenis, apie duomenų subjekto teisę reikalauti ištrinti duomenis. Duomenų valdytojas, vykdydamas savo veiklą, privalo atsižvelgti į prieinamas technologijas ir įgyvendinimo išlaidas[577].

6.1.4. Teisė apriboti duomenų tvarkymą

BDAR 18 straipsnyje duomenų subjektams suteikiami įgaliojimai laikinai apriboti duomenų valdytojo vykdomą jų asmens duomenų tvarkymą. Duomenų subjektai gali prašyti, kad duomenų valdytojas apribotų duomenų tvarkymą, kai:

- ginčijamas asmens duomenų tikslumas;
- duomenys tvarkomi neteisėtai ir duomenų subjektas prašo, užuot ištrynus duomenis, apriboti jų tvarkymą;
- duomenis būtina saugoti siekiant patenkinti arba apginti teisinius reikalavimus;
- turi būti priimtas sprendimas dėl duomenų valdytojo teisėtų interesų, kurie yra viršesni už duomenų subjekto interesus[578].

Būdai, kuriais duomenų valdytojas gali apriboti asmens duomenų tvarkymą, gali apimti, pavyzdžiui, laikiną atrinktų duomenų perkėlimą į kitą duomenų tvarkymo sistemą, dėl kurio duomenys tampa neprieinami naudotojams, arba laikinai pašalinti asmens duomenis[579]. Duomenų valdytojas, prieš panaikindamas duomenų tvarkymui taikomą apribojimą, privalo apie jį pranešti duomenų subjektui[580].

Prievolė pranešti apie asmens duomenų ištaisymą arba ištrynimą arba duomenų tvarkymo apribojimą

Duomenų valdytojas privalo informuoti kiekvieną gavėją, kuriam atskleidė asmens duomenis, apie asmens duomenų ištaisymą arba ištrynimą arba bet kokį duomenų

577 Bendrojo duomenų apsaugos reglamento 17 straipsnio dalis ir 66 konstatuojamoji dalis.

578 *Ten pat*, 18 straipsnio 1 punktas.

579 *Ten pat*, 67 konstatuojamoji dalis.

580 *Ten pat*, 18 straipsnio 3 punktas.

tvarkymo apribojimą, jei tai nėra neįmanoma ar neproporcinga[581]. Jeigu duomenų subjektas prašo pateikti informaciją apie gavėjus, duomenų valdytojas privalo jam pateikti šią informaciją[582].

6.1.5. Teisė į duomenų perkeliamumą

Pagal BDAR duomenų subjektams suteikiama teisė į duomenų perkeliamumą tais atvejais, kai asmens duomenys, kuriuos jie pateikė duomenų valdytojams, tvarkomi automatizuotomis priemonėmis, remiantis sutikimu, arba kai asmens duomenis tvarkyti būtina siekiant įvykdyti sutartį ir duomenys tvarkomi automatizuotomis priemonėmis. Tai reiškia, kad teisė į duomenų perkeliamumą netaikoma, kai asmens duomenų tvarkymas yra pagrįstas kitu teisiniu pagrindu nei sutikimas arba sutartis[583].

Jeigu teisė į duomenų perkeliamumą galioja, duomenų subjektai turi teisę, kad duomenų valdytojas jų asmens duomenis perduotų kitam duomenų valdytojui, jeigu tai techniškai įmanoma[584]. Siekdamas palengvinti šį procesą, duomenų valdytojas turėtų parengti sąveikius formatus, kurie padėtų užtikrinti duomenų perkeliamumą duomenų subjektų atžvilgiu[585]. BDAR nustatyta, kad šie formatai turėtų būti susisteminti, paprastai naudojami ir kompiuterio skaitomi, kad būtų palengvinta sąveika[586]. Plačiąja prasme sąveika gali būti apibūdinama kaip informacinės sistemos, kuriose galima keistis duomenimis ir dalytis informacija[587]. Nors naudojamų formatų paskirtis – užtikrinti sąveiką, BDAR nepateikta konkrečių rekomendacijų dėl konkretaus naudotino formato: įvairiuose sektoriuose gali būti naudojami skirtingi formatai[588].

29 straipsnio darbo grupės rekomendacijose nurodyta, kad teise į duomenų perkeliamumą „remiamas naudotojo pasirinkimas, naudotojo kontrolė ir naudotojo įgalinimas“, siekiant suteikti duomenų subjektams galimybes kontroliuoti savo asmens

581 *Ten pat*, 19 straipsnis.

582 *Ten pat*.

583 *Ten pat*, 68 konstatuojamoji dalis ir 20 straipsnio 1 dalis.

584 *Ten pat*, 20 straipsnio 2 punktas.

585 *Ten pat*, 68 konstatuojamoji dalis ir 20 straipsnio 1 dalis.

586 *Ten pat*, 68 konstatuojamoji dalis.

587 Europos Komisijos komunikatas dėl patikimesnių ir pažangesnių sienų ir saugumo informacinių sistemų, COM(2016) 205 *final*, 2016 m. balandžio 2 d.

588 29 straipsnio darbo grupė (2016 m.), *Rekomendacijos dėl teisės į duomenų perkeliamumą*, WP 242, 2016 m. gruodžio 13 d., peržiūrėta 2017 m. balandžio 5 d., p. 13.

duomenis[589]. Rekomendacijose paaiškinami pagrindiniai duomenų perkeliamumo aspektai, kurie apima:

- duomenų subjektų teisę gauti savo asmens duomenis, kuriuos tvarko duomenų valdytojas, struktūrizuotu, įprastai naudojamu, kompiuterio skaitomu ir sąveikiu formatu;
- teisę be kliūčių perduoti asmens duomenis iš vieno duomenų valdytojo kitam duomenų valdytojui, jei tai techniškai įmanoma;
- duomenų tvarkymo taisyklės – kai duomenų valdytojas atsako į duomenų perkeliamumo prašymą, jis veikia pagal duomenų subjekto nurodymus, o tai reiškia, kad jis neatsako už tai, kaip duomenų gavėjas laikosi duomenų apsaugos teisės aktų, nes duomenų subjektas nusprendžia, kam duomenys perkeliami;
- naudojimasis teise į duomenų perkeliamumą nedaro poveikio jokioms kitoms teisėms, kaip yra bet kokių kitų BDAR nustatytų teisių atveju.

6.1.6. Teisė nesutikti

Duomenų subjektai gali pasinaudoti savo teise nesutikti, kad būtų tvarkomi asmens duomenys, remdamiesi pagrindais, susijusiais su jų konkrečia padėtimi ir su duomenimis, kurie tvarkomi tiesioginės rinkodaros tikslais. Teisė nesutikti gali būti įgyvendinama automatizuotomis priemonėmis.

Teisė nesutikti dėl duomenų subjekto konkrečios padėties

Duomenų subjektai neturi bendros teisės nesutikti, kad jų duomenys būtų tvarkomi[590]. BDAR 21 straipsnio 1 dalyje duomenų subjektui suteikiama teisė pareikšti prieštaravimus, atsižvelgiant į jų konkrečią padėtį, kai duomenų tvarkymo teisinis pagrindas yra duomenų valdytojui pavestų užduočių, vykdomų viešojo intereso labui, atlikimas arba kai duomenų tvarkymas grindžiamas duomenų valdytojo

589 *Ten pat*.

590 Taip pat žr. EŽTT, *M. S. prieš Švediją*, Nr. 20837/92, 1997 m. rugpjūčio 27 d. (byloje medicininiai duomenys buvo perduoti be sutikimo arba galimybės nesutikti); EŽTT, *Leander prieš Švediją*, Nr. 9248/81, 1987 m. kovo 26 d.; EŽTT, *Mosley prieš Jungtinę Karalystę*, Nr. 48009/08, 2011 m. gegužės 10 d.

teisėtais interesais[591]. Teisė nesutikti taikoma profiliavimo veiklai. Panaši teisė pripažįstama atnaujintoje 108-ojoje konvencijoje[592].

Teise nesutikti, remiantis su duomenų subjekto konkrečia padėtimi susijusiais pagrindais, siekiama nustatyti tinkamą duomenų subjekto duomenų apsaugos teisių ir kitų asmenų teisėtų teisių, susijusių su jų duomenų tvarkymu, pusiausvyrą. Tačiau ESTT paaiškino, kad duomenų subjekto teisės paprastai yra viršesnės už duomenų valdytojo ekonominius interesus, priklausomai nuo „atitinkamos informacijos pobūdžio ir jos ypatingumo duomenų subjekto privačiam gyvenimui, taip pat nuo visuomenės intereso gauti prieigą prie šios informacijos“[593]. Pagal BDAR prievolė įrodyti tenka duomenų valdytojams, kurie privalo įrodyti įtikinamas priežastis toliau tvarkyti duomenis[594]. Panašiai, atnaujintos 108-osios konvencijos aiškinamojoje ataskaitoje paaiškinama, kad teisėtus duomenų tvarkymo pagrindus (kurie gali būti viršesni už duomenų subjektų teisę nesutikti) reikia įrodyti kiekvienu konkrečiu atveju[595].

Pavyzdys. Byloje *Manni*[596] ESTT nusprendė, kad dėl teisėto asmens duomenų atskleidimo bendrovių registre tikslo, visų pirma dėl būtinybės apsaugoti trečiųjų asmenų interesus ir užtikrinti teisinį tikrumą, iš esmės S. Manni neturėjo teisės reikalauti, kad jo asmens duomenys bendrovių registre būtų ištrinti. Tačiau ESTT pripažino, kad teisė nesutikti su duomenų tvarkymu galiojo, ir konstatavo, kad „vis dėlto negalima atmesti galimybės, kad gali susiklostyti konkrečios situacijos, kai remiantis privalomais ir teisėtais pagrindais, susijusiais su konkrečia duomenų subjekto padėtimi, galimybė susipažinti su įmonių registre esančiais su tuo asmeniu susijusiais asmens duomenimis pasibaigus pakankamai ilgam laikotarpiui <...> bus apribota taip, kad susipažinti su šiais duomenimis bus leista tik tretiesiems asmenims, įrodžiusiems, kad turi konkretų interesą tai padaryti“.

591 Bendrojo duomenų apsaugos reglamento 69 konstatuojamoji dalis, 6 straipsnio 1 dalies e ir f punktai.

592 Atnaujintos 108-osios konvencijos 9 straipsnio 1 dalies d punktas; Rekomendacijos dėl profiliavimo 5 straipsnio 3 dalis.

593 ESTT, C-131/12, *Google Spain SL, Google Inc. prieš Agencia Española de Protección de Datos (AEPD), Mario Costeja González* (DK), 2014 m. gegužės 13 d., 81 punktas.

594 Taip pat žr. atnaujintos 108-osios konvencijos 98 straipsnio 1 dalies d punktą, kuriame teigiama, kad duomenų subjektas gali nesutikti, kad jo duomenys būtų tvarkomi, „išskyrus atvejus, kai duomenų valdytojas įrodo, kad jo duomenys tvarkomi dėl teisėtų priežasčių, kurios yra viršesnės už jo interesus arba teises ir pagrindines laisves“.

595 Atnaujintos 108-osios konvencijos aiškinamosios ataskaitos 78 punktas.

596 ESTT, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce prieš Salvatore Manni*, 2017 m. kovo 9 d., 47 ir 60 punktai.

ESTT laikėsi nuomonės, kad nacionaliniai teismai kiekvieną atvejį privalo įvertinti atsižvelgdami į visas svarbias asmens aplinkybes ir į tai, ar yra teisėtų ir svarbių priežasčių, kuriomis būtų galima išimties tvarka pateisinti ribotą trečiųjų šalių prieigą prie bendrovių registruose saugomų asmens duomenų. Tačiau ESTT paaiškino, kad S. Manni byloje vien faktas, kad jo asmens duomenų, esančių registre, atskleidimas tariamai turėjo poveikį jo klientūrai, negalėjo būti laikomas tokiu teisėtu ir privalomu pagrindu. Potencialūs S. Manni klientai turi teisėtą interesą susipažinti su informacija, susijusia su jo ankstesnės įmonės bankrotu.

Sėkmingas nesutikimas reiškia, kad duomenų valdytojas nebegali tvarkyti atitinkamų duomenų. Tačiau iki duomenų subjekto nesutikimo atliktos duomenų tvarkymo operacijos išlieka teisėtos.

Teisė nesutikti, kad duomenys būtų tvarkomi tiesioginės rinkodaros tikslais

BDAR 21 straipsnio 2 dalyje nustatyta konkreti teisė nesutikti su asmens duomenų naudojimu tiesioginės rinkodaros tikslais, taip patikslinant E. privatumo direktyvos 13 straipsnį. Tokia teisė taip pat nustatyta atnaujintoje 108-ojoje konvencijoje ir ET Rekomendacijoje dėl tiesioginės rinkodaros[597]. Atnaujintos 108-osios konvencijos aiškinamojoje ataskaitoje paaiškinama, kad nesutikus su duomenų tvarkymu tiesioginės rinkodaros tikslais, atitinkami asmens duomenys turėtų būti besąlygiškai ištrinami arba pašalinami[598].

Duomenų subjektas turi teisę bet kuriuo metu ir nemokamai nesutikti, kad jo asmens duomenys būtų naudojami tiesioginės rinkodaros tikslais. Duomenų subjektai turi būti aiškiai informuoti apie šią teisę atskirai nuo bet kokios kitos informacijos.

Teisė nesutikti automatizuotomis priemonėmis

Jeigu asmens duomenys naudojami ir tvarkomi teikiant informacinės visuomenės paslaugas, duomenų subjektas gali įgyvendinti savo teisę nesutikti su jo asmens duomenų tvarkymu naudodamasis automatizuotomis priemonėmis.

597 Europos Taryba, Ministrų Komitetas (1985 m.), Rekomendacijos *Rec(85)20* valstybėms narėms dėl asmens duomenų, naudojamų tiesioginės rinkodaros tikslais, apsaugos, 1985 m. spalio 25 d., 4 straipsnio 1 dalis.

598 Atnaujintos 108-osios konvencijos aiškinamosios ataskaitos 79 punktas.

Informacinės visuomenės paslaugos apibrėžiamos taip: bet kuri informacinės visuomenės paslauga, t. y. paprastai už atlyginimą per atstumą, elektroninėmis priemonėmis ir asmeniškų paslaugų gavėjo prašymu teikiama paslauga[599].

Informacinės visuomenės paslaugas siūlantys duomenų valdytojai turi būti nustatę tinkamas technines priemones ir procedūras, kad būtų galima veiksmingai pasinaudoti teise nesutikti su automatizuotomis priemonėmis[600]. Pavyzdžiui, tai gali būti slapukų blokavimas tinklalapiuose arba naršymo internete sekimo išjungimas.

Teisė nesutikti, kad duomenys būtų tvarkomi mokslinių ar istorinių tyrimų arba statistiniais tikslais

Pagal ES teisę moksliniai tyrimai turėtų būti aiškinami plačiai, įskaitant, pavyzdžiui, technologijų plėtrą ir demonstravimą, fundamentinius tyrimus, taikomuosius mokslinius tyrimus ir privačiomis lėšomis finansuojamus mokslinius tyrimus[601]. Istoriniai tyrimai taip pat apima genealoginius tyrimus, atsižvelgiant į tai, kad reglamentas neturėtų būti taikomas mirusiems asmenims[602]. Statistiniai tikslai reiškia bet kokią asmens duomenų, būtinų atliekant statistinius tyrimus arba rengiant statistinius rezultatus, rinkimo ir tvarkymo operaciją[603]. Vėlgi, ypatinga duomenų subjekto padėtis yra teisinis pagrindas, susijęs su teise nesutikti, kad asmens duomenys būtų tvarkomi mokslinių tyrimų tikslais[604]. Vienintelė išimtis taikoma tuo atveju, kai duomenis tvarkyti būtina siekiant atlikti užduotį, vykdomą dėl viešojo intereso priežasčių. Tačiau teisė reikalauti ištrinti duomenis netaikoma, kai duomenis tvarkyti būtina (remiantis viešojo intereso priežastimis arba jų nesant) mokslinių ar istorinių tyrimų tikslais arba statistiniais tikslais[605].

BDAR mokslinių, statistinių ar istorinių tyrimų reikalavimai ir duomenų subjektų teisės derinami su 89 straipsnyje nustatytomis konkrečiomis apsaugos priemonėmis ir nukrypti leidžiančiomis nuostatomis. Taigi, Sąjungos arba valstybės narės teisėje gali būti numatytos teisės nesutikti išimtys, jei dėl tokios teisės gali tapti neįmanoma

599 Direktyvos 98/34/EB su pakeitimais, padarytais Direktyva 98/48/EB, nustatančia informacijos apie techninius standartus ir reglamentus teikimo tvarką, 1 straipsnio 2 punktas.

600 Bendrojo duomenų apsaugos reglamento 21 straipsnio 5 dalis.

601 *Ten pat*, 159 konstatuojamoji dalis.

602 *Ten pat*, 160 konstatuojamoji dalis.

603 *Ten pat*, 162 konstatuojamoji dalis.

604 *Ten pat*, 21 straipsnio 6 dalis.

605 *Ten pat*, 17 straipsnio 3 dalies d punktas.

pasiekti mokslinių tyrimų tikslų arba ji gali labai sutrukdyti siekti tų tikslų, ir jei tokios nukrypti leidžiančios nuostatos yra būtinos tiems tikslams pasiekti.

ET teisėje, t. y. atnaujintos 108-osios konvencijos 9 straipsnio 2 dalyje, nustatyta, kad duomenų subjektų teisių, įskaitant teisę nesutikti, apribojimai gali būti numatyti teisės aktuose, susijusiuose su duomenų tvarkymu archyvavimo tikslais viešojo intereso labui, mokslinių ar istorinių tyrimų tikslais arba statistiniais tikslais, kai nėra akivaizdžios rizikos, kad bus pažeistos duomenų subjektų teisės ir pagrindinės laisvės.

Tačiau aiškinamojoje ataskaitoje (41 punktas) taip pat pripažįstama, kad duomenų subjektai turėtų turėti galimybę duoti sutikimą tik dėl tam tikrų mokslinių tyrimų sričių arba mokslinių tyrimų projektų dalių tiek, kiek tai leidžia numatytas tikslas, ir prieštarauti, jei mano, kad duomenų tvarkymas be teisėto pagrindo pernelyg pažeidžia jų teises ir laisves.

Kitaip tariant, toks duomenų tvarkymas būtų laikomas *a priori* suderinamu su vidaus rinka, jeigu yra nustatytos kitos apsaugos priemonės ir jeigu operacijos iš esmės padeda užkirsti kelią bet kokiam gautos informacijos naudojimui priimant sprendimus ar taikant priemones, susijusias su konkrečiu asmeniu.

6.1.7. Automatizuotas individualių sprendimų priėmimas, įskaitant profiliavimą

Automatizuoti sprendimai – tai sprendimai, priimami naudojant asmens duomenis, kurie tvarkomi tik automatizuotomis priemonėmis, visiškai nedalyvaujant žmonėms. **Pagal ES teisę** duomenų subjektams neturi būti taikomi automatizuotai priimami sprendimai, kurie sukelia teisines pasekmes arba turi kitokį panašų svarbų poveikį. Jei tikėtina, kad tokie sprendimai turės didelį poveikį asmenų gyvenimui, nes jie susiję, pavyzdžiui, su kreditingumu, e. įdarbinimu, darbo rezultatais arba elgesio ar patikimumo analize, būtina speciali apsauga, kad būtų išvengta neigiamų pasekmių. Automatizuotas sprendimų priėmimas apima profiliavimą, kurį vykdant automatiškai vertinami „su fiziniu asmeniu susiję asmeniniai aspektai, visų pirma siekiant analizuoti arba numatyti aspektus, susijusius su duomenų subjekto darbo rezultatais, ekonomine padėtimi, sveikatos būkle, asmeniniais pomėgiais ar interesais, patikimumu arba elgesiu, vieta arba judėjimu“[606].

606 *Ten pat*, 71 konstatuojamoji dalis, 4 straipsnio 4 punktas ir 22 straipsnis.

Pavyzdys. Siekdamos greitai įvertinti būsimo kliento kreditingumą, kredito reitingų agentūros (KRA) renka tam tikrus duomenis, pavyzdžiui, apie tai, kaip klientas tvarkė savo kredito ir paslaugų ir (arba) komunalinių paslaugų sąskaitas, išsamius duomenis apie ankstesnius kliento adresus, taip pat informaciją iš viešųjų šaltinių, pavyzdžiui, rinkėjų sąrašus, viešus įrašus (įskaitant teismo sprendimus) arba bankroto ir nemokumo duomenis. Vėliau šie asmens duomenys įtraukiami į vertinimo balais algoritmą, pagal kurį apskaičiuojama bendra vertė, atitinkanti potencialaus kliento kreditingumą.

29 straipsnio darbo grupės nuomone, teisė į tai, kad nebūtų taikomi vien automatizuotu duomenų tvarkymu grindžiami sprendimai, kurie gali turėti teisinių pasekmių duomenų subjektui arba turėti jam didelį poveikį, prilygsta bendram draudimui ir nereikalaujama, kad duomenų subjektas aktyviai siektų prieštarauti tokiam sprendimui[607].

Vis dėlto pagal BDAR automatizuotas sprendimų priėmimas, kuris daro teisinį poveikį arba didelį poveikį asmenims, gali būti priimtinas, jei tai būtina sudarant sutartį arba vykdant sutartį tarp duomenų valdytojo ir duomenų subjekto arba jei duomenų subjektas davė aiškų sutikimą. Be to, automatizuotas sprendimų priėmimas yra priimtinas, jeigu jis leidžiamas pagal įstatymą ir jeigu užtikrinama tinkama duomenų subjekto teisių, laisvių ir teisėtų interesų apsauga[608].

BDAR taip pat nustatyta, kad duomenų valdytojas, be prievolių, susijusių su informacijos teikimu tais atvejais, kai renkami asmens duomenys, taip pat privalo informuoti duomenų subjektus apie automatizuotų sprendimų priėmimą, įskaitant profiliavimą[609]. Tai neturi jokio poveikio teisei susipažinti su duomenų valdytojo tvarkomais asmens duomenimis[610]. Informuojant reikia ne tik nurodyti, kad bus atliekamas profiliavimas, taip pat reikėtų pateikti prasmingą informaciją apie profiliavimo logiką ir numatomas duomenų tvarkymo pasekmes asmenims[611]. Pavyzdžiui, sveikatos draudimo bendrovė, taikanti automatizuotą sprendimų dėl taikomųjų programų priėmimą, turėtų pateikti duomenų subjektams bendro pobūdžio informaciją apie tai, kaip veikia algoritmas, ir apie tai, į kurį algoritmą atsižvelgiama apskaičiuojant

607 29 straipsnio darbo grupė, *Gairės dėl pranešimo apie asmens duomenų saugumo pažeidimą pagal Reglamentą (ES) 2016/679*, WP 251, 2017 m. spalio 3 d., p. 15.

608 Bendrojo duomenų apsaugos reglamento 22 straipsnio 2 dalis.

609 *Ten pat*, 12 straipsnis.

610 *Ten pat*, 15 straipsnis.

611 *Ten pat*, 13 straipsnio 2 dalies f punktas.

jų draudimo įmokas. Panašiai, naudodamiesi savo teise susipažinti su duomenimis, duomenų subjektai gali prašyti duomenų valdytojo suteikti informacijos apie tai, ar sprendimai priimami automatiškai, ir prasmingos informacijos apie loginį pagrindą[612].

Duomenų subjektams pateikiama informacija siekiama užtikrinti skaidrumą ir sudaryti sąlygas duomenų subjektams duoti informuoto asmens sutikimą, jei taip yra, arba reikalauti, kad įsikištų žmogus. Duomenų valdytojas privalo įgyvendinti tinkamas priemones, kad apsaugotų duomenų subjekto teises, laisves ir teisėtus interesus. Tai apima bent teisę duomenų valdytojo reikalauti žmogaus įsikišimo ir duomenų subjekto galimybę pareikšti savo požiūrį ir užginčyti sprendimą, kuris pagrįstas jo asmens duomenų tvarkymu[613].

29 straipsnio darbo grupė pateikė papildomų rekomendacijų dėl automatizuoto sprendimų priėmimo pagal BDAR[614].

Pagal ET teisę asmenys turi teisę, kad jiems nebūtų taikomas sprendimas, kuris turės jiems didelį poveikį ir kuris grindžiamas tik automatizuotu duomenų tvarkymu, neatsižvelgiant į jų nuomonę[615]. Reikalavimas atsižvelgti į duomenų subjekto nuomonę tais atvejais, kai sprendimai yra pagrįsti tik automatizuotu duomenų tvarkymu, reiškia, kad jie turi teisę ginčyti tokius sprendimus, be to, jie turėtų turėti galimybę ginčyti visus netikslius duomenų valdytojo naudojamus asmens duomenis ir ginčyti, ar jiems taikomas koks nors profilis yra tinkamas[616]. Tačiau asmuo negali pasinaudoti šia teise, jei automatizuotą sprendimą leidžiama priimti pagal duomenų valdytojui taikomą įstatymą, kuriame taip pat nustatytos tinkamos priemonės duomenų subjekto teisėms, laisvėms ir teisėtiems interesams apsaugoti. Be to, duomenų subjektai, pateikę prašymą, turi teisę sužinoti priežastis, kuriomis grindžiamas atliktas duomenų tvarkymas[617]. Atnaujintos 108-osios konvencijos aiškinamojoje ataskaitoje pateikiamas kreditų vertinimo balais pavyzdys. Asmenims reikėtų suteikti teisę ne tik žinoti apie patį teigiamą arba neigiamą sprendimą dėl vertinimo balais, bet ir jų asmens duomenų tvarkymo, kuriuo remiantis buvo priimtas toks sprendimas, *loginį* pagrindą. „Šių elementų supratimas padeda veiksmingai naudotis kitomis

612 *Ten pat*, 15 straipsnio 1 dalies h punktas.

613 *Ten pat*, 22 straipsnio 3 punktas.

614 29 straipsnio darbo grupė (2017 m.), *Automatizuoto individualaus sprendimų priėmimo ir profiliavimo taikant Reglamentą 2016/679 rekomendacijos*, WP 251, 2017 m. spalio 3 d.

615 Atnaujintos 108-osios konvencijos 9 straipsnio 1 dalies a punktas.

616 Atnaujintos 108-osios konvencijos aiškinamosios ataskaitos 75 punktas.

617 Atnaujintos 108-osios konvencijos 9 straipsnio 1 dalies c punktas.

esminėmis apsaugos priemonėmis, pavyzdžiui, teise prieštarauti ir teise pateikti skundą kompetentingai institucijai“[618].

Rekomendacijoje dėl profiliavimo, nors ji nėra teisiškai privaloma, nurodytos asmens duomenų rinkimo ir tvarkymo vykdant profiliavimo veiklą sąlygos[619]. Į ją įtrauktos nuostatos dėl poreikio užtikrinti, kad duomenų tvarkymas vykdant profiliavimo veiklą būtų sąžiningas, teisėtas, proporcingas ir derėtų su nustatytais ir teisėtais tikslais. Joje taip pat yra nuostatų dėl informacijos, kurią duomenų valdytojai turėtų pateikti duomenų subjektams. Rekomendacijoje taip pat įtvirtintas duomenų kokybės principas, pagal kurį reikalaujama, kad duomenų valdytojai imtųsi priemonių duomenų netikslumą lemiantiems veiksniams pašalinti, riboti riziką arba dėl profiliavimo atsirandančias klaidas ir periodiškai vertinti duomenų bei naudojamų algoritmų kokybę.

6.2. Teisių gynimo priemonės, atsakomybė, sankcijos ir kompensacija

Pagrindiniai faktai

- Pagal atnaujintą 108-ąją konvenciją susitariančiųjų šalių nacionalinėje teisėje turi būti nustatytos tinkamos teisių gynimo priemonės ir sankcijos, susijusios su teisės į duomenų apsaugą pažeidimais.
- ES lygmeniu BDAR nustatytos duomenų subjektų teisių gynimo priemonės, kuriomis jie gali pasinaudoti pažeidus jų teises, taip pat sankcijos, skiriamos duomenų valdytojams ir duomenų tvarkytojams, kurie nesilaiko reglamento nuostatų. Jame taip pat nustatyta teisė į kompensaciją ir atsakomybė.
    - Duomenų subjektai turi teisę priežiūros institucijai pateikti skundą dėl tariamų reglamento pažeidimų, taip pat teisę į veiksmingą teisminę gynybą ir teisę gauti kompensaciją.
    - Asmenims, įgyvendinantiems savo teisę į veiksmingą teisių gynimą, gali atstovauti duomenų apsaugos srityje veikiančios ne pelno organizacijos.
    - Duomenų valdytojas arba duomenų tvarkytojas atsako už bet kokią dėl pažeidimo padarytą materialinę arba nematerialinę žalą.

618 Atnaujintos 108-osios konvencijos aiškinamosios ataskaitos 77 punktas.

619 Europos Taryba, Rekomendacija *CM/Rec(2010)13* valstybėms narėms dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu profiliavimo kontekste, 5 straipsnio 5 dalis.

- Priežiūros institucijos turi įgaliojimus už reglamento pažeidimus skirti administracines baudas iki 20 000 000 EUR arba, įmonės atveju, – iki 4 % jos bendros metinės pasaulinės apyvartos, atsižvelgiant į tai, kuri suma yra didesnė.

- Duomenų subjektai duomenų apsaugos teisės pažeidimų klausimus gali perduoti spręsti EŽTT ir tai yra tam tikromis sąlygomis taikoma paskutinės išeities priemonė.

- Bet kuris fizinis arba juridinis asmuo turi teisę bet kurį Europos duomenų apsaugos valdybos sprendimą apskųsti ESTT sutartyse nustatytomis sąlygomis.

Siekiant užtikrinti asmens duomenų apsaugą Europoje, nepakanka patvirtinti teisines priemones. Kad Europos duomenų apsaugos taisyklės būtų veiksmingos, būtina nustatyti mechanizmus, kurie sudarytų sąlygas asmenims kovoti su jų teisių pažeidimais ir reikalauti kompensuoti bet kokią patirtą žalą. Taip pat svarbu, kad priežiūros institucijos turėtų įgaliojimus už atitinkamą pažeidimą skirti veiksmingas, atgrasomąsias ir proporcingas sankcijas.

Duomenų apsaugos teisėje nustatytas teises gali įgyvendinti asmuo, kurio teisėms kyla pavojus; šiuo atveju kalbama apie duomenų subjektą. Tačiau kiti asmenys, kurie atitinka būtinuosius reikalavimus pagal nacionalinę teisę, taip pat gali atstovauti duomenų subjektams tais atvejais, kai jie įgyvendina savo teises. Pagal įvairius nacionalinės teisės aktus vaikams ir protinę negalią turintiems asmenims turi atstovauti jų globėjai[620]. Pagal ES duomenų apsaugos teisę asociacija, kurios teisėtas tikslas yra skatinti duomenų apsaugos teises, gali atstovauti duomenų subjektams bet kurioje priežiūros institucijoje arba teisme[621].

6.2.1. Teisė pateikti skundą priežiūros institucijai

Pagal **ET teisę** ir **ES teisę** asmenys turi teisę pateikti prašymus ir skundus kompetentingai priežiūros institucijai, jei mano, kad jų asmens duomenys tvarkomi nesilaikant teisės aktų.

Atnaujintoje 108-ojoje konvencijoje pripažįstama duomenų subjektų teisė pasinaudoti priežiūros institucijos pagalba įgyvendinant savo teises pagal Konvenciją,

620 FRA (2015 m.), Vaiko teises reglamentuojančios Europos teisės vadovas, Liuksemburgas, Leidinių biuras; FRA (2013 m.), *Legal capacity of persons with intellectual disabilities and persons with mental health problems* (liet. „Protinę negalią turinčių asmenų ir psichikos sveikatos problemų turinčių asmenų teisinis veiksnumas“), Liuksemburgas, Leidinių biuras.

621 Bendrojo duomenų apsaugos reglamento 80 straipsnis.

nepaisant jų pilietybės arba gyvenamosios vietos[622]. Pagalbos prašymas gali būti atmestas tik išimtinėmis aplinkybėmis, o duomenų subjektai neturėtų padengti su pagalba susijusių išlaidų ir mokesčių[623].

Panašių nuostatų galima rasti ir ES teisės sistemoje. Pagal BDAR reikalaujama, kad priežiūros institucijos patvirtintų priemones, palengvinančias skundų pateikimą, pavyzdžiui, sukurtų elektroninę skundo pateikimo formą[624]. Duomenų subjektas gali pateikti skundą savo įprastinės gyvenamosios vietos, darbo vietos arba tariamo pažeidimo vietos valstybės narės priežiūros institucijai[625]. Skundus būtina ištirti, o priežiūros institucija privalo informuoti atitinkamą asmenį apie reikalavimo nagrinėjimo procedūros rezultatą[626].

Apie galimus ES institucijų ar įstaigų pažeidimus galima informuoti Europos duomenų apsaugos priežiūros pareigūną[627]. Jei EDAPP per šešis mėnesius nepateikia atsakymo, skundas laikomas atmestu. EDAPP sprendimus galima apskųsti ESTT pagal Reglamentą (EB) Nr. 45/2001, kuriuo ES institucijos ir įstaigos įpareigojamos laikytis duomenų apsaugos taisyklių.

Būtina suteikti galimybę apskųsti teismams nacionalinės priežiūros institucijos sprendimus. Tai taikoma duomenų subjektui ir duomenų valdytojams ir duomenų tvarkytojams, kurie buvo priežiūros institucijoje vykstančios procedūros šalys.

Pavyzdys. 2017 m. rugsėjo mėn. Ispanijos duomenų apsaugos institucija bendrovei *Facebook* skyrė baudą už kelių duomenų apsaugos taisyklių pažeidimą. Priežiūros institucija pasmerkė socialinį tinklą, kuris renka, saugo ir tvarko asmens duomenis, įskaitant specialių kategorijų asmens duomenis, reklamos tikslais be duomenų subjekto sutikimo. Sprendimas buvo pagrįstas tyrimu, kurį priežiūros institucija atliko savo iniciatyva.

622 Atnaujintos 108-osios konvencijos 18 straipsnis.

623 *Ten pat*, 16–17 straipsniai.

624 Bendrojo duomenų apsaugos reglamento 57 straipsnio 2 dalis.

625 *Ten pat*, 77 straipsnio 1 punktas.

626 *Ten pat*, 77 straipsnio 2 punktas.

627 2000 m. gruodžio 18 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 45/2001 dėl asmenų apsaugos Bendrijos institucijoms ir įstaigoms tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo, OL L 8, 2001.

6.2.2. Teisė į veiksmingą teisminę teisių gynimo priemonę

Asmenys turi turėti ne tik teisę pateikti skundą priežiūros institucijai, bet ir teisę į veiksmingą teisminę teisių gynimo priemonę ir teisę kreiptis į teismą. Teisė į teisių gynimo priemonę yra įtvirtinta Europos teisės tradicijoje ir pripažįstama kaip pagrindinė teisė tiek pagal ES pagrindinių teisių chartijos 47 straipsnį, tiek pagal EŽTK 13 straipsnį[628].

Pagal ES teisę tai, kaip svarbu duomenų subjektams suteikti veiksmingas teisių gynimo priemones tuo atveju, kai pažeidžiamos jų teisės, aiškiai matyti tiek iš BDAR nuostatų, kuriomis nustatoma teisė į veiksmingą teisminę teisių gynimo priemonę prieš priežiūros institucijas, duomenų valdytojus ir duomenų tvarkytojus, tiek iš ESTT jurisprudencijos.

Pavyzdys. Byloje *Schrems*[629] ESTT paskelbė, kad „saugaus uosto“ tinkamumo sprendimas negalioja. Tuo sprendimu buvo leista tarptautinius duomenis iš ES perduoti JAV organizacijoms, kurios yra pasitvirtinusios pagal „saugaus uosto“ schemą. ESTT manė, kad „saugaus uosto“ sistema turėjo keletą trūkumų, kuriais buvo pažeidžiamos ES piliečių pagrindinės teisės į privatumo apsaugą, asmens duomenų apsaugą ir teisė į veiksmingą teisių gynybą teisinėmis priemonėmis.

Dėl teisių į privatumą ir duomenų apsaugą pažeidimo ESTT pabrėžė, kad pagal JAV teisės aktus tam tikroms valdžios institucijoms leidžiama susipažinti su asmens duomenimis, perduotais iš valstybių narių į JAV, ir juos tvarkyti tokiu būdu, kuris būtų nesuderinamas su pirminiais perdavimo tikslais ir viršytų tai, kas tikrai būtina ir proporcinga nacionalinio saugumo apsaugai. Dėl teisės į veiksmingą teisinę gynybą jis pažymėjo, kad duomenų subjektai neturi jokių administracinių ar teisminių teisių gynimo priemonių, kad galėtų susipažinti su savo duomenimis, juos ištaisyti ar ištrinti, priklausomai nuo konkretaus atvejo. ESTT padarė išvadą, kad teisės aktais, kuriuose nenumatyta galimybė pasinaudoti teisių gynimo priemonėmis siekiant susipažinti su savo asmens duomenimis, juos ištaisyti ar ištrinti, „negerbiama pagrindinės teisės

628 Žr., pvz., EŽTT, *Karabeyoğlu prieš Turkiją*, Nr. 30083/10, 2016 m. birželio 7 d.; EŽTT, *Mustafa Sezgin Tanrıkulu prieš Turkiją*, Nr. 27473/06, 2017 m. liepos 18 d.

629 ESTT, C-362/14, *Maximillian Schrems prieš Data Protection Commissioner* (DK), 2015 m. spalio 6 d.

į veiksmingą teisminę apsaugą, įtvirtintos Chartijos 47 straipsnyje, esmė“. Jis pažymėjo, kad teisminės teisių gynimo priemonės, užtikrinančios teisės normų laikymąsi, buvimas yra neatsiejamas nuo teisinės valstybės principo.

Asmenys, duomenų valdytojai arba duomenų tvarkytojai, kurie siekia ginčyti priežiūros institucijos teisiškai privalomą sprendimą, gali iškelti bylą teisme[630]. Sąvoka „sprendimas“ turėtų būti aiškinama plačiai ir apimti priežiūros institucijų naudojimąsi tyrimo, sankcijų taikymo ir leidimų suteikimo įgaliojimais, taip pat sprendimus atmesti skundą arba jo nepriimti. Tačiau teisiškai neprivalomos priemonės, pavyzdžiui, priežiūros institucijos pateiktos nuomonės ar patarimai, negali būti ieškinio teisme dalykas[631]. Ieškinys turi būti pareiškiamas valstybės narės, kurioje yra įsisteigusi atitinkama priežiūros institucija, teismuose[632].

Tais atvejais, kai duomenų valdytojas arba duomenų tvarkytojas pažeidžia duomenų subjekto teises, duomenų subjektai turi teisę pateikti skundą teismui[633]. Kai procesas pradedamas prieš duomenų valdytoją arba duomenų tvarkytoją, ypač svarbu, kad asmenims būtų suteikta galimybė pasirinkti, kur pareikšti ieškinį. Jie gali nuspręsti tai padaryti arba valstybėje narėje, kurioje yra duomenų valdytojo arba duomenų tvarkytojo buveinė, arba valstybėje narėje, kurioje yra atitinkamų duomenų subjektų įprastinė gyvenamoji vieta[634]. Antroji galimybė labai palengvina asmenų naudojimąsi savo teisėmis, nes suteikia jiems galimybę pareikšti ieškinius valstybėje, kurioje jie gyvena, ir žinomoje jurisdikcijoje. Bylos nagrinėjimo prieš duomenų valdytojus ir duomenų tvarkytojus vietos apribojimas iki valstybės narės, kurioje duomenų tvarkytojai yra įsisteigę, galėtų atgrasyti duomenų subjektus, gyvenančius kitose valstybėse narėse, pareikšti ieškinį teisme, nes tai reikštų keliavimą ir papildomas išlaidas, o byla galėtų būti nagrinėjama kita kalba užsienio jurisdikcijoje. Vienintelė išimtis yra susijusi su atvejais, kai duomenų valdytojas arba duomenų tvarkytojas yra valdžios institucijos ir duomenys tvarkomi naudojantis jų viešaisiais įgaliojimais. Šiuo atveju tik valstybės, kurioje yra atitinkama valdžios institucija, teismai yra kompetentingi nagrinėti ieškinį[635].

630 Bendrojo duomenų apsaugos reglamento 78 straipsnis.

631 *Ten pat*, 143 konstatuojamoji dalis.

632 *Ten pat*, 78 straipsnio 3 punktas.

633 *Ten pat*, 79 straipsnis.

634 *Ten pat*, 79 straipsnio 2 punktas.

635 *Ten pat*.

Nors daugeliu atvejų su duomenų apsaugos taisyklėmis susijusios bylos bus nagrinėjamos valstybių narių teismuose, kai kurios bylos gali būti perduotos ESTT. Pirmoji galimybė – kai duomenų subjektas, duomenų valdytojas, duomenų tvarkytojas arba priežiūros institucija prašo panaikinti EDAV sprendimą. Tačiau ieškiniui taikomos SESV 263 straipsnyje nustatytos sąlygos, o tai reiškia, jog tam, kad jis būtų priimtas nagrinėti, šie asmenys ir subjektai privalo įrodyti, kad Valdybos sprendimas yra tiesiogiai ir konkrečiai su jais susijęs.

Antrasis scenarijus yra susijęs su atvejais, kai ES institucijos ar įstaigos neteisėtai tvarko asmens duomenis. Jeigu ES institucijos pažeidžia duomenų apsaugos teisę, duomenų subjektai gali pareikšti ieškinį tiesiogiai ES Bendrajame Teisme (Bendrasis Teismas priklauso ESTT). Bendrasis Teismas pirmiausia nagrinėja skundus dėl Sąjungos institucijų padarytų Sąjungos teisės pažeidimų. Tai reiškia, kad skundai dėl EDAPP, kaip ES institucijos, taip pat gali būti teikiami Bendrajam Teismui[636].

Pavyzdys. Byloje *Bavarian Lager*[637] bendrovė paprašė Europos Komisijos leisti susipažinti su visu Komisijos surengto susitikimo, tariamai susijusio su bendrovei svarbiais teisiniais klausimais, protokolu. Komisija atmetė bendrovės prašymą leisti susipažinti su informacija, remdamasi viršesniais duomenų apsaugos interesais[638]. *Bavarian Lager* pagal ES institucijų duomenų apsaugos reglamento 32 straipsnį tą sprendimą apskundė pirmosios instancijos teismui (anksčiau – Bendrasis Teismas). Savo sprendime (byla T194/04, *The Bavarian Lager Co. Ltd prieš Europos Bendrijų Komisiją*) pirmosios instancijos teismas panaikino Komisijos sprendimą atmesti prašymą leisti susipažinti su informacija. Europos Komisija apskundė šį sprendimą ESTT.

ESTT priėmė sprendimą (didžiojoje kolegijoje), kuriuo panaikino pirmosios instancijos teismo sprendimą ir patvirtino, kad Europos Komisija atmetė prašymą leisti susipažinti su visu posėdžio protokolu, kad būtų apsaugoti posėdyje dalyvavusių asmenų asmens duomenys. ESTT laikėsi nuomonės, kad Komisija teisingai atsisakė atskleisti šią informaciją, nes dalyviai nedavė sutikimo atskleisti jų asmens duomenis. Be to, *Bavarian Lager* neįrodė būtinybės susipažinti su šia informacija.

636 Reglamento (EB) Nr. 45/2001 32 straipsnio 3 dalis.

637 ESTT, C-28/08 P, *Europos Komisija prieš The Bavarian Lager Co. Ltd* (DK), 2010 m.

638 Dėl argumentų analizės žr. EDAPP (2011 m.), *Galimybė visuomenei susipažinti su dokumentais priėmus sprendimą Bavarian Lager byloje*, Briuselis, EDAPP.

Galiausiai, duomenų subjektai, priežiūros institucijos, duomenų valdytojai arba duomenų tvarkytojai nacionalinėse bylose gali prašyti nacionalinio teismo pateikti ESTT paaiškinimus dėl ES institucijų, įstaigų, tarnybų ar agentūrų aktų aiškinimo ir galiojimo. Tokie išaiškinimai pateikiami prejudiciniuose sprendimuose. Tai nėra tiesioginė pareiškėjo teisės gynimo priemonė, tačiau ji sudaro sąlygas nacionaliniams teismams užtikrinti, kad ES teisė būtų aiškinama teisingai. Būtent per šį prejudicinių sprendimų mechanizmą ESTT buvo perduotos nagrinėti tokios svarbios bylos kaip *Digital Rights Ireland*, *Kärntner Landesregierung ir kt.*[639] ir *Schrems*[640], kurios turėjo didelės įtakos ES duomenų apsaugos teisės plėtotei.

Pavyzdys. *Digital Rights Ireland* ir *Kärntner Landesregierung ir kt.*[641] buvo Airijos Aukščiausiojo Teismo ir Austrijos Konstitucinio Teismo pateikta bendra byla dėl Direktyvos 2006/24/EB (Duomenų saugojimo direktyva) atitikties ES duomenų apsaugos teisei. Austrijos Konstitucinis Teismas pateikė ESTT klausimus dėl Direktyvos 2006/24/EB 3–9 straipsnių galiojimo atsižvelgiant į ES pagrindinių teisių chartijos 7, 9 ir 11 straipsnius. Taip pat buvo klausiama, ar tam tikros Austrijos federalinio telekomunikacijų įstatymo nuostatos, kuriomis į nacionalinę teisę perkeliama Duomenų saugojimo direktyva, yra nesuderinamos su ankstesnės Duomenų apsaugos direktyvos ir ES institucijų duomenų apsaugos reglamento aspektais.

Byloje *Kärntner Landesregierung ir kt.* vienas iš pareiškėjų Konstitucinio Teismo nagrinėjamoje byloje M. Seitlinger nurodė, kad jis telefonu, internetu ir e. paštu naudojosi tiek profesiniais tikslais, tiek asmeniniame gyvenime. Todėl jo atsiųsta ir gauta informacija buvo perduota per viešuosius telekomunikacijų tinklus. Pagal 2003 m. Austrijos telekomunikacijų įstatymą jo telekomunikacijų paslaugų teikėjas teisiškai privalėjo rinkti ir saugoti duomenis apie naudojimąsi tinklu. M. Seitlinger manė, kad jo asmens duomenų rinkimas ir saugojimas techniniu požiūriu nereikalingas norint siųsti ir gauti informaciją tinkle. Be to, šių duomenų rinkimas ir saugojimas nebuvo būtinas sąskaitoms išrašyti. M. Seitlinger pareiškė, kad jis nesutiko su tokiu jo asmens duomenų naudojimu, kurie buvo renkami ir saugomi remiantis tik 2003 m. Austrijos telekomunikacijų įstatymu.

639 ESTT, sujungtos bylos C-293/12 ir C-594/12, *Digital Rights Ireland Ltd prieš Minister for Communications, Marine and Natural Resources ir kt.* ir Kärntner Landesregierung ir kt. (DK), 2014 m. balandžio 8 d.

640 ESTT, C-362/14, *Maximilian Schrems prieš Data Protection Commissioner* (DK), 2015 m. spalio 6 d.

641 ESTT, sujungtos bylos C-293/12 ir C-594/12, *Digital Rights Ireland Ltd prieš Minister for Communications, Marine and Natural Resources ir kt.* ir *Kärntner Landesregierung ir kt.* (DK), 2014 m. balandžio 8 d.

Todėl M. Seitlinger pareiškė ieškinį Austrijos Konstituciniame Teisme, kuriame teigė, kad telekomunikacijos paslaugų teikėjui teisės akte nustatytais įpareigojimais buvo pažeistos jo pagrindinės teisės pagal ES pagrindinių teisių chartijos 8 straipsnį. Atsižvelgdamas į tai, kad Austrijos teisės aktais įgyvendinta ES teisė (tuometinė Duomenų saugojimo direktyva), Austrijos Konstitucinis Teismas perdavė šį klausimą ESTT, kad šis priimtų sprendimą dėl direktyvos suderinamumo su ES pagrindinių teisių chartijoje įtvirtintomis teisėmis į privatumą ir duomenų apsaugą.

ESTT didžioji kolegija priėmė sprendimą byloje, dėl kurio buvo panaikinta ES duomenų saugojimo direktyva. ESTT nustatė, kad direktyva ypač rimtai pažeidžiamos pagrindinės teisės į privatumą ir duomenų apsaugą, tačiau šis apribojimas neapima to, kas tikrai būtina. Direktyva buvo siekiama teisėto tikslo, nes ji suteikė nacionalinėms valdžios institucijoms papildomų galimybių tirti sunkius nusikaltimus ir patraukti už juos baudžiamojon atsakomybėn, todėl ji buvo vertinga priemonė vykdant nusikalstamų veikų tyrimus. Tačiau ESTT pažymėjo, kad pagrindinių teisių apribojimai turėtų būti taikomi tik tuo atveju, jei tai tikrai būtina, ir kartu turėtų būti nustatytos aiškios ir tikslios jų taikymo srities taisyklės, taip pat fizinių asmenų apsaugos priemonės.

Pasak ESTT, direktyva neatitiko šio būtinumo kriterijaus. Pirma, ji nenustatė aiškių ir tikslių taisyklių, kuriomis būtų ribojamas kišimosi mastas. Užuot reikalavus ryšio tarp saugomų duomenų ir sunkių nusikaltimų, direktyva buvo taikoma visiems visų elektroninių ryšių priemonių naudotojų metaduomenims. Todėl tai buvo praktiškai visų ES gyventojų teisės į privatumą ir duomenų apsaugą apribojimas, kuris galėtų būti laikomas neproporcingu. Jame nebuvo sąlygų apriboti asmenų, kuriems leidžiama susipažinti su asmens duomenimis, skaičių, taip pat nebuvo nustatyta tokių procedūrinių sąlygų, kaip reikalavimas prieš susipažįstant su duomenimis gauti administracinės institucijos ar teismo sutikimą. Galiausiai direktyvoje nebuvo nustatytos aiškios saugomų duomenų apsaugos priemonės. Todėl ji neužtikrino veiksmingos duomenų apsaugos nuo piktnaudžiavimo rizikos ir nuo bet kokios neteisėtos prieigos prie duomenų ir jų naudojimo[642].

642 ESTT, sujungtos bylos C-293/12 ir C-594/12, *Digital Rights Ireland Ltd prieš Minister for Communications, Marine and Natural Resources ir kt.* ir *Kärntner Landesregierung ir kt.* (DK), 2014 m. balandžio 8 d., 69 punktas.

Iš esmės ESTT turi atsakyti į prejudicinius klausimus ir negali atsisakyti priimti prejudicinio sprendimo motyvuodamas tuo, kad šis atsakymas nebūtų nei aktualus, nei pateiktas laiku pirminei bylai. Tačiau jis gali atsisakyti priimti prejudicinį sprendimą, jei neturi kompetencijos nagrinėti klausimo[643]. ESTT priima sprendimą tik dėl prašymo priimti prejudicinį sprendimą sudedamųjų dalių, o nacionalinis teismas išlaiko kompetenciją priimti sprendimą pagrindinėje byloje[644].

Pagal ET teisę susitariančiosios šalys privalo nustatyti tinkamas teismines ir neteismines teisių gynimo priemones, kuriomis būtų galima pasinaudoti atnaujintos 108-osios konvencijos nuostatų pažeidimų atveju[645]. EŽTK susitariančiajai šaliai pareikštus įtarimus, susijusius su tuo, kad duomenų apsaugos teisių pažeidimai prieštarauja EŽTK 8 straipsniui, taip pat galima perduoti EŽTT, kai išnaudojamos visos prieinamos nacionalinės teisių gynimo priemonės. EŽTT pateiktas pareiškimas dėl EŽTK 8 straipsnio pažeidimo taip pat turi atitikti kitus priimtinumo kriterijus (EŽTK 34–35 straipsniai)[646].

Nors prašymai EŽTT gali būti adresuoti tik susitariančiosioms šalims, jie taip pat gali būti netiesiogiai susiję su privačių šalių veiksmais ar neveikimu, jeigu susitariančioji šalis neįvykdė savo „pozityviųjų“ prievolių pagal EŽTK ir savo nacionalinėje teisėje nesuteikė pakankamos apsaugos nuo duomenų apsaugos teisių pažeidimų.

Pavyzdys. *K. U. prieš Suomiją*[647] nepilnametis pareiškėjas pateikė skundą dėl jo vardu paskelbto seksualinio turinio skelbimo interneto pažinčių svetainėje. Paslaugų teikėjas neatskleidė šią informaciją paskelbusio asmens tapatybės dėl konfidencialumo reikalavimų pagal Suomijos įstatymus. Skundo pateikėjas tvirtino, kad Suomijos įstatymai nesuteikė jam pakankamos apsaugos nuo privataus asmens, internete paskelbusio kompromituojančių duomenų apie skundo pateikėją, veiksmų. EŽTT nusprendė, kad valstybės ne tik buvo priverstos susilaikyti nuo savavališko asmenų privataus gyvenimo apribojimo, bet joms taip pat turi būti nustatytos „pozityviosios“ prievolės, susijusios su „priemonių, kurios padėtų apsaugoti pagarbą privačiam gyvenimui net ir

643 ESTT, C-244/80, *Pasquale Foglia prieš Mariella Novello (No. 2)*, 1981 m. gruodžio 16 d.; ESTT, C-467/04, *Baudžiamoji byla prieš Gasparini ir kt.*, 2006 m. rugsėjo 28 d.

644 ESTT, C-438/05, *International Transport Workers' Federation, Finnish Seamen's Union prieš Viking Line ABP, OÜ Viking Line Eesti* (DK), 2007 m. gruodžio 11 d., 85 punktas.

645 Atnaujintos 108-osios konvencijos 12 straipsnis.

646 EŽTK 34–37 straipsniai.

647 EŽTT, *K. U. prieš Suomiją*, Nr. 2872/02, 2008 m. gruodžio 2 d.

asmenų tarpusavio santykių srityje, nustatymu“. Pareiškėjo byloje praktinė ir veiksminga apsauga reiškė būtinybę imtis veiksmingų priemonių nusikaltėliui nustatyti ir patraukti jį baudžiamojon atsakomybėn. Tačiau valstybė tokios apsaugos nesuteikė, ir EŽTT padarė išvadą, kad buvo pažeistas EŽTK 8 straipsnis.

Pavyzdys. Byloje *Köpke prieš Vokietiją*[648] pareiškėja buvo įtariama vagyste darbe ir stebima slapta vaizdo kamera. EŽTT padarė išvadą, kad „nebuvo jokių aplinkybių, rodančių, kad nacionalinės institucijos, veikdamos savo nuožiūra, nesugebėjo nustatyti tinkamos pareiškėjos teisės į privatų gyvenimą pagal 8 straipsnį ir jos darbdavio interesų, susijusių su savo nuosavybės apsauga, ir viešojo intereso, susijusio su tinkamu teisingumo vykdymu, pusiausvyros“. Todėl pareiškimas nebuvo priimtas nagrinėti.

Jei EŽTT nustato, kad susitariančioji šalis pažeidė kurią nors EŽTK saugomą teisę, ta susitariančioji šalis privalo vykdyti EŽTT sprendimą (EŽTK 46 straipsnis). Vykdymo priemonėmis visų pirma turi būti nutraukiamas pažeidimas ir, kiek tai įmanoma, ištaisomos neigiamos pažeidimo pasekmės, su kuriomis susidūrė pareiškėjas. Teismo sprendimų vykdymas taip pat gali reikšti bendrų priemonių, padedančių užkirsti kelią panašiems EŽTT nustatytiems pažeidimams, taikymą. Šiuo tikslu gali būti keičiami teisės aktai, teismų praktika arba nustatomos kitos priemonės.

Tais atvejais, kai EŽTT nustato EŽTK pažeidimą, EŽTK 41 straipsnyje nustatyta, kad jis gali priteisti pareiškėjui „teisingą atlyginimą“, kurį turės sumokėti susitariančioji šalis.

Teisė įgalioti ne pelno įstaigą, organizaciją ar asociaciją

Pagal BDAR asmenims suteikiama galimybė pateikti skundą priežiūros institucijai arba teisme pareikšti ieškinį ir įgalioti ne pelno įstaigą, organizaciją ar asociaciją jiems atstovauti[649]. Šie ne pelno subjektai turi turėti įstatymais nustatytus tikslus viešojo intereso srityje ir aktyviai veikti duomenų apsaugos srityje. Jie gali pateikti skundą arba pasinaudoti teise į teisminę teisių gynimo priemonę duomenų subjekto (-ų) vardu. Reglamentu valstybėms narėms suteikiama galimybė pagal nacionalinę teisę nuspręsti, ar įstaiga gali teikti skundus duomenų subjektų vardu neturėdama tų duomenų subjektų įgaliojimo.

648 EŽTT, *Köpke prieš Vokietiją*, Nr. 420/07, 2010 m. spalio 5 d.

649 Bendrojo duomenų apsaugos reglamento 80 straipsnis.

Ši atstovavimo teisė suteikia asmenims galimybę pasinaudoti tokių ne pelno subjektų kompetencija ir organizaciniu bei finansiniu pajėgumu ir taip labai palengvina asmenų galimybes pasinaudoti savo teisėmis. Pagal BDAR šie subjektai gali pareikšti kolektyvinius ieškinius kelių duomenų subjektų vardu. Tai taip pat naudinga teismų sistemos veikimui ir veiksmingumui, nes panašūs ieškiniai grupuojami ir nagrinėjami kartu.

6.2.3. Atsakomybė ir teisė į kompensaciją

Naudodamiesi teise į veiksmingą teisių gynimą, asmenys turi turėti galimybę reikalauti kompensuoti bet kokią žalą, kurią jie patyrė dėl jų asmens duomenų tvarkymo, dėl kurio buvo pažeisti taikomi teisės aktai. BDAR aiškiai pripažįstama duomenų valdytojų ir duomenų tvarkytojų atsakomybė už neteisėtą duomenų tvarkymą[650]. Reglamente asmenims suteikiama teisė, kad duomenų valdytojas arba duomenų tvarkytojas kompensuotų materialinę ir nematerialinę žalą, o jo konstatuojamosiose dalyse nustatyta, kad „[ž]alos sąvoka turėtų būti aiškinama plačiai, atsižvelgiant į Teisingumo Teismo praktiką, taip, kad būtų visapusiškai atspindėti šio reglamento tikslai“[651]. Duomenų valdytojai yra atsakingi ir jiems gali būti pareikšti reikalavimai atlyginti žalą, jeigu jie nevykdo savo prievolių pagal reglamentą. Asmens duomenų tvarkytojai atsako už tvarkant duomenis padarytą žalą tik tuo atveju, jei jie nesilaikė specialiai duomenų tvarkytojams nustatytų reglamento prievolių arba veikė nesilaikydami teisėtų duomenų valdytojo nurodymų arba juos pažeisdami. Jeigu duomenų valdytojas arba duomenų tvarkytojas sumokėjo visą kompensaciją, BDAR nustatyta, kad duomenų valdytojas arba duomenų tvarkytojas turi teisę reikalauti iš kitų tame pačiame duomenų tvarkymo procese dalyvavusių duomenų valdytojų arba duomenų tvarkytojų, kad jie sugrąžintų jam kompensacijos dalį, atitinkančią jų atsakomybės dalį[652]. Be to, atsakomybės išimtys yra labai griežtos ir jas taikant būtina įrodyti, kad duomenų valdytojas arba duomenų tvarkytojas jokiais būdais neatsako už įvykį, dėl kurio atsirado žala.

Patirta žala turi būti kompensuojama „visa ir veiksmingai“. Jeigu žalą sukelia kelių duomenų valdytojų ir duomenų tvarkytojų vykdomas duomenų tvarkymas, kiekvienas duomenų valdytojas arba duomenų tvarkytojas privalo atsakyti už visą žalą. Šia taisykle siekiama užtikrinti veiksmingą kompensavimą duomenų subjektams ir

650 *Ten pat*, 82 straipsnis.

651 *Ten pat*, 146 konstatuojamoji dalis.

652 *Ten pat*, 85 straipsnio 2 ir 5 dalys.

koordinuotą požiūrį į tai, kaip duomenų tvarkymo veikloje dalyvaujantys duomenų valdytojai ir duomenų tvarkytojai laikosi reikalavimų.

Pavyzdys. Nereikalaujama, kad duomenų subjektai iškeltų bylą ir reikalautų kompensacijos iš visų už žalą atsakingų subjektų, nes toks procesas gali brangiai kainuoti ir ilgai trukti. Pakanka iškelti bylą vienam iš bendrų duomenų valdytojų, kuris tuomet gali būti laikomas atsakingu už visą žalą. Tokiais atvejais duomenų valdytojas arba duomenų tvarkytojas, kuris sumoka žalą, vėliau turi teisę susigrąžinti sumokėtą sumą iš kitų subjektų, susijusių su duomenų tvarkymu ir atsakingų už pažeidimą, už jų atsakomybės už žalą dalį. Šie procesai tarp skirtingų bendrų duomenų valdytojų ir duomenų tvarkytojų vyksta duomenų subjektui gavus kompensaciją, ir duomenų subjektas juose nedalyvauja.

Pagal ET teisinę sistemą, t. y. atnaujintos 108-osios konvencijos 12 straipsnį, reikalaujama, kad susitariančiosios šalys nustatytų tinkamas teisių gynimo priemones, kuriomis būtų galima pasinaudoti tais atvejais, kai pažeidžiami nacionaliniai įstatymai, kuriais įgyvendinami Konvencijos reikalavimai. Atnaujintos 108-osios konvencijos aiškinamojoje ataskaitoje nurodyta, kad tarp teisių gynimo priemonių turi būti galimybė teisme ginčyti sprendimą arba praktiką, be to, taip pat turi būti prieinamos neteisminės teisių gynimo priemonės[653]. Sąlygos ir skirtingos taisyklės, susijusios su galimybe pasinaudoti šiomis teisių gynimo priemonėmis, taip pat procedūra, kurios reikia laikytis, paliekamos kiekvienos susitariančiosios šalies nuožiūrai. Susitariančiosios šalys ir nacionaliniai teismai taip pat turėtų apsvarstyti nuostatas dėl finansinės kompensacijos už materialinę ir nematerialinę žalą, padarytą dėl duomenų tvarkymo, taip pat galimybę sudaryti sąlygas pareikšti kolektyvinius ieškinius[654].

6.2.4. Sankcijos

Pagal ET teisę, atnaujintos 108-osios konvencijos 12 straipsnyje nustatyta, kad kiekviena susitariančioji šalis privalo nustatyti tinkamas sankcijas ir teisių gynimo priemones už nacionalinės teisės nuostatų, kuriomis įgyvendinami pagrindiniai 108-ojoje konvencijoje nustatyti duomenų apsaugos principai, pažeidimus. Konvencijoje nenustatomas konkretus privalomų ar neprivalomų sankcijų rinkinys. Priešingai, joje aiškiai nurodyta, kad kiekviena susitariančioji šalis turi diskreciją nustatyti

653 Atnaujintos 108-osios konvencijos aiškinamosios ataskaitos 100 punktas.

654 *Ten pat*.

teisminių arba neteisminių sankcijų, kurios gali būti baudžiamosios, administracinės arba civilinės, pobūdį. Atnaujintos 108-osios konvencijos aiškinamojoje ataskaitoje nustatyta, kad sankcijos turi būti veiksmingos, proporcingos ir atgrasomos[655]. Susitariančiosios šalys, savo nacionalinėje teisėje nustatydamos sankcijų pobūdį ir griežtumą, privalo paisyti šio principo.

Pagal ES teisę, BDAR 83 straipsnyje valstybių narių priežiūros institucijoms suteikiami įgaliojimai nustatyti administracines baudas už reglamento pažeidimus. Baudų dydis ir aplinkybės, į kurias atsižvelgia nacionalinės valdžios institucijos, spręsdamos, ar skirti baudą, taip pat bendros didžiausios tos baudos ribos taip pat nustatytos 83 straipsnyje. Taigi visoje ES galioja vienoda sankcijų skyrimo tvarka.

BDAR nustatytos baudos yra diferencijuotos. Priežiūros institucijos turi įgaliojimus už reglamento pažeidimus skirti administracines baudas iki 20 000 000 EUR arba įmonės atveju – iki 4 % jos bendros metinės pasaulinės apyvartos, atsižvelgiant į tai, kuri suma yra didesnė. Pažeidimai, už kuriuos gali būti skiriamos tokio dydžio baudos, apima pagrindinių duomenų tvarkymo principų ir sutikimo sąlygų pažeidimus, duomenų subjektų teisių ir reglamento nuostatų, kuriomis reglamentuojamas asmens duomenų perdavimas trečiųjų šalių gavėjams, pažeidimus. Už kitus pažeidimus priežiūros institucijos gali skirti baudas iki 10 000 000 EUR arba įmonės atveju – iki 2 % jos bendros metinės pasaulinės apyvartos, atsižvelgiant į tai, kuri suma yra didesnė.

Nustatydamos skiriamos baudos rūšį ir dydį, priežiūros institucijos privalo atsižvelgti į įvairius veiksnius[656]. Pavyzdžiui, jos privalo tinkamai atsižvelgti į pažeidimo pobūdį, rimtumą ir trukmę, asmens duomenų, kuriems padaryta žala, kategorijas ir tai, ar pažeidimas buvo padarytas tyčia, ar dėl aplaidumo. Jeigu duomenų valdytojas arba duomenų tvarkytojas ėmėsi veiksmų duomenų subjektų patirtai žalai sumažinti, į tai taip pat reikėtų atsižvelgti. Panašiai, bendradarbiavimo su priežiūros institucijomis po pažeidimo mastas ir būdas, kuriuo priežiūros institucija sužinojo apie pažeidimą (pavyzdžiui, ar apie jį pranešė už duomenų tvarkymą atsakingas subjektas, ar duomenų subjektas, kurio teisės buvo pažeistos), yra kiti svarbūs veiksniai, padedantys priežiūros institucijoms priimti sprendimą[657].

655 *Ten pat*.

656 Bendrojo duomenų apsaugos reglamento 83 straipsnio 2 dalis.

657 29 straipsnio darbo grupė (2017 m.), *Administracinių baudų taikymo ir nustatymo įgyvendinant Reglamentą 2016/679 rekomendacijos*, WP 253, 2017 m. spalio 3 d.

Priežiūros institucijos gali skirti ne tik administracines baudas, jos taip pat turi plačius įgaliojimus imtis taisomųjų veiksmų. Priežiūros institucijų vadinamieji įgaliojimai imtis „taisomųjų veiksmų“ išdėstyti BDAR 58 straipsnyje. Šie įgaliojimai apima įsakymų priėmimą, įspėjimus ir papeikimų pareiškimą duomenų valdytojams ir duomenų tvarkytojams, taip pat laikiną ar net nuolatinį draudimą vykdyti duomenų tvarkymo veiklą.

Kalbant apie sankcijas už ES institucijų ar įstaigų padarytus ES teisės pažeidimus, atsižvelgiant į ypatingą ES institucijų duomenų apsaugos reglamento taikymo sritį, sankcijos gali būti numatytos kaip drausminės priemonės. Pagal to reglamento 49 straipsnį „[j]eigu pareigūnas ar kitas Europos Bendrijų tarnautojas tyčia ar per aplaidumą nevykdo šiame reglamente nustatytų įsipareigojimų, <...> jam gali būti iškelta drausminė byla“.

7

Tarpvalstybinis duomenų perdavimas ir asmens duomenų judėjimas

ES	Reglamentuojami klausimai	ET
Asmens duomenų perdavimas		
Bendrojo duomenų apsaugos reglamento 44 straipsnis	Koncepcija	Atnaujintos 108-osios konvencijos 14 straipsnio 1 ir 2 dalys
Laisvas asmens duomenų judėjimas		
Bendrojo duomenų apsaugos reglamento 1 straipsnio 3 dalis ir 170 konstatuojamoji dalis	Tarp ES valstybių narių	
	Tarp 108-osios konvencijos susitariančiųjų šalių	Atnaujintos 108-osios konvencijos 14 straipsnio 1 dalis
Asmens duomenų perdavimas trečiosioms šalims arba tarptautinėms organizacijoms		
Bendrojo duomenų apsaugos reglamento 45 straipsnis C-362/14, *Maximillian Schrems prieš Data Protection Commissioner* (DK), 2015 m.	Sprendimas dėl tinkamumo / trečiosios šalys arba tarptautinės organizacijos, kuriose užtikrinamas tinkamas apsaugos lygis	Atnaujintos 108-osios konvencijos 14 straipsnio 2 dalis
Bendrojo duomenų apsaugos reglamento 46 straipsnio 1 dalis ir 46 straipsnio 2 dalis	Tinkamos apsaugos priemonės, įskaitant įgyvendinamas teises ir teisines teisių gynimo priemones, kuriomis gali pasinaudoti duomenų subjektai, nustatytas standartinėse sutarčių sąlygose, įmonėms privalomos taisyklės, elgesio kodeksai ir sertifikavimo mechanizmai.	Atnaujintos 108-osios konvencijos 14 straipsnio 2, 3, 5 ir 6 dalys

ES	Reglamentuojami klausimai	ET
Bendrojo duomenų apsaugos reglamento 46 straipsnio 3 dalis	Gavus kompetentingos priežiūros institucijos leidimą: sutarčių sąlygos ir nuostatos, įtrauktos į valdžios institucijų administracinius susitarimus	
Bendrojo duomenų apsaugos reglamento 46 straipsnio 5 dalis	Galiojantys leidimai pagal Direktyvą 95/46/EB	
Bendrojo duomenų apsaugos reglamento 47 straipsnis	Įmonėms privalomos taisyklės	
Bendrojo duomenų apsaugos reglamento 49 straipsnis	Konkrečiais atvejais nukrypti leidžiančios nuostatos	Atnaujintos 108-osios konvencijos 14 straipsnio 4 dalis
Pavyzdžiai: ES ir JAV PNR susitarimas ES ir JAV SWIFT susitarimas	Tarptautiniai susitarimai	Atnaujintos 108-osios konvencijos 14 straipsnio 3 dalies a punktas

ES teisėje, Bendrajame duomenų apsaugos reglamente, nustatyta, kad duomenys Europos Sąjungoje gali judėti laisvai. Tačiau jame nustatyti specialūs reikalavimai, susiję su asmens duomenų perdavimu užsienio trečiosioms šalims ir tarptautinėms organizacijoms. Reglamente pripažįstama tokio duomenų judėjimo svarba, visų pirma atsižvelgiant į tarptautinę prekybą ir bendradarbiavimą, be to, pripažįstama didesnė asmens duomenims kylanti rizika. Todėl reglamentu siekiama užtikrinti, kad, perduodant duomenis trečiosioms šalims, būtų užtikrinamas toks pat asmens duomenų apsaugos lygis, kuris galioja ES[658]. ET teisėje taip pat pripažįstama tarpvalstybinio duomenų judėjimo įgyvendinimo taisyklių, grindžiamų laisvu šalių judėjimu ir konkrečiais perdavimo ne šalims reikalavimais, svarba.

7.1. Asmens duomenų perdavimo pobūdis

Pagrindiniai faktai

- ES ir ET teisės aktuose nustatytos asmens duomenų perdavimo trečiosiose šalyse esantiems gavėjams arba tarptautinėms organizacijoms taisyklės.
- Užtikrinus, kad būtų apsaugotos duomenų subjekto teisės, kai duomenys perduodami už ES ribų, ES teisės aktais užtikrinama apsauga leidžia stebėti iš ES kilusius asmens duomenis.

658 Bendrojo duomenų apsaugos reglamento 101 ir 116 konstatuojamosios dalys.

Pagal **ET teisę** tarpvalstybinis duomenų judėjimas apibūdinamas kaip asmens duomenų perdavimas gavėjams, kuriems taikomos užsienio jurisdikcijos taisyklės[659]. Tarpvalstybinis duomenų judėjimas juos perduodant gavėjui, kuriam netaikomos susitariančiosios šalies jurisdikcijos taisyklės, yra leidžiamas, tik jeigu esama tinkamo apsaugos lygio[660].

ES teisėje reglamentuojamas „[a]smens duomen[ų], kurie yra tvarkomi arba kuriuos ketinama tvarkyti juos perdavus į trečiąją valstybę arba tarptautinei organizacijai“, perdavimas[661]. Toks duomenų judėjimas leidžiamas, tik jeigu jis atitinka BDAR V skyriuje nustatytas taisykles.

Tarpvalstybinis asmens duomenų judėjimas leidžiamas gavėjui, kuriam atitinkamai pagal ET teisę arba ES teisę taikoma susitariančiosios šalies arba valstybės narės jurisdikcija. Abiejose teisinėse sistemose taip pat leidžiama perduoti duomenis į šalį, kuri nėra susitariančioji šalis arba valstybė narė, jeigu įvykdomos tam tikros sąlygos.

7.2. Laisvas asmens duomenų judėjimas tarp valstybių narių arba susitariančiųjų šalių

Pagrindiniai faktai

- Asmens duomenų judėjimas Europos Sąjungoje, taip pat asmens duomenų perdavimas tarp atnaujintos 108-osios konvencijos susitariančiųjų šalių turi būti vykdomas be apribojimų. Tačiau ne visos atnaujintos 108-osios konvencijos susitariančiosios šalys yra ES valstybės narės, todėl duomenų perdavimas iš ES valstybės narės trečiajai šaliai, t. y. bet kuriuo atveju 108-osios konvencijos susitariančiajai šaliai, nėra įmanomas, išskyrus atvejus, kai jos atitinka BDAR nustatytas sąlygas.

Pagal ET teisę turi būti užtikrinamas laisvas asmens duomenų judėjimas tarp atnaujintos 108-osios konvencijos susitariančiųjų šalių. Tačiau perdavimas gali būti uždraustas, jei yra „realus ir rimtas pavojus, kad dėl perdavimo kitai Šaliai bus apeinamos Konvencijos nuostatos“ arba jei Šalis privalo tai daryti vadovaudamasi „suderintomis apsaugos taisyklėmis, kuriomis dalijasi valstybės, priklausančios regioninei tarptautinei organizacijai“[662].

659 Atnaujintos 108-osios konvencijos aiškinamosios ataskaitos 102 punktas.

660 Atnaujintos 108-osios konvencijos 14 straipsnio 2 dalis.

661 Bendrojo duomenų apsaugos reglamento 44 straipsnis.

662 Atnaujintos 108-osios konvencijos 14 straipsnio 1 dalis.

Pagal ES teisę laisvo asmens duomenų judėjimo tarp ES valstybių narių apribojimai arba draudimai atsižvelgiant į priežastis, susijusias su fizinių asmenų apsauga tvarkant asmens duomenis, yra negalimi[663]. Laisvo duomenų judėjimo erdvė praplėsta susitarimu dėl Europos ekonominės erdvės (EEE)[664], kuriuo į vidaus rinką įtraukiama Islandija, Lichtenšteinas ir Norvegija.

Pavyzdys. Jei tarptautinės bendrovių grupės, įsteigtos keliose valstybėse narėse, įskaitant Slovėniją ir Prancūziją, filialas siunčia asmens duomenis iš Slovėnijos į Prancūziją, toks duomenų judėjimas neturi būti ribojamas ar draudžiamas pagal Slovėnijos nacionalinę teisę dėl priežasčių, susijusių su asmens duomenų apsauga.

Tačiau jeigu ta pati Slovėnijos susijusi bendrovė nori perduoti tuos pačius asmens duomenis patronuojančiajai bendrovei Malaizijoje, Slovėnijos duomenų eksportuotojas privalo atsižvelgti į BDAR V skyriaus taisykles. Šiomis nuostatomis siekiama apsaugoti ES jurisdikcijai priklausančių duomenų subjektų asmens duomenis.

Pagal ES teisę asmens duomenų judėjimui į EEE valstybes nares nusikalstamų veikų prevencijos, tyrimo, nustatymo ar traukimo baudžiamojon atsakomybėn už jas arba baudžiamųjų sankcijų vykdymo tikslais taikoma Direktyva (ES) 2016/680[665]. Taip, be kita ko, užtikrinama, kad kompetentingų institucijų keitimasis asmens duomenimis Sąjungoje nebūtų ribojamas ar draudžiamas dėl duomenų apsaugos priežasčių. Pagal ET teisę visų asmens duomenų tvarkymas (įskaitant jų tarpvalstybinį judėjimą į kitas 108-osios konvencijos šalis), nedarant jokių išimčių, pagrįstų tikslais arba veiklos sritimis, patenka į 108-osios konvencijos taikymo sritį, tačiau susitariančiosios šalys gali daryti išimtis. Visos EEE narės taip pat yra 108-osios konvencijos šalys.

663 Bendrojo duomenų apsaugos reglamento 1 straipsnio 3 dalis.

664 1993 m. gruodžio 13 d. Tarybos ir Komisijos sprendimas dėl Europos ekonominės erdvės sutarties sudarymo tarp Europos Bendrijų, jų valstybių narių ir Austrijos Respublikos, Suomijos Respublikos, Islandijos Respublikos, Lichtenšteino Kunigaikštystės, Norvegijos Karalystės, Švedijos Karalystės ir Šveicarijos Konfederacijos, OL L 1, 1994.

665 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, ir kuria panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR, OL L 119, 2016.

7.3. Asmens duomenų perdavimas trečiosioms šalims / šalims, kurios nėra 108-osios konvencijos susitariančiosios šalys, arba tarptautinėms organizacijoms

Pagrindiniai faktai

- **ET** ir **ES** leidžia perduoti asmens duomenis trečiosioms šalims arba tarptautinėms organizacijoms, jeigu įvykdomos tam tikros asmens duomenų apsaugos sąlygos.
  - **Pagal ET teisę** tinkamas apsaugos lygis gali būti pasiekiamas pagal valstybės arba tarptautinės organizacijos teisę arba nustatant tinkamus standartus.
  - **Pagal ES teisę** duomenys gali būti perduodami, jeigu trečioji šalis užtikrina tinkamą apsaugos lygį arba jeigu duomenų valdytojas arba duomenų tvarkytojas numato tinkamas apsaugos priemones, įskaitant užtikrinamas duomenų subjektų teises ir teisines teisių gynimo priemones šiuo tikslu, pavyzdžiui, nustatydamas standartines duomenų apsaugos sąlygas arba įmonėms privalomas taisykles.
- **ET ir ES teisėje** numatytos nukrypti leidžiančios nuostatos, pagal kurias asmens duomenis konkrečiomis aplinkybėmis leidžiama perduoti net tais atvejais, kai neužtikrinamas tinkamas apsaugos lygis ir kai nėra nustatytų tinkamų apsaugos priemonių.

Pagal ET teisę ir ES teisę leidžiamas duomenų judėjimas į trečiąsias šalis arba tarptautines organizacijas, tačiau šiose teisinėse sistemose nustatytos skirtingos sąlygos. Kiekviename sąlygų rinkinyje atsižvelgiama į skirtingą atitinkamos organizacijos struktūrą ir tikslus.

Pagal **ES teisę** asmens duomenis trečiosioms šalims arba tarptautinėms organizacijoms leidžiama perduoti iš esmės dviem būdais. Asmens duomenys gali būti perduodami remiantis Europos Komisijos sprendimu dėl tinkamumo[666] arba, jeigu tokio sprendimo nėra, duomenų valdytojo arba duomenų tvarkytojo numatytomis tinkamomis apsaugos priemonėmis, įskaitant įgyvendinamas teises ir duomenų subjekto teisines gynimo priemones[667]. Jeigu nėra nei sprendimo dėl tinkamumo, nei tinkamų apsaugos priemonių, galima pasinaudoti įvairiomis nukrypti leidžiančiomis nuostatomis.

666 Bendrojo duomenų apsaugos reglamento 45 straipsnis.

667 *Ten pat*, 46 straipsnis.

Tačiau pagal **ET teisę** laisvas duomenų perdavimas šalims, kurios nėra Konvencijos susitariančiosios šalys, leidžiamas tik remiantis:

- tos valstybės arba tarptautinės organizacijos teise, įskaitant taikytinas tarptautines sutartis arba susitarimus, kuriais garantuojamos tinkamos apsaugos priemonės;

- *ad hoc* arba patvirtintomis standartizuotomis apsaugos priemonėmis, numatytomis teisiškai privalomose ir užtikrinamose priemonėse, kurias priėmė ir įgyvendino su duomenų perdavimu ir tolesniu tvarkymu susiję asmenys[668].

Kaip ir ES teisėje, jeigu neužtikrinamas tinkamas duomenų apsaugos lygis, galima pasinaudoti įvairiomis nukrypti leidžiančiomis nuostatomis.

7.3.1. Duomenų perdavimas remiantis sprendimu dėl tinkamumo

Pagal ES teisę laisvas asmens duomenų judėjimas į trečiąsias šalis, kuriose užtikrinamas tinkamas duomenų apsaugos lygis, numatytas BDAR 45 straipsnyje. ESTT paaiškino, kad pagal sąvoką „[tinkamas] apsaugos lygis" reikalaujama, kad trečioji šalis užtikrintų „iš esmės tokį patį"[669] pagrindinių teisių ir laisvių apsaugos lygį, koks garantuojamas ES teisėje. Kartu priemonės, kuriomis trečioji šalis gali pasinaudoti siekdama užtikrinti tokį apsaugos lygį, gali skirtis nuo Europos Sąjungos viduje naudojamų priemonių, todėl pagal tinkamumo standartą nereikalaujama, kad ES taisyklės būtų tiesiogiai atkartojamos[670].

Europos Komisija duomenų apsaugos lygį užsienio šalyse įvertina nagrinėdama jų nacionalinę teisę ir taikomus tarptautinius įsipareigojimus. Taip pat reikia atsižvelgti į šalies dalyvavimą daugiašalėse arba regioninėse sistemose, visų pirma asmens duomenų apsaugos srityje. Jeigu Europos Komisija nustato, kad trečioji šalis arba tarptautinė organizacija užtikrina tinkamą apsaugos lygį, ji gali priimti privalomą

668 Atnaujintos 108-osios konvencijos 14 straipsnio 3 dalies a ir b punktai.

669 ESTT, C-362/14, *Maximillian Schrems prieš Data Protection Commissioner* (DK), 2015 m. spalio 6 d., 96 punktas.

670 *Ten pat*, 74 punktas. Taip pat žr. Europos Komisija (2017 m.), Komisijos komunikatas Europos Parlamentui ir Tarybai „Keitimasis asmens duomenimis ir jų apsauga globaliame pasaulyje", COM(2017) 7 *final*, 2017 m. sausio 10 d., p. 6.

galią turintį sprendimą dėl tinkamumo[671]. Vis dėlto ESTT nurodė, kad nacionalinės priežiūros institucijos vis dar turi kompetenciją nagrinėti asmens skundą dėl asmens duomenų, kurie buvo perduoti trečiajai šaliai ir kuriuos Komisija laiko užtikrinančiais tinkamą apsaugos lygį, apsaugos, jei tas asmuo teigia, kad trečiojoje šalyje galiojančiais teisės aktais ir praktika neužtikrinamas tinkamas apsaugos lygis[672].

Europos Komisija taip pat gali įvertinti teritorijos tinkamumą trečiojoje šalyje arba apsiriboti konkrečiais sektoriais, pavyzdžiui, Kanados privačių prekybos teisės aktų atveju[673]. Taip pat padarytos išvados dėl duomenų perdavimo remiantis ES ir trečiųjų šalių susitarimais tinkamumo. Šie sprendimai susiję tik su vienos rūšies duomenų perdavimu, pavyzdžiui, oro transporto bendrovės keleivio duomenų įrašų (PNR) perdavimu užsienio sienų kontrolės institucijoms, kai oro transporto bendrovė vykdo skrydžius iš ES į tam tikras užsienio paskirties vietas (žr. 7.3.4 skirsnį).

Sprendimai dėl tinkamumo nuolat stebimi. Europos Komisija reguliariai peržiūri tokius sprendimus, kad nustatytų pokyčius, kurie galėtų turėti įtakos jų statusui. Taigi, jei Europos Komisija nustato, kad trečioji šalis arba tarptautinė organizacija nebeatitinka sąlygų, kuriomis grindžiamas sprendimas dėl tinkamumo, ji gali iš dalies pakeisti, sustabdyti arba panaikinti sprendimo galiojimą. Komisija taip pat gali pradėti derybas su atitinkama trečiąja šalimi arba tarptautine organizacija, kad išspręstų klausimą, dėl kurio ji priėmė sprendimą.

Sprendimai dėl tinkamumo, kuriuos Europos Komisija priėmė remdamasi Direktyva 95/46/EB, lieka galioti, kol Komisijos sprendimu, priimtu pagal BDAR 45 straipsnyje nustatytas taisykles, jie bus iš dalies pakeisti, pakeisti naujais sprendimais arba panaikinti.

Iki šiol Europos Komisija pripažino, kad Andora, Argentina, Kanada (komercinės organizacijos, kurioms taikomas Asmeninės informacijos ir elektroninių dokumentų įstatymas (PIPEDA)), Farerų salos, Gernsis, Meno sala, Izraelis, Džersis, Naujoji Zelandija, Šveicarija ir Urugvajus suteikia tinkamą apsaugą. Kalbant apie duomenų perdavimą JAV, pažymėtina, kad Europos Komisija 2000 m. priėmė sprendimą dėl tinkamumo,

671 Nuolat atnaujinamas šalių, kurios gavo išvadą dėl tinkamumo, sąrašas pateikiamas Europos Komisijos Teisingumo generalinio direktorato pradžios tinklalapyje.

672 ESTT, C-362/14, *Maximilian Schrems prieš Data Protection Commissioner* (DK), 2015 m. spalio 6 d., 63 ir 65–66 punktai.

673 Europos Komisija (2002 m.), 2001 m. gruodžio 20 d. Sprendimas 2002/2/EB dėl Kanados asmens duomenų apsaugos ir elektroninių dokumentų įstatyme numatytos tinkamos asmens duomenų apsaugos pagal Europos Parlamento ir Tarybos direktyvą 95/46/EB, OL L 2, 2002.

kuriuo leidžiama duomenis perduoti įmonėms, kurios pačios patvirtino, kad apsaugos iš ES perduotus duomenis ir laikysis vadinamųjų „saugaus uosto“ principų[674]. ESTT 2015 m. sprendimu pripažino šį sprendimą negaliojančiu, o 2016 m. liepos mėn. buvo priimtas naujas sprendimas dėl tinkamumo, kuriuo bendrovėms leista prisijungti nuo 2016 m. rugpjūčio 1 d.

Pavyzdys. Byloje *Schrems*[675] Austrijos pilietis Maximilian Schrems keletą metų naudojosi *Facebook*. Dalis arba visi duomenys, kuriuos M. Schrems pateikė *Facebook*, buvo perduoti iš *Facebook* Airijos patronuojamosios bendrovės į JAV esančius serverius, kur jie buvo tvarkomi. M. Schrems pateikė skundą Airijos duomenų apsaugos institucijai, manydamas, kad, atsižvelgiant į JAV informatoriaus Edwardo Snowdeno atskleistą informaciją dėl JAV žvalgybos tarnybų sekimo veiklos, JAV teisė ir praktika neužtikrina pakankamos šiai šaliai perduotų duomenų apsaugos. Airijos valdžios institucija skundą atmetė, motyvuodama tuo, kad 2000 m. liepos 26 d. sprendime Komisija nusprendė, jog pagal „saugaus uosto“ schemą JAV užtikrina tinkamą perduodamų asmens duomenų apsaugos lygį. Byla buvo iškelta Airijos aukštajame teisme, kuris kreipėsi į ESTT prašydamas priimti prejudicinį sprendimą.

ESTT nusprendė, kad Komisijos sprendimas dėl „saugaus uosto“ sistemos tinkamumo negaliojo. ESTT pirmiausia pažymėjo, kad sprendimu buvo leista apriboti „saugaus uosto“ duomenų apsaugos principų taikymą remiantis nacionalinio saugumo, viešojo intereso ar teisėsaugos reikalavimais arba JAV nacionalinės teisės aktais. Todėl šis sprendimas leido apriboti asmenų, kurių asmens duomenys buvo arba galėjo būti perduoti JAV, pagrindines teises[676]. Jis taip pat pažymėjo, kad sprendime nepateikta jokių išvadų dėl to, ar JAV yra taisyklių, kuriomis siekiama apriboti tokį kišimąsi, ar dėl veiksmingos teisinės apsaugos nuo tokio kišimosi buvimo[677]. ESTT atkreipė dėmesį į tai, kad, atsižvelgiant į ES garantuojamų pagrindinių teisių ir laisvių lygį, reikėjo, kad teisės aktuose, kuriais apribojamas 7 ir 8 straipsnių taikymas, būtų nustatytos aiškios ir tikslios taisyklės, kuriomis apibrėžiamas priemonės mastas ir taikymo sritis, ir nustatomos minimalios apsaugos priemonės, nukrypti

674 2000 m. liepos 26 d. Komisijos sprendimas 2000/520/EB dėl „saugaus uosto“ privatumo principų teikiamos apsaugos pakankamumo pagal Europos Parlamento ir Tarybos direktyvą 95/46/EB ir susijusių JAV komercijos departamento pateiktų dažnai užduodamų klausimų, OL L 215. Šį sprendimą ESTT pripažino negaliojančiu byloje C-632/14, *Maximilian Schrems prieš Data Protection Commissioner* (DK).

675 ESTT, C-362/14, *Maximilian Schrems prieš Data Protection Commissioner* (DK), 2015 m. spalio 6 d.

676 *Ten pat*, 84 punktas.

677 *Ten pat*, 88–89 punktai.

leidžiančios nuostatos ir apribojimai, susiję su asmens duomenų apsauga[678]. Atsižvelgdamas į tai, kad Komisijos sprendime nebuvo nurodyta, kad JAV iš tikrųjų užtikrina tokį apsaugos lygį savo nacionalinėje teisėje arba tarptautiniais įsipareigojimais, ESTT padarė išvadą, kad JAV nesugebėjo įvykdyti atitinkamos Duomenų apsaugos direktyvos nuostatos dėl perdavimo, todėl jis negaliojo[679].

Todėl JAV pagrindinių teisių ir laisvių apsaugos lygis „iš esmės [nebuvo] toks pat“, kokį garantavo ES[680]. ESTT teigė, kad buvo pažeisti įvairūs ES pagrindinių teisių chartijos straipsniai. Pirma, buvo pažeista 7 straipsnio esmė, nes pagal JAV teisės aktą „valdžios institucijoms, remiantis bendrais pagrindais, buvo leidžiama susipažinti su elektroninių ryšių turiniu“. Antra, taip pat buvo pažeista 47 straipsnio esmė, nes teisės akte nebuvo galimybės asmenims pasinaudoti teisių gynimo priemonėmis, susijusiomis su galimybe susipažinti su asmens duomenimis arba ištaisyti ar ištrinti asmens duomenis. Galiausiai, atsižvelgiant į tai, kad „saugaus uosto“ susitarimu buvo pažeisti minėti straipsniai, asmens duomenys nebebuvo tvarkomi teisėtai, todėl buvo pažeistas 8 straipsnis.

ESTT paskelbus „saugaus uosto“ susitarimą negaliojančiu, Komisija ir JAV susitarė dėl naujos ES ir JAV „privatumo skydo“ sistemos. 2016 m. liepos 12 d. Komisija priėmė sprendimą, kuriuo paskelbė, kad JAV pagal „privatumo skydo“ sistemą užtikrina tinkamą duomenų, kurie iš Sąjungos perduodami JAV organizacijoms, apsaugos lygį[681].

Panašiai kaip ir „saugaus uosto“ susitarimu, ES ir JAV „privatumo skydo“ sistema siekiama apsaugoti asmens duomenis, kurie iš ES perduodami į JAV komerciniais tikslais[682]. JAV bendrovės gali savanoriškai pačios patvirtinti, kad jos laikosi „privatumo

678 *Ten pat*, 91–92 punktai.

679 *Ten pat*, 96–97 punktai.

680 *Ten pat*, 73–74 ir 96 punktai.

681 2016 m. liepos 12 d. Komisijos įgyvendinimo sprendimas (ES) 2016/1250 dėl ES ir JAV „privatumo skydo“ užtikrinamos apsaugos tinkamumo pagal Europos Parlamento ir Tarybos direktyvą 95/46/EB, OL L 207. 29 straipsnio darbo grupė palankiai įvertino „privatumo skydo“ mechanizmo patobulinimus, palyginti su sprendimu dėl apsaugos taisyklės, ir palankiai įvertino tai, kad Komisija ir JAV valdžios institucijos galutinėje „privatumo skydo“ dokumentų redakcijoje atsižvelgė į jų nuomonėje WP 238 dėl ES ir JAV sprendimo dėl „privatumo skydo“ tinkamumo projekto išdėstytus susirūpinimą keliančius klausimus. Vis dėlto ji atkreipė dėmesį į keletą neišspręstų klausimų. Daugiau informacijos žr. 29 straipsnio duomenų apsaugos darbo grupė, *Nuomonė Nr. 01/2016 dėl sprendimo dėl ES ir JAV „privatumo skydo“ tinkamumo projekto*, priimta 2016 m. balandžio 13 d., 16/EN WP 238.

682 Daugiau informacijos žr. ES ir JAV „privatumo skydo“ informacijos suvestinė.

skydo“ sąrašo įsipareigodamos laikytis sistemos duomenų apsaugos standartų. Kompetentingos JAV institucijos stebi ir tikrina, kaip sertifikuotos bendrovės laikosi šių standartų.

Visų pirma „privatumo skydo“ sistemoje numatyta:

- duomenų apsaugos prievolės, taikomos iš ES asmens duomenis gaunančioms bendrovėms;

- asmenų apsauga ir teisių gynimas, visų pirma ombudsmeno mechanizmo, kuris yra nepriklausomas nuo JAV žvalgybos tarnybų ir nagrinėja asmenų, manančių, kad JAV institucijos jų asmens duomenis nacionalinio saugumo tikslais naudojo neteisėtai, teisių gynimo priemonių nustatymas;

- metinė bendra peržiūra, siekiant stebėti, kaip įgyvendinama sistema[683]; pirmoji peržiūra atlikta 2017 m. rugsėjo mėn.[684]

Prie sprendimo dėl „privatumo skydo“ JAV vyriausybė pridėjo rašytinius įsipareigojimus ir garantijas. Juose numatyti JAV vyriausybės galimybės susipažinti su asmens duomenimis teisėsaugos ir nacionalinio saugumo tikslais apribojimai ir su tuo susijusios apsaugos priemonės.

7.3.2. Duomenų perdavimas taikant tinkamas apsaugos priemones

ES ir **ET teisėje** pripažįstama, kad tinkamos apsaugos priemonės, kurias taiko duomenis eksportuojantis duomenų valdytojas ir gavėjas trečiojoje šalyje arba tarptautinė organizacija, yra būdas, galintis padėti užtikrinti pakankamą duomenų apsaugos lygį gavėjo atžvilgiu.

Pagal **ES teisę** asmens duomenų perdavimas į trečiąją šalį arba tarptautinę organizaciją leidžiamas, jeigu duomenų valdytojas arba duomenų tvarkytojas užtikrina tinkamas apsaugos priemones ir įgyvendinamas teises ir jeigu duomenų subjektai gali

683 Daugiau informacijos žr. Europos Komisijos svetainės tinklalapyje apie ES ir JAV „privatumo skydą“.

684 Europos Komisija, Komisijos ataskaita Europos Parlamentui ir Tarybai dėl pirmosios metinės ES ir JAV „privatumo skydo“ veikimo peržiūros, COM(2017) 611 *final*, 2017 m. spalio 18 d. Taip pat žr. 29 straipsnio darbo grupė, *ES ir JAV „privatumo skydo“ pirmoji metinė bendra peržiūra*, priimta 2017 m. lapkričio 28 d., 17/EN WP 255.

pasinaudoti veiksmingomis teisinėmis teisių gynimo priemonėmis[685]. Priimtinų „tinkamų apsaugos priemonių“ sąrašas pateikiamas tik ES duomenų apsaugos teisėje. Tinkamos apsaugos priemonės gali būti nustatytos:

- valdžios institucijų arba įstaigų tarpusavio dokumente, kuris yra teisiškai privalomas ir vykdytinas;
- įmonėms privalomose taisyklėse;
- Europos Komisijos arba priežiūros institucijos priimtose standartinėse duomenų apsaugos sąlygose;
- elgesio kodeksuose;
- sertifikavimo mechanizmais[686].

Pritaikytos ES duomenų valdytojo arba duomenų tvarkytojo ir duomenų gavėjo trečiojoje šalyje sutarčių sąlygos yra dar viena tinkamų apsaugos priemonių užtikrinimo priemonė. Tačiau tokias sutarčių sąlygas turi patvirtinti kompetentinga priežiūros institucija ir tik paskui jomis galima remtis kaip asmens duomenų perdavimo priemonėmis. Panašiai, valdžios institucijos gali pasinaudoti jų administracinėse taisyklėse įtvirtintomis duomenų apsaugos nuostatomis, jeigu jas patvirtino priežiūros institucija[687].

Pagal ET teisę duomenų judėjimas į valstybę arba tarptautinę organizaciją, kuri nėra atnaujintos 108-osios konvencijos susitariančioji šalis, leidžiamas, jeigu užtikrinamas tinkamas apsaugos lygis. Tai galima pasiekti:

- valstybės arba tarptautinės organizacijos teisėje arba
- numatant *ad hoc* arba standartizuotas apsaugos priemones teisiškai privalomame dokumente[688].

685 Bendrojo duomenų apsaugos reglamento 46 straipsnis.

686 Bendrojo duomenų apsaugos reglamento 46 straipsnio 1 dalies c ir d punktai, 2 dalies a, b, e, f punktai ir 47 straipsnis.

687 *Ten pat*, 46 straipsnio 3 dalis.

688 Atnaujintos 108-osios konvencijos 14 straipsnio 3 dalies b punktas.

Duomenų perdavimas, kuriam taikomos sutarčių sąlygos

ET ir **ES teisėje** pripažįstama, kad sutarčių sąlygos, kurias taiko duomenis eksportuojantis duomenų valdytojas ir gavėjas trečiojoje šalyje, yra būdas, galintis padėti užtikrinti pakankamą duomenų apsaugos lygį gavėjo atžvilgiu[689].

ES lygmeniu Europos Komisija, padedama 29 straipsnio darbo grupės, parengė standartines duomenų apsaugos sąlygas, kurios buvo oficialiai patvirtintos Komisijos sprendimu, kuriuo įrodoma tinkama duomenų apsauga[690]. Kadangi Komisijos sprendimai valstybėse narėse yra privalomi visa apimtimi, duomenų perdavimo priežiūrą vykdančios nacionalinės institucijos savo procedūrose turi pripažinti šias standartines sutarčių sąlygas[691]. Todėl jeigu duomenis teikiantis duomenų valdytojas ir trečioji valstybė duomenų gavėja sutinka su šiomis sąlygomis ir jas pasirašo, tokia aplinkybė priežiūros institucijai turėtų būti pakankamas įrodymas, kad tinkamos apsaugos priemonės yra nustatytos. Vis dėlto *Schrems* byloje ESTT nusprendė, kad Europos Komisija neturi kompetencijos apriboti nacionalinių priežiūros institucijų įgaliojimų prižiūrėti asmens duomenų perdavimo į trečiąją šalį, kuriai taikomas Komisijos sprendimas dėl tinkamumo[692]. Taigi nacionalinėms priežiūros institucijoms neužkertamas kelias naudotis savo įgaliojimais, įskaitant įgaliojimą sustabdyti arba uždrausti asmens duomenų perdavimą, kai duomenys perduodami pažeidžiant ES arba nacionalinę duomenų apsaugos teisę, pavyzdžiui, kai duomenų importuotojas nesilaiko standartinių sutarčių sąlygų[693].

Standartinės duomenų apsaugos sąlygos ES teisinėje sistemoje neužkerta kelio duomenų valdytojams suformuluoti kitų *ad hoc* individualių sutarčių sąlygų, jeigu jas patvirtino priežiūros institucija[694]. Tačiau jomis turi būti užtikrinamas toks pat apsaugos lygis, koks numatytas standartinėse duomenų apsaugos sąlygose. Reikalaujama, kad, patvirtindamos *ad hoc* sąlygas, priežiūros institucijos taikytų nuoseklumo

689 Bendrojo duomenų apsaugos reglamento 46 straipsnio 3 dalis; atnaujintos 108-osios konvencijos 14 straipsnio 3 dalies b punktas.

690 *Ten pat*, 46 straipsnio 2 dalies b punktas ir 46 straipsnio 5 dalis.

691 *Ten pat*, 46 straipsnio 2 dalies c punktas.; Sutarties dėl Europos Sąjungos veikimo 288 straipsnis.

692 ESTT, C-362/14, *Maximilian Schrems prieš Data Protection Commissioner* (DK), 2015 m. spalio 6 d., 96–98 ir 102–105 punktai.

693 Siekdama atsižvelgti į ESTT poziciją *Schrems* byloje, Komisija iš dalies pakeitė savo sprendimą dėl standartinių sutarčių sąlygų. 2016 m. gruodžio 16 d. Komisijos įgyvendinimo sprendimas (ES) 2016/2297, kuriuo iš dalies keičiami sprendimai 2001/497/EB ir 2010/87/ES dėl sutarčių standartinių sąlygų, nustatytų asmens duomenų perdavimui trečiosioms šalims ir tokiose šalyse įsikūrusiems tvarkytojams pagal Europos Parlamento ir Tarybos direktyvos 95/46/EB nuostatas, OL L344, 2016.

694 Bendrojo duomenų apsaugos reglamento 46 straipsnio 3 dalies a punktas.

užtikrinimo mechanizmą ir taip užtikrintų vienodą reguliavimo požiūrį visoje ES[695]. Tai reiškia, kad kompetentinga priežiūros institucija privalo perduoti savo sprendimo dėl sąlygų projektą EDAV. EDAV šiuo klausimu priima nuomonę, o priežiūros institucija, priimdama savo sprendimą, privalo visapusiškai atsižvelgti į šią nuomonę. Jeigu ji neketina vadovautis EDAV nuomone, EDAV taiko ginčų sprendimo mechanizmą ir priima privalomą sprendimą[696].

Svarbiausi standartinių sutarčių sąlygų ypatumai:

- trečiosios šalies labui nustatyta sąlyga, kuri sudaro sąlygas duomenų subjektams įgyvendinti sutartyje nustatytas teises, net jeigu ji nėra sutarties šalis;

- duomenų gavėjas ar importuotojas sutinka kilus ginčui paisyti duomenis eksportuojančio duomenų valdytojo nacionalinės priežiūros institucijos ir (arba) teismų kompetencijos.

Šiuo metu duomenų valdytojui perduodant duomenis kitam duomenų valdytojui galima taikyti du standartinių sąlygų rinkinius, iš kurių duomenis eksportuojantis duomenų valdytojas gali pasirinkti[697]. Jei duomenis duomenų valdytojas perduoda duomenų tvarkytojui, galioja tik vienas standartinių sutarčių sąlygų rinkinys[698]. Tačiau dėl šių standartinių sutarčių sąlygų šiuo metu vyksta teismo procesas.

Pavyzdys. ESTT paskelbus „saugaus uosto“ sprendimą negaliojančiu[699], asmens duomenų perdavimo į JAV nebebuvo galima grįsti tuo sprendimu dėl tinkamumo. Nors derybos su JAV institucijomis tebevyko ir turėjo būti priimtas naujas sprendimas dėl tinkamumo (jis galiausiai buvo priimtas

695 *Ten pat*, 63 straipsnis ir 64 straipsnio 1 dalies e punktas.

696 *Ten pat*, 64 ir 65 straipsniai.

697 I rinkinys pateiktas Europos Komisijos priede (2001 m.), 2001 m. birželio 15 d. Komisijos sprendime 2001/497/EB dėl sutarčių standartinių punktų, taikomų asmens duomenų perdavimui trečiosioms šalims pagal Direktyvą 95/46/EB, OL L 181, 2001; II rinkinys pateiktas Europos Komisijos priede (2004 m.), 2004 m. gruodžio 27 d. Komisijos sprendimas 2004/915/EB, iš dalies keičiantis Sprendimą 2001/497/EB dėl sutarčių standartinių sąlygų, taikomų asmens duomenų perdavimui trečiosioms šalims, nustatymo, OL L 385, 2004.

698 Europos Komisija (2010 m.), 2010 m. vasario 5 d. Komisijos sprendimas 2010/87 dėl sutarčių standartinių sąlygų, nustatytų asmens duomenų perdavimui trečiosiose šalyse įsikūrusiems tvarkytojams pagal Europos Parlamento ir Tarybos direktyvos 95/46/EB nuostatas, OL L 39, 2010. Rengiant šį vadovą, dėl standartinių sutarčių sąlygų, kuriomis remiantis asmens duomenys perduodami JAV, Airijos aukštajame teisme vyko teisminis procesas.

699 ESTT, C-362/14, *Maximillian Schrems prieš Data Protection Commissioner* (DK), 2015 m. spalio 6 d.

2016 m. liepos 12 d.)[700], duomenis buvo galima perduoti remiantis tik kitais teisiniais pagrindais, pavyzdžiui, standartinėmis sutarčių sąlygomis arba įmonėms privalomomis taisyklėmis. Keletas bendrovių, įskaitant *Facebook Ireland* (kuriai buvo iškelta byla, kurioje „saugaus uosto" sprendimas buvo pripažintas negaliojančiu), nusprendė taikyti standartines sutarčių sąlygas, kad toliau perduotų duomenis tarp JAV ir ES.

M. Schrems pateikė skundą Airijos priežiūros institucijai prašydamas jos sustabdyti standartinėmis sutarčių sąlygomis grindžiamą duomenų perdavimą į JAV. Iš esmės jis teigė, kad tais atvejais, kai duomenys iš *Facebook* Airijos patronuojamosios bendrovės perduodami į *Facebook Inc.* ir JAV esančius serverius, nėra jokios garantijos, kad duomenys bus apsaugoti. *Facebook Inc.* yra saistoma JAV įstatymų, kuriais ji galėtų būti įpareigota atskleisti asmens duomenis JAV teisėsaugos institucijoms, ir europiečiai negali pasinaudoti jokiomis teisminių teisių gynimo priemonėmis, kuriomis galėtų ginčyti tokią praktiką[701]. Todėl ESTT padarė išvadą, kad „saugaus uosto" sprendimas negaliojo ir nors ESTT savo sprendime nagrinėjo tik tą sprendimą, pareiškėjas manė, kad iškelti klausimai yra svarbūs tais atvejais, kai duomenų perdavimas grindžiamas sutarčių sąlygomis. Rengiant šį vadovą, byla buvo nagrinėjama Airijos aukštajame teisme. Akivaizdu, kad pareiškėjas ketina perduoti bylą ESTT, nes jis siekia ginčyti Europos Komisijos sprendimo dėl standartinių sutarčių sąlygų galiojimą. Kaip aprašyta 5 skyriuje, tik ESTT turi kompetenciją paskelbti ES priemonę negaliojančia.

Duomenų perdavimas laikantis įmonėms privalomų taisyklių

Pagal **ES teisę** asmens duomenų perdavimą, kuris grindžiamas įmonėms privalomomis taisyklėmis, susijusiomis su tarptautiniu duomenų perdavimu, taip pat galima atlikti įmonių arba bendrovių, kurios vykdo bendrą ekonominę veiklą, grupėje[702]. Įmonėms privalomos taisyklės, kaip asmens duomenų perdavimo priemonė, gali būti taikoma po to, kai kompetentinga priežiūros institucija jas patvirtina laikydamasi įmonėms privalomų taisyklių ir naudodama nuoseklumo užtikrinimo mechanizmą.

700 2016 m. liepos 12 d. Komisijos įgyvendinimo sprendimas (ES) 2016/1250 dėl ES ir JAV „privatumo skydo" užtikrinamos apsaugos tinkamumo pagal Europos Parlamento ir Tarybos direktyvą 95/46/EB, OL L 207.

701 Daugiau informacijos žr. peržiūrėtą skundą dėl *Facebook Ireland Ltd* bendrovės, kurį Airijos duomenų apsaugos komisarui 2015 m. gruodžio 1 d. pateikė Maximilian Schrems.

702 Bendrojo duomenų apsaugos reglamento 47 straipsnis.

Kad būtų galima patvirtinti įmonėms privalomas taisykles, jos turi būti teisiškai privalomos, apimti visus esminius duomenų apsaugos principus ir jas turi taikyti ir jų vykdymą užtikrinti kiekvienas grupės narys. Jomis turi būti aiškiai suteikiamos įgyvendinamos teisės duomenų subjektams, jos turi apimti visus esminius duomenų apsaugos principus ir atitikti tam tikrus formalius reikalavimus, pavyzdžiui, turi būti nurodoma įmonės struktūra, aprašomas duomenų perdavimas ir kaip bus taikomi duomenų apsaugos principai. Tai apima tokios informacijos suteikimą duomenų subjektams. Įmonėms privalomose taisyklėse, be kita ko, būtina nurodyti duomenų subjektų teises ir nuostatas dėl atsakomybės už bet kokius taisyklių pažeidimus[703]. Tvirtinant įmonėms privalomas taisykles, bus taikomas priežiūros institucijų bendradarbiavimo nuoseklumo užtikrinimo mechanizmas (aprašytas 5 skyriuje).

Taikant nuoseklumo užtikrinimo mechanizmą, vadovaujančioji priežiūros institucija peržiūri siūlomas įmonėms privalomas taisykles, priima sprendimo projektą ir perduoda jį EDAV. Valdyba šiuo klausimu priima nuomonę, o vadovaujančioji priežiūros institucija gali oficialiai patvirtinti įmonėms privalomas taisykles, kartu visapusiškai atsižvelgdama į Valdybos nuomonę. Ši nuomonė nėra teisiškai privaloma, tačiau jeigu priežiūros institucija ketina nepaisyti nuomonės, tuomet bus taikomas ginčų sprendimo mechanizmas ir Valdybos bus prašoma dviejų trečdalių jos narių balsų dauguma priimti teisiškai privalomą sprendimą[704].

Pagal **ET teisę** *ad hoc* arba standartizuotos apsaugos priemonės, kurios yra numatytos teisiškai privalomame dokumente[705], taip pat apima įmonėms privalomas taisykles.

7.3.3. Konkrečiais atvejais nukrypti leidžiančios nuostatos

Pagal ES teisę asmens duomenų perdavimas į trečiąją šalį gali būti pateisinamas net ir nesant sprendimo dėl tinkamumo arba apsaugos priemonių, pavyzdžiui, standartinių sutarčių sąlygų arba įmonėms privalomų taisyklių, bet kuriomis iš toliau nurodytų aplinkybių:

- duomenų subjektas duoda aiškų sutikimą, kad duomenys būtų tvarkomi;

703 Išsamesnis aprašymas pateikiamas Bendrojo duomenų apsaugos reglamento 47 straipsnyje.

704 *Ten pat*, 57 straipsnio 1 dalies s punktas, 58 straipsnio 1 dalies j punktas, 64 straipsnio 1 dalies f punktas, 65 straipsnio 1 ir 2 dalys.

705 Atnaujintos 108-osios konvencijos 14 straipsnio 3 dalies b punktas.

- duomenų subjektas sudaro arba rengiasi sudaryti sutartį, pagal kurią duomenis būtina perduoti į užsienį;
- siekiant sudaryti duomenų valdytojo ir trečiosios šalies sutartį duomenų subjekto labui;
- atsižvelgiant į svarbias viešojo intereso priežastis;
- siekiant nustatyti, įgyvendinti arba apginti teisinius reikalavimus;
- siekiant apsaugoti duomenų subjekto gyvybinius interesus;
- siekiant perduoti duomenis iš viešųjų registrų (tai yra vienas svarbiausių plačiosios visuomenės interesų turėti prieigą prie viešuosiuose registruose saugomos informacijos)[706].

Kai nė viena iš šių sąlygų netaikoma ir kai duomenų perdavimas negali būti grindžiamas sprendimu dėl tinkamumo arba tinkamomis apsaugos priemonėmis, duomenų perdavimas gali būti vykdomas tik tuo atveju, kai jis nėra pasikartojantis, susijęs su ribotu duomenų subjektų skaičiumi ir yra būtinas duomenų valdytojo įtikinamų teisėtų interesų tikslais, su sąlyga, kad duomenų subjekto teisės nėra viršesnės už šias teises[707]. Šiais atvejais duomenų valdytojas privalo įvertinti su duomenų perdavimu susijusias aplinkybes ir numatyti apsaugos priemones. Jis taip pat privalo informuoti priežiūros instituciją ir duomenų subjektus apie duomenų perdavimą ir jį pateisinantį teisėtą interesą.

Faktas, kad nukrypti leidžiančios nuostatos yra kraštutinė teisėto perdavimo priemonė[708] (jos turi būti taikomos tik tuo atveju, jei nepriimtas sprendimas dėl tinkamumo ir jei nėra jokių kitų apsaugos priemonių), išryškina jų išimtinį pobūdį, kuris dar kartą akcentuojamas BDAR konstatuojamosiose dalyse[709]. Todėl nukrypti leidžiančios nuostatos yra priimtinos kaip galimybė „duomenis perduoti tam tikromis aplinkybėmis“ ir kai „duomenų perdavimas atliekamas nereguliariai“[710] atsižvelgiant į sutartį arba teisinį reikalavimą.

706 Bendrojo duomenų apsaugos reglamento 49 straipsnis.

707 *Ten pat*.

708 *Ten pat*, 49 straipsnio 1 dalis.

709 Žr. Bendrojo duomenų apsaugos reglamento 49 straipsnio 1 dalies a, b ir e punktus ir 113 konstatuojamąją dalį.

710 *Ten pat*, 49 straipsnio 1 dalis.

Be to, pagal 29 straipsnio darbo grupės rekomendacijas konkrečiose situacijose nukrypti leidžiančių nuostatų taikymas turi būti išimtinis, pagrįstas individualiais atvejais ir negali būti naudojamas masiniam arba pasikartojančiam duomenų perdavimui[711]. Europos duomenų apsaugos priežiūros pareigūnas taip pat pabrėžė išimtinį nukrypti leidžiančių nuostatų, kurios naudojamos kaip duomenų perdavimo pagal Reglamentą (EB) Nr. 45/2001 teisinis pagrindas, pobūdį ir pažymėjo, kad šis sprendimas turėtų būti naudojamas „tik tam tikrais atvejais" ir „retkarčiais perduodant duomenis"[712].

Pavyzdys. Pasaulinės paskirstymo sistemos (GDS) paslaugų bendrovė, kurios būstinė yra JAV, teikia internetinę rezervavimo sistemą įvairioms oro transporto bendrovėms, viešbučiams ir kruizams visame pasaulyje, tvarko dešimčių milijonų ES gyventojų duomenis. GDS bendrovė, iš pradžių perduodama duomenis į savo serverius JAV, remiasi nukrypti leidžiančia nuostata kaip teisėtu perdavimo pagrindu, t. y. būtinybe sudaryti sutartį. Taigi ji nenustato jokių kitų apsaugos priemonių, susijusių su asmens duomenimis, kilusiais iš Europos, perduotais JAV ir vėliau perplatintais į viešbučius visame pasaulyje (t. y. jokių apsaugos priemonių tolesniam perdavimui). GDS bendrovė nesilaiko Bendrojo duomenų apsaugos reglamento reikalavimų dėl teisėto tarptautinio duomenų perdavimo, nes ji remiasi nukrypti leidžiančia nuostata kaip teisėta masinio duomenų perdavimo priežastimi.

Išskyrus atvejus, kai priimtas sprendimas dėl tinkamumo, ES arba jos valstybės narės dėl svarbių viešojo intereso priežasčių yra įgaliotos nustatyti konkrečių kategorijų asmens duomenų perdavimo į trečiąją šalį ribas, nepaisant to, kad tenkinamos kitos tokio perdavimo sąlygos. Šie apribojimai turėtų būti suvokiami kaip išimtiniai, ir valstybės narės turi pranešti Komisijai apie atitinkamas nuostatas[713].

Pagal **ET teisę** duomenis leidžiama perduoti į teritorijas, kuriose neužtikrinama tinkama duomenų apsauga, tais atvejais, kai:

- duomenų subjektas davė sutikimą;

711 29 straipsnio darbo grupė (2005 m.), *Darbo dokumentas dėl 1995 m. spalio 24 d. Direktyvos 95/46/EB 26 straipsnio 1 dalies vienodo aiškinimo*, WP 114, Briuselis, 2005 m. lapkričio 25 d.

712 Europos duomenų apsaugos priežiūros pareigūnas, *Asmens duomenų perdavimas trečiosioms šalims ir tarptautinėms organizacijoms, kurį vykdo ES institucijos ir įstaigos*, poziciją nusakantis dokumentas, Briuselis, 2014 m. liepos 14 d., p. 15.

713 Žr. Bendrojo duomenų apsaugos reglamento 49 straipsnio 5 dalį.

- toks duomenų perdavimas yra reikalingas atsižvelgiant į duomenų subjekto interesus;

- esama įstatyme nustatytų viršesnių teisėtų interesų, visų pirma svarbių viešųjų interesų;

- toks perdavimas reiškia būtiną ir proporcingą priemonę demokratinėje visuomenėje[714].

7.3.4. Duomenų perdavimas pagal tarptautinius susitarimus

ES gali sudaryti tarptautinius susitarimus su trečiosiomis šalimis, kuriais reglamentuojamas asmens duomenų perdavimas konkrečiais tikslais. Šiuose susitarimuose turi būti numatytos tinkamos apsaugos priemonės atitinkamų asmenų asmens duomenų apsaugai užtikrinti. BDAR taikomas nedarant poveikio šiems tarptautiniams susitarimams[715].

Valstybės narės taip pat gali sudaryti tarptautinius susitarimus su trečiosiomis šalimis arba tarptautinėmis organizacijomis, kuriais užtikrinamas tinkamas asmenų pagrindinių teisių ir laisvių apsaugos lygis, jei tie susitarimai nedaro poveikio BDAR taikymui.

Panaši taisyklė nustatyta atnaujintos 108-osios konvencijos 12 straipsnio 3 dalies a punkte.

Tarptautinių susitarimų, susijusių su asmens duomenų perdavimu, pavyzdžiai yra susitarimai dėl keleivio duomenų įrašų (PNR).

Keleivio duomenų įrašai

PNR duomenis, įskaitant, be kita ko, oro keleivių vardus, pavardes, adresus, kredito kortelių duomenis ir vietų numerius, renka oro vežėjai skrydžio užsakymo metu. Oro vežėjai šią informaciją renka ir savo komerciniais tikslais. ES su tam tikromis trečiosiomis šalimis (Australija, Kanada ir JAV) sudarė susitarimus dėl PNR duomenų perdavimo teroristinių nusikaltimų ar sunkių tarpvalstybinių nusikaltimų prevencijos,

714 Atnaujintos 108-osios konvencijos 14 straipsnio 4 dalis.

715 Bendrojo duomenų apsaugos reglamento 102 konstatuojamoji dalis.

nustatymo, tyrimo ir patraukimo už juos baudžiamojon atsakomybėn tikslais. Be to, 2016 m. Sąjunga priėmė Direktyvą (ES) 2016/861, kuri dar žinoma kaip ES PNR direktyva[716]. Šioje direktyvoje nustatyta ES valstybių narių atliekamo PNR duomenų perdavimo kitų trečiųjų šalių kompetentingoms institucijoms tvarka, kuria taip pat siekiama užkirsti kelią teroristiniams nusikaltimams ir sunkiems nusikaltimams, juos nustatyti, tirti ar patraukti už juos baudžiamojon atsakomybėn. PNR duomenų perdavimas trečiosios šalies institucijoms vykdomas kiekvienu konkrečiu atveju, kartu atskirai įvertinant, ar duomenis perduoti būtina direktyvoje nurodytais tikslais ir ar perduodant duomenis laikomasi pagrindinių teisių.

Kalbant apie ES ir trečiųjų šalių PNR susitarimus, pažymėtina, kad jų suderinamumas su pagrindinėmis teisėmis į privatumą ir ES pagrindinių teisių chartijoje numatyta duomenų apsauga buvo ginčijamas. Kai po derybų su Kanada 2014 m. ES pasirašė susitarimą dėl PNR duomenų perdavimo ir tvarkymo, Europos Parlamentas nusprendė perduoti šį klausimą ESTT, kad šis įvertintų susitarimo teisėtumą pagal ES teisę, visų pirma Chartijos 7 ir 8 straipsnius.

Pavyzdys. Savo nuomonėje dėl ES ir Kanados PNR susitarimo[717] ESTT nusprendė, kad, atsižvelgiant į dabartinę jo formą, numatytas susitarimas buvo nesuderinamas su Chartijoje pripažįstamomis pagrindinėmis teisėmis, todėl jo nebuvo galima sudaryti. Kadangi susitarimas buvo susijęs su asmens duomenų tvarkymu, juo buvo ribojama teisė į asmens duomenų apsaugą, kuri užtikrinama pagal Chartijos 8 straipsnį. Kartu susitarimu taip pat apribota teisė į privatų gyvenimą, numatyta 7 straipsnyje, atsižvelgiant į tai, kad apskritai PNR duomenys gali būti apibendrinami ir analizuojami taip, kad būtų atskleisti keliavimo įpročiai, įvairių asmenų santykiai, informacija apie jų finansinę padėtį, mitybos įpročius ir sveikatos būklę, taip kišantis į jų privatų gyvenimą.

Pagrindinių teisių apribojimu, kuris buvo nustatytas numatytuoju susitarimu, buvo siekiama bendrojo intereso tikslo, t. y. visuomenės saugumo ir kovos su terorizmu bei sunkiais tarpvalstybiniais nusikaltimais. Tačiau ESTT priminė, kad tam, jog būtų pateisinamas, apribojimas turi būti susijęs su tuo, kas yra griežtai būtina siekiamam tikslui pasiekti. Išanalizavęs susitarimo

716 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/681 dėl keleivio duomenų įrašo (PNR) duomenų naudojimo teroristinių nusikaltimų ir sunkių nusikaltimų prevencijos, nustatymo, tyrimo ir patraukimo už juos baudžiamojon atsakomybėn tikslais, OL L 119, 2016.

717 ESTT, *Teisingumo Teismo (didžioji kolegija) nuomonė 1/15*, 2017 m. liepos 26 d.

nuostatas, ESTT padarė išvadą, kad numatytasis susitarimas neatitiko „griežto būtinumo“ kriterijaus. Siekdamas prieiti prie tos išvados, ESTT, be kita ko, nagrinėjo toliau minimus veiksnius.

- Numatytojo susitarimo sąsajos su neskelbtinų duomenų perdavimu. Pagal numatytąjį susitarimą surinkti PNR galėjo apimti neskelbtinus duomenis, pavyzdžiui, keleivio rasinę arba etninę kilmę, religinius įsitikinimus arba sveikatos būklę atspindinčią informaciją. Kanados valdžios institucijų atliekamas neskelbtinų duomenų perdavimas ir tvarkymas galėtų kelti pavojų nediskriminavimo principui, todėl reikia tikslaus ir tvirto pateisinimo, grindžiamo ne tik visuomenės saugumu ir kova su sunkiais nusikaltimais, bet ir kitais motyvais. Numatytajame susitarime toks pagrindimas nebuvo pateiktas[718].

- Nuolatinis visų keleivių PNR duomenų saugojimas penkerių metų laikotarpį net ir po to, kai keleivis išvyko iš Kanados, taip pat buvo laikomas viršijančiu griežtai būtinas ribas. ESTT laikėsi nuomonės, kad Kanados valdžios institucijoms būtų leidžiama saugoti keleivių, kurie, remiantis objektyviais įrodymais, gali kelti grėsmę visuomenės saugumui, duomenis net ir tiems asmenims išvykus iš Kanados. Priešingai, *visų* keleivių, kurių atveju nėra net netiesioginių įrodymų, kad jie kelia pavojų visuomenės saugumui, asmens duomenų saugojimas nėra pateisinamas[719].

108-osios konvencijos konsultacinis komitetas pateikė nuomonę dėl PNR susitarimų poveikio duomenų apsaugai pagal ET teisę[720].

Pranešimų duomenys

Belgijoje įsikūrusi Pasaulinė tarpbankinių finansinių telekomunikacijų draugija (SWIFT), kuri yra daugumos pasaulinių pinigų pervedimų iš Europos bankų tvarkytoja, vykdė veiklą turėdama „veidrodinį“ centrą JAV ir gavo prašymą atskleisti

718 *Ten pat*, 165 punktas.

719 *Ten pat*, 204–207 punktai.

720 Europos Taryba, *Nuomonė dėl keleivio duomenų įrašų tvarkymo poveikio duomenų apsaugai*, T-PD(2016)18rev, 2016 m. rugpjūčio 19 d.

duomenis JAV iždo departamentui terorizmo tyrimo tikslais pagal terorizmo finansavimo sekimo programą[721].

Žvelgiant iš ES perspektyvos, nebuvo pakankamo teisinio pagrindo atskleisti šiuos duomenis, daugiausia apie ES piliečius, JAV vien dėl to, kad ten buvo įsikūręs vienas iš SWIFT duomenų tvarkymo centrų.

Siekiant suteikti būtiną teisinį pagrindą ir užtikrinti tinkamus duomenų apsaugos standartus, 2010 m. sudarytas specialus ES ir JAV susitarimas, vadinamas SWIFT susitarimu[722].

Pagal šį susitarimą SWIFT saugomi finansiniai duomenys toliau teikiami JAV iždo departamentui teroristinių nusikaltimų arba terorizmo finansavimo prevencijos, tyrimo, nustatymo ar patraukimo baudžiamojon atsakomybėn už juos tikslais. JAV iždo departamentas gali prašyti finansinių duomenų iš SWIFT, jeigu prašyme:

- kuo aiškiau nurodomi finansiniai duomenys;
- aiškiai pagrindžiama duomenų būtinybė;
- nurodomos kuo siauresnės formuluotės, kad būtų pateiktas kuo mažesnis prašomų duomenų kiekis;
- neprašoma pateikti kokių nors duomenų, susijusių su bendra mokėjimų eurais erdve (SEPA)[723].

Europolas privalo gauti kiekvieno JAV iždo departamento pateikto prašymo kopiją ir patikrinti, ar laikomasi SWIFT susitarimo principų[724]. Jei patvirtinama, kad prin-

721 Šiuo klausimu žr. 29 straipsnio darbo grupės (2011 m.) *Nuomonę Nr. 14/2011 dėl duomenų apsaugos klausimų, susijusių su pinigų plovimo ir teroristų finansavimo prevencija*, WP 186, Briuselis, 2011 m. birželio 13 d.; 29 straipsnio darbo grupės nuomonę (2006 m.), *Nuomonę Nr. 10/2006 dėl Pasaulinės tarpbankinių finansinių telekomunikacijų organizacijos (SWIFT) atliekamo asmens duomenų tvarkymo*, WP 128, Briuselis, 2006 m. lapkričio 22 d.; Belgijos privatumo apsaugos komisijos (*Commission de la protection de la vie privée*) (2008 m.) sprendimą *„Kontrolės ir rekomendacijų teikimo procedūra, pradėta dėl bendrovės SWIFT scrl“*, 2008 m. gruodžio 9 d.

722 2010 m. liepos 13 d. Tarybos sprendimas 2010/412/ES dėl Europos Sąjungos ir Jungtinių Amerikos Valstijų susitarimo dėl finansinių mokėjimų pranešimų duomenų tvarkymo ir perdavimo iš Europos Sąjungos į Jungtines Valstijas Terorizmo finansavimo sekimo programos tikslais sudarymo, OL L 195, 2010, p. 3 ir 4. Susitarimo tekstas pridedamas prie šio sprendimo, OL L 195, 2010, p. 5–14.

723 *Ten pat*, 4 straipsnio 2 dalis.

724 Europolo jungtinė priežiūros institucija atliko Europolo veiklos šioje srityje auditą.

cipų laikomasi, SWIFT privalo tiesiogiai JAV iždo departamentui pateikti finansinius duomenis. Departamentas privalo saugoti finansinius duomenis saugioje fizinėje aplinkoje, kurioje su jais gali susipažinti tik teroristinius nusikaltimus arba terorizmo finansavimą tiriantys analitikai, ir finansiniai duomenys negali būti susiejami su kuria nors kita duomenų baze. Apskritai iš SWIFT gauti finansiniai duomenys turi būti ištrinti ne vėliau kaip per penkerius metus nuo jų gavimo. Finansiniai duomenys, susiję su konkrečiais tyrimais ar baudžiamuoju persekiojimu, gali būti saugomi tik tol, kol duomenys yra būtini šiems tyrimams ar baudžiamajam persekiojimui.

JAV iždo departamentas gali perduoti informaciją iš SWIFT gautų duomenų konkrečioms teisėsaugos, visuomenės saugumo ar kovos su terorizmu institucijoms JAV ar už jos ribų tik terorizmo ir jo finansavimo tyrimo, nustatymo, prevencijos ar baudžiamojo persekiojimo už juos tikslais. Jeigu tolesnis finansinių duomenų perdavimas yra susijęs su ES valstybės narės piliečiu arba gyventoju, bet kokiam dalijimuisi duomenimis su trečiosios valstybės institucijomis būtinas išankstinis atitinkamos valstybės narės institucijų sutikimas. Išimtys gali būti numatomos tais atvejais, kai dalytis duomenimis labai svarbu siekiant išvengti staigaus ir didelio pavojaus visuomenės saugumui.

Nepriklausomi prižiūrėtojai, įskaitant Europos Komisijos paskirtą asmenį, stebi, kaip laikomasi SWIFT susitarimo principų. Jie turi galimybę tikruoju laiku ir atgaline data peržiūrėti visas atliktas pateiktų duomenų paieškas, prašyti papildomos informacijos, kad būtų galima pagrįsti šių paieškų ryšį su terorizmu, ir teisę blokuoti bet kokią arba visas paieškas, kuriomis, atrodo, pažeidžiamos susitarime nustatytos apsaugos priemonės.

Duomenų subjektai turi teisę gauti kompetentingos ES priežiūros institucijos patvirtinimą, kad jų asmens duomenų apsaugos teisių buvo laikomasi. Duomenų subjektai taip pat turi teisę reikalauti, kad jų duomenys, kuriuos pagal SWIFT susitarimą surinko ir saugojo JAV iždo departamentas, būtų ištaisyti, ištrinti arba užblokuoti. Tačiau duomenų subjektų teisėms susipažinti su duomenimis gali būti taikomi tam tikri teisiniai apribojimai. Jei atsisakoma suteikti prieigą, duomenų subjektas turi būti raštu informuojamas apie atsisakymą suteikti prieigą ir apie jo teisę siekti administracinių ir teisminių teisių gynimo priemonių JAV.

SWIFT susitarimas galioja penkerius metus, pirmasis jo galiojimo laikotarpis truko iki 2015 m. rugpjūčio mėn. Jo galiojimas automatiškai pratęsiamas vieniems metams, išskyrus atvejus, kai viena susitariančioji šalis ne vėliau kaip prieš šešis mėnesius

praneša kitai šaliai apie ketinimą nepratęsti susitarimo galiojimo. Automatinis pratęsimas taikytas 2015, 2016 ir 2017 m. rugpjūčio mėn. taip užtikrinant, kad SWIFT susitarimas galiotų bent iki 2018 m. rugpjūčio mėn.[725]

725 *Ten pat*, 23 straipsnio 2 dalis.

8

Duomenų apsauga policijos ir baudžiamosios teisenos srityje

ES	Reglamentuojami klausimai	ET
Duomenų apsaugos policijos ir baudžiamosios teisenos institucijoms tvarkant asmens duomenis direktyva	**Bendri klausimai**	Atnaujinta 108-oji konvencija
	Policija	Rekomendacija dėl policijos Praktinis asmens duomenų naudojimo policijos sektoriuje vadovas
	Sekimas	EŽTT, *B. B. prieš Prancūziją*, Nr. 5335/06, 2009 m. EŽTT, *S. ir Marper prieš Jungtinę Karalystę* (DK), Nr. 30562/04 ir 30566/04, 2008 m. EŽTT, *Allan prieš Jungtinę Karalystę*, Nr. 48539/99, 2002 m. EŽTT, *Malone prieš Jungtinę Karalystę*, Nr. 8691/79, 1984 m. EŽTT, *Klass ir kiti prieš Vokietiją*, Nr. 5029/71, 1978 m. EŽTT, *Szabó ir Vissy prieš Vengriją*, Nr. 37138/14, 2016 m. EŽTT, *Vetter prieš Prancūziją*, Nr. 59842/00, 2005 m.
	Kibernetiniai nusikaltimai	Konvencija dėl elektroninių nusikaltimų

ES	Reglamentuojami klausimai	ET
Kiti konkretūs nacionalinės teisės aktai		
Priumo sprendimas	**Specialūs duomenys: pirštų atspaudai, DNR, chuliganizmas, informacija apie oro transporto keleivius, telekomunikacijų duomenys ir pan.**	Atnaujintos 108-osios konvencijos 6 straipsnis Rekomendacija dėl policijos, Praktinis asmens duomenų naudojimo policijos sektoriuje vadovas
Švedijos iniciatyva (Tarybos pamatinis sprendimas 2006/960/TVR)	**Keitimosi informacija ir žvalgybos duomenimis tarp teisėsaugos institucijų supaprastinimas**	EŽTT, *S. ir Marper prieš Jungtinę Karalystę* (DK), Nr. 30562/04 ir 30566/04, 2008 m.
Direktyva (ES) 2016/681 dėl keleivio duomenų įrašo (PNR) duomenų naudojimo teroristinių nusikaltimų ir sunkių nusikaltimų prevencijos, nustatymo, tyrimo ir patraukimo už juos baudžiamojon atsakomybėn tikslais ESTT, sujungtos bylos C-293/12 ir C-594/12, *Digital Rights Ireland* ir Kärntner Landesregierung ir kt. (DK), 2014 m. ESTT, sujungtos bylos C-203/15 ir C-698/15, *Tele2 Sverige* ir *Home Department prieš Tom Watson ir kt.* (DK), 2016 m.	**Asmens duomenų saugojimas**	EŽTT, *B. B. prieš Prancūziją*, Nr. 5335/06, 2009 m.
Europolo reglamentas Eurojusto sprendimas	**Duomenų apsauga specialiose agentūrose**	Rekomendacija dėl policijos
Šengeno II sprendimas VIS reglamentas EURODAC reglamentas MIS sprendimas	**Duomenų apsauga specialiose bendrose informacinėse sistemose**	Rekomendacija dėl policijos EŽTT, Dalea prieš Prancūziją, Nr. 964/07, 2010 m.

Siekdamos nustatyti su duomenų apsauga susijusių asmens interesų ir su duomenų rinkimu, siekiant kovoti su nusikalstamumu ir užtikrinti nacionalinį ir visuomenės saugumą, susijusių visuomenės interesų pusiausvyrą, ET ir ES nustatė specialias teisines priemones. Šiame skirsnyje pateikiama ET (8.1 skirsnis) ir ES teisės (8.2

skirsnis) apžvalga atsižvelgiant į duomenų apsaugą policijos ir baudžiamosios teisenos bylose.

8.1. ET teisė dėl duomenų apsaugos ir nacionalinio saugumo, policijos ir baudžiamosios teisenos bylose

Pagrindiniai faktai

- Atnaujinta 108-oji konvencija ir ET rekomendacija dėl policijos taikomos duomenų apsaugai visose policijos veiklos srityse.
- Konvencija dėl elektroninių nusikaltimų (Budapešto konvencija) yra privalomas tarptautinis teisinis dokumentas, kuriame aptariami prieš elektroninius tinklus ir per juos padaryti nusikaltimai. Jis taip pat svarbus tiriant ne elektroninio pobūdžio nusikaltimus, kuriuos nagrinėjant pateikiami elektroniniai įrodymai.

Vienas svarbus skirtumas tarp ET ir ES teisės yra tas, kad kitaip nei ES teisė, **ET teisė** taip pat taikoma nacionalinio saugumo sričiai. Tai reiškia, kad susitariančiosios šalys privalo toliau laikytis EŽTK 8 straipsnio, net jei tai apima veiklą, susijusią su nacionaliniu saugumu. Keletas EŽTT sprendimų yra susiję su valstybės veikla opiose nacionalinio saugumo teisės ir praktikos srityse[726].

Kalbant apie policiją ir baudžiamąją teiseną, pažymėtina, kad Europos lygmeniu atnaujinta 108-oji konvencija apima visas asmens duomenų tvarkymo sritis, o jos nuostatomis siekiama apskritai reglamentuoti asmens duomenų tvarkymą. Todėl atnaujinta 108-oji konvencija taikoma duomenų apsaugai policijos ir baudžiamosios teisenos srityje. Genetinių duomenų, asmens duomenų, susijusių su nusikalstamomis veikomis, baudžiamosiomis bylomis ir apkaltinamaisiais nuosprendžiais, ir visų susijusių saugumo priemonių, biometrinių duomenų, kuriais konkrečiai nustatoma asmens tapatybė, taip pat neskelbtinų asmens duomenų tvarkymas leidžiamas tik tais atvejais, kai taikomos tinkamos apsaugos priemonės nuo rizikos, kurią tokių

726 Žr., pvz., EŽTT, *Klass ir kiti prieš Vokietiją*, Nr. 5029/71, 1978 m. rugsėjo 6 d.; EŽTT, *Rotaru prieš Rumuniją* (DK), Nr. 28341/95, 2000 m. gegužės 4 d., ir EŽTT, *Szabó ir Vissy prieš Vengriją*, Nr. 37138/14, 2016 m. sausio 12 d.

duomenų tvarkymas gali kelti duomenų subjekto interesams, teisėms ir pagrindinėms laisvėms; visų pirma tai pasakytina apie diskriminacijos riziką[727].

Policijos ir baudžiamosios teisenos institucijų teisinėms užduotims vykdyti dažnai reikia tvarkyti asmens duomenis, o tai gali turėti rimtų pasekmių atitinkamiems asmenims. 1987 m. ET priimtoje Rekomendacijoje dėl policijos ET valstybėms narėms pateikiamos rekomendacijos, kaip jos turėtų įgyvendinti 108-osios konvencijos principus policijos institucijoms tvarkant asmens duomenis[728]. Rekomendacija buvo papildyta praktiniu vadovu dėl asmens duomenų naudojimo policijos sektoriuje, kurį priėmė 108-osios konvencijos konsultacinis komitetas[729].

Pavyzdys. Byloje *D. L. prieš Bulgariją*[730] socialinės tarnybos remdamosi teismo nutartimi įkurdino pareiškėją uždaroje švietimo įstaigoje. Visą susirašinėjimą ir pokalbius telefonu institucija stebėjo visa apimtimi ir be atrankos. EŽTT nusprendė, kad 8 straipsnis buvo pažeistas, nes nagrinėjama priemonė nebuvo būtina demokratinėje visuomenėje. Teisingumo Teismas nurodė, jog reikia padaryti viską, kad institucijoje apgyvendinti nepilnamečiai turėtų pakankamai ryšių su išoriniu pasauliu, nes tai yra neatsiejama jų teisės į orumą dalis ir yra būtina siekiant pasirengti jų reintegracijai į visuomenę. Tai pasakytina tiek apie vizitus, tiek apie susirašinėjimą ar pokalbius telefonu. Be to, vykdant stebėjimą nebuvo daromas skirtumas tarp bendravimo su šeimos nariais ir NVO, atstovaujančių vaikų teisėms, ar advokatų. Be to, sprendimas perimti pranešimą nebuvo pagrįstas individualia rizikos analize kiekvienu konkrečiu atveju.

Pavyzdys. Byloje *Dragojević prieš Kroatiją*[731] buvo įtariama, kad pareiškėjas užsiima neteisėta prekyba narkotikais. Jis buvo pripažintas kaltu po to, kai ikiteisminio tyrimo teisėjas leido naudoti slaptas sekimo priemones, kad perimtų pareiškėjo telefono skambučius. EŽTT nusprendė, kad priemonė, dėl kurios pateiktas skundas, yra teisės į privatų gyvenimą ir susirašinėjimą apribojimas. Tyrimą atliekančio teisėjo leidimas buvo pagrįstas tik baudžiamojo

727 Atnaujintos 108-osios konvencijos 6 straipsnis.

728 Europos Taryba, Ministrų komitetas (1987 m.), Rekomendacija *Rec(87)15* valstybėms narėms, reglamentuojanti asmens duomenų naudojimą policijos sektoriuje, 1987 m. rugsėjo 17 d.

729 Europos Taryba (2018 m.), 108-osios konvencijos konsultacinis komitetas, Praktinis asmens duomenų naudojimo policijos sektoriuje vadovas, T-PD(2018)1.

730 EŽTT, *D. L. prieš Bulgariją*, Nr. 7472/14, 2016 m. gegužės 19 d.

731 EŽTT, *Dragojević prieš Kroatiją*, Nr. 68955/11, 2015 m. sausio 15 d.

persekiojimo institucijos pareiškimu, kad „tyrimo negalima atlikti kitomis priemonėmis“. EŽTT taip pat pažymėjo, kad baudžiamieji teismai apribojo savo vertinimą dėl stebėjimo priemonių naudojimo ir kad vyriausybė nenurodė galimų teisių gynimo priemonių. Todėl 8 straipsnis buvo pažeistas.

8.1.1. Rekomendacija dėl policijos

EŽTT ne kartą konstatavo, kad policijos ar nacionalinio saugumo institucijų laikomi asmens duomenys reiškia EŽTK 8 straipsnio 1 dalies apribojimą. Daugumoje EŽTT sprendimų nagrinėjamas tokio apribojimo pagrįstumas[732].

Pavyzdys. Byloje *B. B. prieš Prancūziją*[733] pareiškėjas buvo nuteistas už seksualinius nusikaltimus prieš 15 metų nepilnamečius, kuriuos padarė pasinaudodamas jų pasitikėjimu. 2000 m. jis baigė atlikti laisvės atėmimo bausmę. Po metų jis paprašė išbraukti šią bausmę iš nuosprendžių registro, tačiau prašymas buvo atmestas. 2004 m. Prancūzijos įstatymu buvo sukurta nacionalinė teismo duomenų apie seksualinius nusikaltimus padariusius asmenis bazė ir pareiškėjas buvo informuotas, kad yra įtrauktas į šią duomenų bazę. EŽTT nusprendė, kad nuteisto seksualinio nusikaltėlio įtraukimas į nacionalinę teismų duomenų bazę patenka į EŽTK 8 straipsnio taikymo sritį. Tačiau, atsižvelgiant į tai, kad įgyvendintos pakankamos duomenų apsaugos priemonės, pavyzdžiui, duomenų subjekto teisė prašyti ištrinti duomenis, ribotas duomenų saugojimo laikas ir apribota galimybė susipažinti su tokiais duomenimis, tarp nagrinėjamų konkuruojančių privačiųjų ir viešųjų interesų buvo nustatyta tinkama pusiausvyra. EŽTT padarė išvadą, kad EŽTK 8 straipsnis nebuvo pažeistas.

Pavyzdys. Byloje *S. ir Marper prieš Jungtinę Karalystę*[734] abiem pareiškėjams pateikti kaltinimai dėl nusikalstamų veikų, tačiau jie nebuvo už jas nuteisti. Vis dėlto, policija laikė ir saugojo jų pirštų atspaudus, ląstelių mėginius ir DNR profilius. Neribotas minėtų biometrinių duomenų saugojimas buvo leidžiamas pagal įstatymą, kai asmuo buvo įtariamas padaręs nusikalstamą

732 Žr., pvz., EŽTT, *Leander prieš Švediją*, Nr. 9248/81, 1987 m. kovo 26 d.; EŽTT, *M. M. prieš Jungtinę Karalystę*, Nr. 24029/07, 2012 m. lapkričio 13 d.; EŽTT, *M. K. prieš Prancūziją*, Nr. 19522/09, 2013 m. balandžio 18 d., arba EŽTT, *Aycaguer prieš Prancūziją*, Nr. 8806/12, 2017 m. birželio 22 d.

733 EŽTT, *B. B. prieš Prancūziją*, Nr. 5335/06, 2009 m. gruodžio 17 d.

734 EŽTT, *S. ir Marper prieš Jungtinę Karalystę* (DK), Nr. 30562/04 ir 30566/04, 2008 m. gruodžio 4 d., 119 ir 125 punktai.

veiką, net jei įtariamasis vėliau buvo išteisintas arba pripažintas kaltu. EŽTT nusprendė, kad visa apimantis ir nediferencijuotas asmens duomenų saugojimas, kurio terminas nebuvo nustatytas, kai išteisinti asmenys turėjo tik ribotas galimybes prašyti ištrinti duomenis, reiškė neproporcingą pareiškėjo teisės į privatų gyvenimą apribojimą. Teismas padarė išvadą, kad buvo pažeistas EŽTK 8 straipsnis.

Elektroninių ryšių srityje itin svarbus klausimas yra valdžios institucijų kišimasis į teisę į privatumą ir duomenų apsaugą. Ryšio sekimo ar perėmimo priemonės, pavyzdžiui, klausymosi ar informacijos išgavimo prietaisai, leidžiami tik tuo atveju, jei tai numatyta įstatyme ir jei tai demokratinėje visuomenėje yra būtina priemonė siekiant:

- apsaugoti valstybės saugumą;
- visuomenės saugumą;
- valstybės piniginius interesus;
- užkardyti nusikalstamas veikas;
- apsaugoti duomenų subjektą arba kitų asmenų teises ir laisves.

Daugelyje kitų EŽTT sprendimų nagrinėjamas teisės į privatumą apribojimo atliekant sekimą pagrindimas.

Pavyzdys. Sprendime *Allan prieš Jungtinę Karalystę*[735] valdžios institucijos slapta įrašė kalinio pokalbius su draugu kalinių lankymo salėje ir pokalbius su kitu kaliniu kalėjimo kameroje. EŽTT nusprendė, kad naudojant garso ir vaizdo įrašymo prietaisus pareiškėjo kameroje, kalinių lankymo zonoje ir kito kalinio atžvilgiu buvo pažeista pareiškėjo teisė į privatų gyvenimą. Kadangi tuo metu nebuvo teisinės sistemos, kuri reglamentuotų policijos naudojimąsi slaptais įrašais, šis apribojimas neatitiko įstatymų. EŽTT padarė išvadą, kad buvo pažeistas EŽTK 8 straipsnis.

735 EŽTT, *Allan prieš Jungtinę Karalystę*, Nr. 48539/99, 2002 m. lapkričio 5 d.

Pavyzdys. Byloje *Roman Zakharov prieš Rusiją*[736] pareiškėjas iškėlė bylą trims judriojo ryšio tinklų operatoriams. Jis teigė, kad buvo pažeista jo teisė į telefoninių pranešimų privatumą, nes operatoriai įdiegė įrangą, leidžiančią Federalinei saugumo tarnybai be išankstinio teismo leidimo perimti jo telefoninius pranešimus. EŽTT nusprendė, kad nacionalinės teisės nuostatos, kuriomis reglamentuojamas pranešimų perėmimas, nesuteikia pakankamų ir veiksmingų garantijų nuo savivalės ir piktnaudžiavimo rizikos. Visų pirma pagal nacionalinę teisę nebuvo reikalaujama ištrinti saugomų duomenų pasiekus jų saugojimo tikslą. Be to, nors teismo leidimas buvo reikalingas, teisminė kontrolė buvo ribota.

Pavyzdys. Byloje *Szabó ir Vissy prieš Vengriją*[737] pareiškėjai teigė, kad Vengrijos teisės aktai pažeidė EŽTK 8 straipsnį, nes jie nėra pakankamai išsamūs ar tikslūs. Be to, buvo teigiama, kad teisės aktai nesuteikia pakankamų garantijų dėl piktnaudžiavimo ir savivalės. EŽTT nusprendė, kad pagal Vengrijos teisę nereikalaujama, kad sekimui būtų taikomas reikalavimas gauti teismo leidimą. Vis dėlto EŽTT pažymėjo, kad nors ši kontrolė buvo vykdoma gavus teisingumo ministro pritarimą, ji buvo labai politinio pobūdžio ir negalėjo užtikrinti reikalaujamo „griežto būtinumo“ vertinimo. Be to, nacionalinėje teisėje nebuvo numatyta galimybė atlikti teisminę peržiūrą, nes subjektams nebuvo siunčiamas joks pranešimas. Teismas padarė išvadą, kad buvo pažeistas EŽTK 8 straipsnis.

Kadangi policijos vykdomas duomenų tvarkymas gali turėti didelį poveikį atitinkamiems asmenims, ypač reikalingos išsamios asmens duomenų tvarkymo šioje srityje taisyklės. Europos Tarybos rekomendacija dėl policijos buvo siekiama spręsti šį klausimą, pateikiant gaires, kaip turėtų būti renkami asmens duomenys policijos darbo tikslais; kam turėtų būti leidžiama susipažinti su šiomis bylomis, įskaitant asmens duomenų perdavimo užsienio policijos institucijoms sąlygas; kaip duomenų subjektams reikėtų pasinaudoti savo duomenų apsaugos teisėmis ir kaip turėtų būti įgyvendinama nepriklausomų institucijų vykdoma kontrolė. Taip pat buvo nagrinėjama prievolė užtikrinti tinkamą duomenų saugumą.

Rekomendacijoje nenumatyta, kad policijos institucijos neribotai ir be atrankos rinktų asmens duomenis. Pagal ją policijos institucijos gali rinkti tik tuos asmens duomenis, kurie yra būtini siekiant užkirsti kelią realiam pavojui arba patraukti baudžiamojon

736 EŽTT, *Roman Zakharov prieš Rusiją*, Nr. 47143/06, 2015 m. gruodžio 4 d.

737 EŽTT, *Szabó ir Vissy prieš Vengriją*, Nr. 37138/14, 2016 m. sausio 12 d.

atsakomybėn už konkrečią nusikalstamą veiką. Bet kokie papildomi duomenys turi būti renkami remiantis nacionalinės teisės aktuose nustatytais pagrindais. Neskelbtinų duomenų tvarkymas turėtų apsiriboti tuo, kas tikrai būtina atliekant konkretų tyrimą.

Kai asmens duomenys renkami duomenų subjektui nežinant, duomenų subjektas turi būti informuojamas apie duomenų rinkimą, kai tik toks atskleidimas nebekenkia tyrimui. Duomenų rinkimas techninėmis stebėjimo ar kitomis automatizuotomis priemonėmis turi turėti konkretų teisinį pagrindą.

Pavyzdys. Byloje *Versini-Campinchi ir Crasnianski prieš Prancūziją*[738] pareiškėja, t. y. advokatė, bendravo telefonu su klientu, kurio telefono linija buvo perimta tyrimą atliekančio teisėjo prašymu. Pokalbio stenograma parodė, kad joje buvo atskleista informacija, kuriai taikoma profesinės paslapties apsauga. Prokuroras šią informaciją nusiuntė Advokatų tarybai, kuri skyrė pareiškėjai bausmę. EŽTT pripažino, kad buvo apribota ne tik asmens, kurio pokalbių telefonu buvo slapta klausomasi, bet ir pareiškėjos, kurios ryšiai buvo perimti ir transkribuoti, teisė į privatų gyvenimą ir susirašinėjimo slaptumą. Apribojimas buvo taikomas pagal įstatymą ir juo buvo siekiama teisėto tikslo, kuriuo siekta užkirsti kelią neramumams. Pareiškėjos prašymas peržiūrėti pateiktų įrašytų telefono pokalbių stenogramų teisėtumą, atsižvelgiant į prieš ją pradėtą drausminę bylą, buvo patenkintas. Nors ji negalėjo prašyti panaikinti pokalbio telefonu stenogramos, EŽTT nusprendė, kad buvo vykdoma veiksminga kontrolė, galinti apriboti skundžiamą kišimąsi tiek, kiek tai būtina demokratinėje visuomenėje. EŽTT nusprendė, kad argumentas, jog galimybė pradėti baudžiamąjį procesą prieš advokatę remiantis stenograma gali turėti atgrasomąjį poveikį advokatės ir jos kliento bendravimo laisvei, taigi ir jos teisei į gynybą, nėra įtikinamas, jei pačios advokatės padarytas atskleidimas gali prilygti neteisėtam jos elgesiui. Todėl nenustatyta, kad buvo pažeistas 8 straipsnis.

ET Rekomendacijoje dėl policijos nustatyta, kad, saugant asmens duomenis, būtina aiškiai atskirti administracinius duomenis ir policijos duomenis; skirtingų rūšių duomenų subjektų asmens duomenis, pavyzdžiui, įtariamųjų, nuteistų asmenų aukų ir liudytojų, ir duomenis, kurie laikomi svariais faktais, įtarimais arba spekuliacijomis pagrįstus duomenis.

738 EŽTT, *Versini-Campinchi ir Crasnianski prieš Prancūziją*, Nr. 49176/11, 2016 m. birželio 16 d.

Tikslas, kuriuo policija gali naudoti duomenis, turi būti griežtai ribotas. Tai sukelia pasekmes, kai policijos duomenys atskleidžiami trečiosioms šalims: tokių duomenų perdavimas arba atskleidimas policijos sektoriuje turėtų būti reglamentuojamas, nepaisant to, ar yra teisėtas interesas dalytis informacija. Perduoti arba atskleisti tokius duomenis už policijos sektoriaus ribų turėtų būti leidžiama tik tuo atveju, jei yra aiški teisinė prievolė arba leidimas.

Pavyzdys. Byloje *Karabeyoğlu prieš Turkiją*[739] pareiškėjo, t. y. teisėjo, telefono linijos buvo stebimos vykdant nusikalstamos veikos tyrimą dėl neteisėtos organizacijos, kuriai jis, kaip buvo įtariama, priklauso, arba kuriai, kaip buvo manoma, jis teikė pagalbą ir paramą. Priėmus sprendimą nevykdyti baudžiamojo persekiojimo, už baudžiamąjį tyrimą atsakingas prokuroras sunaikino atitinkamus įrašus. Tačiau kopija liko teismo tyrėjų žinioje, kurie vėliau panaudojo atitinkamą medžiagą drausminiam tyrimui prieš pareiškėją. EŽTT nusprendė, kad atitinkami teisės aktai buvo pažeisti, nes informacija buvo panaudota kitiems tikslams nei tie, dėl kurių ji buvo surinkta, ir nebuvo sunaikinta per įstatyme nustatytą terminą. Pareiškėjo teisės į jo privatų gyvenimą apribojimas neatitiko įstatymo atsižvelgiant į prieš jį pradėtą drausminę bylą.

Tarptautinis duomenų perdavimas arba atskleidimas turėtų būti vykdomas tik užsienio policijos institucijoms ir turėtų būti pagrįstas specialiomis teisinėmis nuostatomis, galbūt tarptautiniais susitarimais, išskyrus atvejus, kai tai yra būtina siekiant užkirsti kelią rimtam ir neišvengiamam pavojui.

Policijos tvarkomiems duomenims turi būti taikoma nepriklausoma priežiūra siekiant užtikrinti atitiktį nacionalinei duomenų apsaugos teisei. Duomenų subjektams turi būti suteiktos visos atnaujintoje 108-ojoje konvencijoje numatytos teisės susipažinti su duomenimis. Jeigu duomenų subjektų teisės susipažinti su informacija buvo apribotos pagal 108-osios konvencijos 9 straipsnį, siekiant užtikrinti veiksmingus policijos tyrimus ir baudžiamųjų sankcijų vykdymą, duomenų subjektas turi turėti teisę pagal nacionalinę teisę pateikti skundą nacionalinei duomenų apsaugos priežiūros institucijai arba kitai nepriklausomai įstaigai.

739 EŽTT, *Karabeyoğlu prieš Turkiją*, Nr. 30083/10, 2016 m. birželio 7 d.

8.1.2. Budapešto konvencija dėl elektroninių nusikaltimų

Kadangi nusikalstamoms veikoms vis dažniau naudojamos elektroninės duomenų tvarkymo sistemos ir šios sistemos nukenčia nuo tokių nusikalstamų veikų, šiam uždaviniui spręsti reikalingos naujos baudžiamosios teisinės nuostatos. Todėl ET priėmė tarptautinį teisinį dokumentą, t. y. Konvenciją dėl elektroninių nusikaltimų, kuri dar vadinama Budapešto konvencija, kad spręstų prieš elektroninius tinklus ir per juos daromų nusikaltimų problemą[740]. Prie šios konvencijos taip pat gali prisijungti ET nepriklausantys nariai. 2018 m. pradžioje Budapešto konvencijos šalimis buvo 14 ET nepriklausančių valstybių[741] ir dar septynios ET nepriklausančios valstybės narės pakviestos prisijungti prie konvencijos.

Konvencija dėl elektroninių nusikaltimų išlieka didžiausią įtaką turinčia tarptautine sutartimi, kurioje reglamentuojami internete arba kituose informacijos tinkluose daromi teisės aktų pažeidimai. Pagal ją reikalaujama, kad šalys atnaujintų ir suderintų savo baudžiamuosius teisės aktus atsižvelgdamos į įsilaužimus ir kitus saugumo pažeidimus, įskaitant autorių teisių pažeidimus, sukčiavimą naudojant kompiuterius, vaikų pornografiją ir kitą neteisėtą kibernetinę veiklą. Konvencijoje taip pat numatyti procedūriniai įgaliojimai, kurie apima kompiuterinių tinklų paiešką ir ryšių perėmimą kovos su elektroniniais nusikaltimais srityje. Galiausiai ji sudaro sąlygas veiksmingam tarptautiniam bendradarbiavimui. Konvencijos papildomame protokole aptariami baudžiamosios atsakomybės už rasinę ir ksenofobinę propagandą kompiuteriniuose tinkluose numatymo klausimai.

Nors konvencija nėra priemonė, kuria siekiama skatinti duomenų apsaugą, joje kriminalizuojamos veikos, kuriomis, tikėtina, pažeidžiama duomenų subjekto teisė į jo duomenų apsaugą. Be to, joje reikalaujama, kad susitariančiosios šalys priimtų teisėkūros priemones, kad jų nacionalinės institucijos galėtų perimti srauto ir turinio duomenis[742]. Joje susitariančiosioms šalims taip pat nustatyta prievolė įgyvendinant konvenciją numatyti tinkamą žmogaus teisių ir laisvių apsaugą, įskaitant pagal EŽTK

740 Europos Taryba, Ministrų Komitetas (2001 m.), Konvencija dėl elektroninių nusikaltimų, CETS Nr. 185, Budapeštas, 2001 m. lapkričio 23 d., įsigaliojo 2004 m. liepos 1 d.

741 Australija, Kanada, Čilė, Kolumbija, Dominikos Respublika, Izraelis, Japonija, Mauricijus, Panama, Senegalas, Šri Lanka, Tonga, Tunisas ir Jungtinės Amerikos Valstijos. Žr. Sutartį Nr. 185 pasirašiusių ir ratifikavusių šalių sąrašą (remiantis 2017 m. liepos mėn. duomenimis).

742 Europos Taryba, Ministrų Komitetas (2001 m.), Konvencijos dėl elektroninių nusikaltimų, CETS Nr. 185, Budapeštas, 2001 m. lapkričio 23 d., 20 ir 21 straipsniai.

garantuojamas teises, pavyzdžiui, teisę į duomenų apsaugą[743]. Kad galėtų prisijungti prie Budapešto konvencijos dėl elektroninių nusikaltimų, susitariančiosioms šalims nebūtina taip pat prisijungti prie 108-osios konvencijos.

8.2. ES duomenų teisė dėl duomenų apsaugos policijos ir baudžiamosios teisenos bylose

Pagrindiniai faktai

- ES lygmeniu duomenų apsauga policijos ir baudžiamosios teisenos bylose reglamentuojama atsižvelgiant į nacionalinį ir tarpvalstybinį valstybių narių policijos ir baudžiamosios teisenos institucijų ir ES subjektų vykdomą duomenų tvarkymą.
- Valstybės narės lygmeniu Duomenų apsaugos policijos ir baudžiamosios teisenos institucijoms tvarkant asmens duomenis direktyvą reikia perkelti į nacionalinę teisę.
- Duomenų apsauga policijos ir teisėsaugos tarpvalstybinio bendradarbiavimo srityje, ypač kovojant su terorizmu ir tarpvalstybiniu nusikalstamumu, reglamentuojama konkrečiomis teisinėmis priemonėmis.
- Galioja specialios duomenų apsaugos taisyklės, taikomos Europos policijos biurui (Europolui), Europos teisminio bendradarbiavimo padaliniui (Eurojustui) ir naujai sukurtai Europos prokuratūrai, kurios yra tarpvalstybinį teisėsaugos bendradarbiavimą palengvinančios ir skatinančios ES įstaigos.
- Specialios duomenų apsaugos taisyklės, kuriomis reglamentuojamas tarpvalstybinis keitimasis informacija tarp kompetentingų policijos ir teisminių institucijų, taip pat galioja bendroms ES lygmeniu įsteigtoms informacinėms sistemoms. Svarbūs pavyzdžiai yra Šengeno informacinė sistema II (SIS II), Vizų informacinė sistema (VIS) ir sistema EURODAC, t. y. centralizuota sistema, kurioje pateikiami trečiųjų šalių piliečių ir asmenų be pilietybės, prašančių suteikti prieglobstį vienoje iš ES valstybių narių, pirštų atspaudų duomenys.
- Šiuo metu ES atnaujina pirmiau išvardytas duomenų apsaugos nuostatas, kad jos atitiktų Duomenų apsaugos policijos ir baudžiamosios teisenos institucijoms tvarkant asmens duomenis direktyvos nuostatas.

743 *Ten pat*, 15 straipsnio 1 dalis.

8.2.1. Duomenų apsaugos policijos ir baudžiamosios teisenos institucijoms tvarkant asmens duomenis direktyva

Direktyva (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo[744] (Duomenų apsaugos policijos ir baudžiamosios teisenos institucijoms tvarkant asmens duomenis direktyva) siekiama apsaugoti baudžiamosios teisenos tikslais renkamus ir tvarkomus asmens duomenis, be kita ko:

- užtikrinti nusikalstamų veikų prevenciją, tyrimą, atskleidimą, baudžiamąjį persekiojimą už jas, įskaitant apsaugą nuo grėsmių visuomenės saugumui ir šių grėsmių prevenciją, arba bausmių vykdymą;
- įvykdyti baudžiamąją sankciją ir
- tokiais atvejais, kai policija ar kitos teisėsaugos institucijos imasi veiksmų, kad užtikrintų įstatymų laikymąsi ir apsaugotų nuo grėsmių visuomenės saugumui ir pagrindinėms visuomenės teisėms, kurios galėtų būti laikomos nusikalstama veika, ir užkirstų joms kelią.

Duomenų apsaugos policijos ir baudžiamosios teisenos institucijoms tvarkant asmens duomenis direktyva apsaugomi įvairių kategorijų asmenų, dalyvaujančių baudžiamajame procese, pavyzdžiui, liudytojų, informatorių, aukų, įtariamųjų ir bendrininkų, asmens duomenys. Policijos ir baudžiamosios teisenos institucijos privalo laikytis direktyvos nuostatų visais atvejais, kai jos tvarko tokius asmens duomenis teisėsaugos tikslais atsižvelgdamos į asmeninę ir dalykinę direktyvos taikymo sritį[745].

744 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, ir kuria panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR, OL L 119, 2016, p. 89 (Duomenų apsaugos policijos ir baudžiamosios teisenos institucijoms tvarkant asmens duomenis direktyva).

745 Duomenų apsaugos policijos ir baudžiamosios teisenos institucijoms tvarkant asmens duomenis direktyvos 2 straipsnio 1 dalis.

Tačiau tam tikromis sąlygomis duomenis taip pat leidžiama naudoti kitu tikslu. Duomenis tvarkyti kitu teisėsaugos tikslu nei tuo, kuriam jie buvo surinkti, leidžiama, tik jeigu tai teisėta, būtina ir proporcinga pagal nacionalinę arba ES teisę[746]. Jeigu duomenys tvarkomi kitais tikslais, taikomos Bendrojo duomenų apsaugos reglamento taisyklės. Duomenų mainų registravimas ir dokumentavimas yra viena iš konkrečių kompetentingų institucijų prievolių, siekiant padėti išaiškinti su skundais susijusią atsakomybę.

Policijos ir baudžiamosios teisenos srityje dirbančios kompetentingos institucijos yra valdžios institucijos arba institucijos, kurioms pagal nacionalinę teisę ir viešus įgaliojimus suteikta teisė vykdyti valdžios institucijos funkcijas[747], pavyzdžiui, privatūs kalėjimai[748]. Direktyva taip pat taikoma tiek duomenų tvarkymui nacionaliniu lygmeniu, tiek tarpvalstybiniam duomenų tvarkymui valstybių narių policijos ir teisminėse institucijose, taip pat tarptautiniam kompetentingų institucijų vykdomam duomenų perdavimui trečiosioms šalims ir tarptautinėms organizacijoms[749]. Ji neapima nacionalinio saugumo arba asmens duomenų tvarkymo ES institucijose, įstaigose, biuruose ir agentūrose[750].

Direktyvoje atsižvelgiama į specifinį policijos ir baudžiamosios teisenos sričių pobūdį ir ji iš esmės grindžiama Bendrajame duomenų apsaugos reglamente nustatytais principais ir apibrėžtimis. Priežiūrą gali vykdyti tos pačios valstybės narės institucijos, kurios ją vykdo pagal Bendrąjį duomenų apsaugos reglamentą. Direktyvoje nustatytos naujos policijos ir baudžiamosios teisenos institucijų prievolės – paskirti duomenų apsaugos pareigūnus ir atlikti poveikio duomenų apsaugai vertinimą[751]. Nors šios koncepcijos pagrįstos Bendruoju duomenų apsaugos reglamentu, direktyvoje aptartas konkretus policijos ir baudžiamosios teisenos institucijų pobūdis. Palyginti su reglamente nustatytu duomenų tvarkymu komerciniais tikslais, su

746 *Ten pat*, 4 straipsnio 2 punktas.

747 *Ten pat*, 3 straipsnio 7 dalis.

748 Europos Komisija (2016 m.), Komisijos komunikatas Europos Parlamentui pagal Sutarties dėl Europos Sąjungos veikimo 294 straipsnio 6 dalį dėl Tarybos pozicijos dėl Europos Parlamento ir Tarybos direktyvos dėl asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, nustatymo ar traukimo baudžiamojon atsakomybėn už jas arba baudžiamųjų sankcijų vykdymo tikslais ir laisvo tokių duomenų judėjimo, kuria panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR, priėmimo 2008/977/TVR, COM(2016) 213 *final*, Briuselis, 2016 m. balandžio 11 d.

749 Duomenų apsaugos policijos ir baudžiamosios teisenos institucijoms tvarkant asmens duomenis direktyvos V skyrius.

750 *Ten pat*, 2 straipsnio 3 dalis.

751 *Ten pat*, atitinkamai 32 ir 27 straipsniai.

saugumu susijusiam duomenų tvarkymui gali prireikti tam tikro lankstumo. Pavyzdžiui, jei duomenų subjektams būtų suteikta tokio paties lygio apsauga atsižvelgiant į teises gauti informaciją, susipažinti su savo asmens duomenimis arba juos ištrinti, kaip numatyta Bendrajame duomenų apsaugos reglamente, tai galėtų reikšti, kad bet kokia sekimo operacija, vykdoma teisėsaugos tikslais, taptų neveiksminga teisėsaugos srityje. Todėl direktyvoje nenumatytas skaidrumo principas. Panašiai, duomenų kiekio mažinimo ir tikslų apribojimo principai, pagal kuriuos reikalaujama, kad asmens duomenys būtų tvarkomi tik tiek, kiek būtina atsižvelgiant į tikslus, dėl kurių jie tvarkomi, ir kad jie būtų tvarkomi siekiant konkrečių ir aiškių tikslų, taip pat turi būti lanksčiai taikomi tvarkant duomenis saugumo srityje. Kompetentingų institucijų surinkta ir saugoma informacija apie konkretų atvejį gali būti labai naudinga sprendžiant būsimas bylas.

Su duomenų tvarkymu susiję principai

Duomenų apsaugos policijos ir baudžiamosios teisenos institucijoms tvarkant asmens duomenis direktyvoje nustatytos tam tikros pagrindinės apsaugos priemonės, susijusios su asmens duomenų naudojimu. Joje taip pat išvardyti šių duomenų tvarkymą reglamentuojantys principai. Valstybės narės privalo užtikrinti, kad asmens duomenys būtų:

- tvarkomi teisėtai ir sąžiningai;
- renkami konkrečiai nustatytais, aiškiai apibrėžtais ir teisėtais tikslais ir negali būti tvarkomi tokiu būdu, kuris būtų nesuderinamas su tais tikslais;
- tinkami, aktualūs ir ne pernelyg išsamūs atsižvelgiant į tikslus, kuriais jie yra tvarkomi;
- tikslūs ir prireikus atnaujinami; turi būti imamasi visų pagrįstų priemonių siekiant užtikrinti, kad asmens duomenys, kurie nėra tikslūs, atsižvelgiant į jų tvarkymo tikslus, būtų nedelsiant ištrinti arba ištaisyti;
- saugomi tokia forma, kad duomenų subjektų tapatybės būtų galima nustatyti ne ilgiau, nei tai yra būtina tais tikslais, kuriais jie tvarkomi;
- tvarkomi taip, kad būtų užtikrintas tinkamas asmens duomenų saugumas, įskaitant apsaugą nuo tvarkymo be leidimo arba neteisėto tvarkymo ir nuo netyčinio

praradimo, sunaikinimo ar sugadinimo, taikant tinkamas technines ar organizacines priemones[752].

Pagal direktyvą duomenų tvarkymas yra teisėtas tik tada, kai jis atliekamas tiek, kiek tai būtina atitinkamai užduočiai atlikti. Be to, tai turėtų daryti kompetentinga institucija, siekdama direktyvoje nustatytų tikslų, taip pat toks duomenų tvarkymas turi būti pagrįstas ES arba nacionaline teise[753]. Duomenys negali būti saugomi ilgiau nei tai būtina ir jie turi būti ištrinti arba periodiškai peržiūrimi laikantis tam tikrų terminų. Juos privalo naudoti tik kompetentinga institucija ir tik tuo tikslu, kuriuo duomenys buvo renkami, perduodami ar pateikiami.

Duomenų subjekto teisės

Direktyvoje taip pat nustatytos duomenų subjekto teisės. Tai yra:

- Teisė gauti informaciją. Valstybės narės numato, kad duomenų valdytojas duomenų subjektui leistų susipažinti bent su šia informacija: 1) duomenų valdytojo tapatybė ir kontaktai; 2) duomenų apsaugos pareigūno kontaktai; 3) duomenų tvarkymo tikslai, kuriais renkami asmens duomenys; 4) informacija apie teisę pateikti skundą priežiūros institucijai ir priežiūros institucijos kontaktai; ir 5) duomenų subjekto teisė susipažinti su asmens duomenimis, juos ištaisyti arba ištrinti ir apriboti duomenų tvarkymą[754]. Be šių bendrųjų informacijos reikalavimų, direktyvoje nustatyta, kad tam tikrais atvejais ir tam, kad duomenų valdytojai galėtų pasinaudoti savo teisėmis, jie turi suteikti duomenų subjektams informaciją apie duomenų tvarkymo teisinį pagrindą ir apie tai, kiek laiko duomenys bus saugomi. Jeigu asmens duomenys turi būti perduodami kitiems gavėjams, įskaitant gavėjus trečiosiose šalyse arba tarptautines organizacijas, duomenų subjektus būtina informuoti apie tokių gavėjų kategorijas. Galiausiai duomenų valdytojai privalo pateikti bet kurią papildomą informaciją, atsižvelgdami į konkrečias aplinkybes, kuriomis tvarkomi duomenys, pavyzdžiui, kai asmens duomenys buvo surinkti slapto sekimo metu, t. y. be duomenų subjekto žinios. Taip garantuojamas sąžiningas duomenų tvarkymas duomenų subjekto atžvilgiu[755].

752 *Ten pat*, 4 straipsnio 1 punktas.

753 *Ten pat*, 8 straipsnis.

754 *Ten pat*, 13 straipsnio 1 dalis.

755 *Ten pat*, 13 straipsnio 2 dalis.

- Teisė susipažinti su asmens duomenimis. Valstybės narės privalo užtikrinti, kad duomenų subjektas galėtų pasinaudoti teise žinoti, ar jo duomenys yra tvarkomi, ar ne. Jei duomenys yra tvarkomi, duomenų subjektas turėtų turėti galimybę susipažinti su tam tikra informacija, pavyzdžiui, tvarkomų duomenų kategorijomis[756]. Tačiau ši teisė gali būti apribota, pavyzdžiui, siekiant užkirsti kelią trukdymui atlikti tyrimą ar pakenkti patraukimui baudžiamojon atsakomybėn už nusikaltimą arba apsaugoti visuomenės saugumą ir kitų asmenų teises ir laisves[757].

- Teisė ištaisyti asmens duomenis. Valstybės narės privalo užtikrinti, kad duomenų subjektas turėtų teisę, kad neteisingi jo asmens duomenys būtų ištaisyti nepagrįstai nedelsiant. Be to, duomenų subjektas taip pat turi teisę, kad neišsamūs asmens duomenys būtų papildyti[758].

- Teisė ištrinti asmens duomenis ir apriboti duomenų tvarkymą. Tam tikrais atvejais duomenų valdytojas privalo ištrinti asmens duomenis. Be to, duomenų subjektas gali užtikrinti, kad jo asmens duomenys būtų ištrinti, tačiau tik tuo atveju, kai jie tvarkomi neteisėtai[759]. Tam tikrose situacijose, užuot ištrynus duomenis, jų tvarkymas gali būti apribotas. Tai gali įvykti tais atvejais, kai 1) asmens duomenų tikslumas buvo ginčijamas, tačiau to negalima patvirtinti, arba 2) kai asmens duomenys yra reikalingi kaip įrodymas[760].

Tais atvejais, kai duomenų valdytojas atsisako ištaisyti arba ištrinti asmens duomenis arba apriboti duomenų tvarkymą, apie tai duomenų subjektą būtina informuoti raštu. Valstybės narės gali apriboti šią teisę gauti informaciją, be kita ko, siekdamos apsaugoti visuomenės saugumą arba kitų asmenų teises ir laisves, remdamosi tomis pačiomis priežastimis, dėl kurių ribojama teisė gauti informaciją[761].

Duomenų subjektas paprastai turi teisę gauti informaciją apie savo asmens duomenų tvarkymą ir turi teisę susipažinti su duomenimis, kurių tvarkymui taikomi apribojimai, juos ištaisyti arba ištrinti duomenis, ir šias teises duomenų subjektas gali įgyvendinti duomenų valdytojo atžvilgiu. Kita vertus, pagal Duomenų apsaugos policijos ir baudžiamosios teisenos institucijoms tvarkant asmens duomenis direktyvą

756 *Ten pat*, 14 straipsnis.
757 *Ten pat*, 15 straipsnis.
758 *Ten pat*, 16 straipsnio 1 dalis.
759 *Ten pat*, 16 straipsnio 2 dalis.
760 *Ten pat*, 16 straipsnio 3 dalis.
761 *Ten pat*, 16 straipsnio 4 punktas.

duomenų subjektas gali netiesiogiai įgyvendinti savo teises per duomenų apsaugos priežiūros instituciją, kai duomenų valdytojas apriboja duomenų subjekto teises[762]. Pagal direktyvos 17 straipsnį reikalaujama, kad valstybės narės priimtų priemones, kuriomis užtikrinama, kad duomenų subjektų teisės taip pat galėtų būti įgyvendinamos per jų priežiūros instituciją. Būtent todėl duomenų valdytojas privalo informuoti duomenų subjektą apie galimybę netiesiogiai susipažinti su informacija.

Duomenų valdytojo ir duomenų tvarkytojo prievolės

Kalbant apie Duomenų apsaugos policijos ir baudžiamosios teisenos institucijoms tvarkant asmens duomenis direktyvą, pažymėtina, kad duomenų valdytojai yra kompetentingos valdžios institucijos arba kitos atitinkamos viešuosius įgaliojimus ir teises turinčios įstaigos, nustatančios asmens duomenų tvarkymo tikslus ir priemones. Direktyvoje nustatyta keletas prievolių duomenų valdytojams, kad būtų užtikrintas aukštas teisėsaugos tikslais tvarkomų asmens duomenų apsaugos lygis.

Kompetentingos institucijos privalo saugoti duomenų tvarkymo operacijų, kurias jos vykdo automatizuotose duomenų tvarkymo sistemose, registracijos įrašus. Registracijos įrašai turi būti saugomi bent asmens duomenų rinkimo, keitimo, susipažinimo su jais, atskleidimo, įskaitant perdavimą, sujungimo ir ištrynimo tikslais[763]. Direktyvoje nustatyta, kad iš registracijos įrašų apie susipažinimą su duomenimis ir jų atskleidimą turi būti įmanoma nustatyti operacijų datą ir laiką, jų pagrindimą ir, kiek įmanoma, asmens, kuris naudojosi sistema arba atskleidė asmens duomenis, tapatybę bei atitinkamų asmens duomenų gavėjus. Registracijos įrašai turi būti naudojami tik siekiant patikrinti duomenų tvarkymo teisėtumą, savikontrolės tikslais, siekiant užtikrinti asmens duomenų vientisumą ir saugumą ir baudžiamosiose bylose[764]. Priežiūros institucijos prašymu duomenų valdytojas ir duomenų tvarkytojas privalo leisti jai susipažinti su registracijos įrašais.

Visų pirma galioja bendra duomenų valdytojų prievolė įgyvendinti tinkamas technines ir organizacines priemones siekiant užtikrinti, kad duomenys būtų tvarkomi pagal direktyvą ir kad duomenų valdytojai sugebėtų įrodyti tokio tvarkymo teisėtumą[765]. Kurdami tokias priemones, duomenų valdytojai privalo atsižvelgti į duomenų tvarkymo pobūdį, aprėptį, kontekstą bei tikslus, ypač į bet kokią riziką fizinių

762 *Ten pat*, 17 straipsnis.

763 *Ten pat*, 25 straipsnio 1 punktas.

764 *Ten pat*, 25 straipsnio 2 punktas.

765 *Ten pat*, 19 straipsnis.

asmenų teisėms ir laisvėms. Duomenų valdytojai turėtų nustatyti nacionalinę politiką ir įgyvendinti priemones, kurios palengvintų duomenų apsaugos principų laikymąsi, visų pirma tai pasakytina apie pritaikytosios ir standartizuotosios duomenų apsaugos principą[766]. Jeigu tikėtina, kad duomenų tvarkymas kels didelę riziką asmenų teisėms dėl, pavyzdžiui, naujų technologijų naudojimo, duomenų valdytojai prieš pradėdami tvarkyti duomenis privalo atlikti poveikio duomenų apsaugai vertinimą[767]. Direktyvoje taip pat išvardytos priemonės, kurias duomenų valdytojai privalo įgyvendinti, kad užtikrintų saugų duomenų tvarkymą. Tai, be kita ko, yra priemonės, kuriomis siekiama užkirsti kelią neteisėtai prieigai prie jų tvarkomų asmens duomenų, užtikrinti, kad įgaliotieji asmenys turėtų prieigą tik prie asmens duomenų, su kuriais jie gali susipažinti, kad duomenų tvarkymo sistemos funkcijos veiktų tinkamai ir kad saugomi asmens duomenys negalėtų būti iškraipyti dėl sistemos gedimo[768]. Jeigu padaromas asmens duomenų saugumo pažeidimas, tuomet duomenų valdytojai privalo per tris dienas informuoti priežiūros instituciją aprašydami pažeidimo pobūdį, jo tikėtinas pasekmes, susijusių asmens duomenų kategorijas ir apytikslį atitinkamų nukentėjusių duomenų subjektų skaičių. Apie asmens duomenų saugumo pažeidimą taip pat būtina pranešti duomenų subjektui „nepagrįstai nedelsiant“, jeigu tikėtina, kad pažeidimas sukels didelį pavojų jo teisėms ir laisvėms[769].

Direktyvoje įtvirtintas atskaitomybės principas, pagal kurį duomenų valdytojai įpareigojami įgyvendinti priemones, kuriomis užtikrinamas šio principo laikymasis. Duomenų valdytojai privalo saugoti visų kategorijų duomenų tvarkymo veiklos, už kurią jie yra atsakingi, įrašus: išsamus tokių įrašų turinys nustatytas direktyvos 24 straipsnyje. Priežiūros institucijai paprašius, jai turi būti leista susipažinti su įrašais, kad ji galėtų stebėti duomenų valdytojo tvarkymo operacijas. Kita svarbi atskaitomybės didinimo priemonė yra duomenų apsaugos pareigūno (DAP) paskyrimas. Duomenų valdytojai privalo paskirti DAP, nors pagal direktyvą valstybėms narėms leidžiama šios prievolės netaikyti teismams ir kitoms nepriklausomoms teisminėms institucijoms[770]. DAP pareigos yra panašios į tas, kurios nustatytos Bendrajame duomenų apsaugos reglamente. DAP stebi, ar laikomasi direktyvos, teikia informaciją ir pataria darbuotojams, kurie tvarko duomenis, apie jų prievoles pagal duomenų apsaugos teisės aktus. DAP taip pat teikia konsultacijas apie poreikį atlikti poveikio duomenų apsaugai vertinimą ir veikia kaip priežiūros institucijos kontaktinis asmuo.

766 *Ten pat*, 20 straipsnis.

767 *Ten pat*, 27 straipsnis.

768 *Ten pat*, 29 straipsnis.

769 *Ten pat*, 30 ir 31 straipsniai.

770 *Ten pat*, 32 straipsnis.

Duomenų perdavimas trečiosioms šalims arba tarptautinėms organizacijoms

Panašiai kaip ir Bendrajame duomenų apsaugos reglamente, direktyvoje nustatytos asmens duomenų perdavimo trečiosioms šalims arba tarptautinėms organizacijoms sąlygos. Jeigu asmens duomenys buvo perduoti laisvai už ES jurisdikcijos, gali būti pakenkta apsaugos priemonėms ir griežtai apsaugai, kuri užtikrinama pagal ES teisę. Tačiau pačios sąlygos gerokai skiriasi nuo nustatytų Bendrajame duomenų apsaugos reglamente. Asmens duomenis trečiosioms šalims arba tarptautinėms organizacijoms leidžiama perduoti, jeigu[771]:

- duomenis perduoti būtina siekiant direktyvos tikslų;
- asmens duomenys perduodami trečiosios šalies kompetentingai institucijai arba tarptautinei organizacijai, kaip apibrėžta direktyvoje, nors individualiais ir konkrečiais atvejais galioja nukrypti nuo šios taisyklės leidžianti nuostata[772];
- norint trečiosioms šalims arba tarptautinėms organizacijoms perduoti tarpvalstybinio bendradarbiavimo metu gautus asmens duomenis, reikia gauti valstybės narės, iš kurios gauti duomenys, leidimą, nors skubiais atvejais taikomos išimtys;
- Europos Komisija priėmė sprendimą dėl tinkamumo, buvo nustatytos tinkamos apsaugos priemonės arba konkrečiose situacijose duomenų perdavimui taikoma nukrypti leidžianti nuostata;
- tolesniam asmens duomenų perdavimui į kitą trečiąją šalį arba tarptautinei organizacijai reikia išankstinio juos parengusios kompetentingos institucijos leidimo, kuri, be kita ko, atsižvelgs į nusikalstamos veikos sunkumą ir duomenų apsaugos lygį antro tarptautinio duomenų perdavimo paskirties šalyje[773].

Pagal direktyvą asmens duomenis galima perduoti, jeigu įvykdoma viena iš trijų sąlygų. Pirmoji sąlyga yra susijusi su tuo, kad Europos Komisija pagal tą direktyvą priėmė sprendimą dėl tinkamumo. Sprendimas gali būti taikomas visai trečiosios šalies teritorijai arba konkretiems trečiosios šalies sektoriams, arba tarptautinei organizacijai. Tačiau tai galima padaryti tik tuo atveju, jei užtikrinamas tinkamas apsaugos

771 *Ten pat*, 35 straipsnis.

772 *Ten pat*, 39 straipsnis

773 *Ten pat*, 35 straipsnio 1 dalis.

lygis ir tenkinamos direktyvoje nustatytos sąlygos[774]. Tokiais atvejais asmens duomenims perduoti valstybės narės leidimas nereikalingas[775]. Europos Komisija turi stebėti pokyčius, kurie galėtų turėti įtakos sprendimų dėl tinkamumo veikimui. Be to, sprendime turi būti numatytas periodinės peržiūros mechanizmas. Komisija taip pat gali panaikinti, iš dalies pakeisti arba sustabdyti sprendimo galiojimą, jei iš turimos informacijos matyti, kad sąlygos trečiojoje šalyje arba tarptautinėje organizacijoje nebeužtikrina tinkamo apsaugos lygio. Jeigu taip, Komisija turi pradėti konsultacijas su trečiąja šalimi arba tarptautine organizacija, siekdama ištaisyti padėtį.

Jeigu sprendimo dėl tinkamumo nėra, duomenis galima perduoti užtikrinant tinkamas apsaugos priemones. Jos gali būti nustatytos teisiškai privalomame teisės akte arba duomenų valdytojas gali savarankiškai įvertinti su asmens duomenų perdavimu susijusias aplinkybes ir padaryti išvadą, kad tinkamos apsaugos priemonės egzistuoja. Atliekant savarankišką vertinimą, reikėtų atsižvelgti į galimus Europolo ar Eurojusto ir trečiosios valstybės ar tarptautinės organizacijos bendradarbiavimo susitarimus, pareigas išlaikyti konfidencialumą ir tikslo apribojimą, taip pat į garantijas, kad duomenys nebus naudojami jokiam žiauriam ir nežmoniškam elgesiui, įskaitant mirties bausmę[776]. Pastaruoju atveju duomenų valdytojas privalo informuoti kompetentingą priežiūros instituciją apie pagal šią kategoriją atliekamo duomenų perdavimo kategorijas[777].

Tais atvejais, kai nepriimtas sprendimas dėl tinkamumo arba nenustatytos tinkamos apsaugos priemonės, duomenis vis tiek gali būti leidžiama perduoti tam tikromis direktyvoje nurodytomis aplinkybėmis. Tai, be kita ko, apima duomenų subjekto arba kito asmens gyvybinių interesų apsaugą ir neišvengiamo ir rimto pavojaus, susijusio su valstybės narės arba trečiosios šalies visuomenės saugumu, prevenciją[778].

Pavieniais ir konkrečiais atvejais kompetentingos institucijos duomenis trečiosiose šalyse įsteigtiems gavėjams gali perduoti, jeigu, be vienos iš trijų pirmiau aprašytų sąlygų, taip pat įvykdomos papildomos direktyvos 39 straipsnyje nustatytos sąlygos. Visų pirma duomenis perduoti turi būti būtina, kad perduodančioji kompetentinga institucija, kuri taip pat privalo nustatyti, kad jokios pagrindinės asmenų teisės

774 *Ten pat*, 36 straipsnis.

775 *Ten pat*, 36 straipsnio 1 dalis.

776 *Ten pat*, 71 konstatuojamoji dalis.

777 *Ten pat*, 37 straipsnio 1 dalis.

778 *Ten pat*, 38 straipsnio 1 punktas.

ar laisvės nėra viršesnės už duomenų perdavimą pateisinantį viešąjį interesą, galėtų atlikti užduotį. Toks duomenų perdavimas turi būti dokumentuojamas, o perduodančioji kompetentinga institucija turi informuoti kompetentingą priežiūros instituciją[779].

Galiausiai, kalbant apie trečiąsias šalis ir tarptautines organizacijas, direktyvoje taip pat reikalaujama plėtoti tarptautinio bendradarbiavimo mechanizmus, kad būtų sudarytos palankesnės sąlygos veiksmingam teisės aktų vykdymui ir taip padedama duomenų apsaugos priežiūros institucijoms bendradarbiauti su atitinkamomis užsienio institucijomis[780].

Nepriklausoma priežiūra ir duomenų subjektų teisių gynimo priemonės

Kiekviena valstybė narė privalo užtikrinti, kad viena ar kelios nepriklausomos nacionalinės priežiūros institucijos patartų ir prižiūrėtų, kaip taikomos pagal šią direktyvą priimtos nuostatos[781]. Pagal šią direktyvą įsteigta priežiūros institucija gali būti ta pati kaip ir pagal Bendrąjį duomenų apsaugos reglamentą įsteigta priežiūros institucija, tačiau valstybės narės gali paskirti kitą instituciją, jeigu ji atitinka nepriklausomumo kriterijus. Priežiūros institucijos taip pat nagrinėja bet kurio asmens pateiktus ieškinius dėl jo teisių ir laisvių apsaugos kompetentingoms institucijoms tvarkant asmens duomenis.

Jei duomenų subjektui atsisakoma leisti pasinaudoti savo teisėmis dėl įtikinamų priežasčių, jis turi turėti teisę pateikti skundą kompetentingai nacionalinei priežiūros institucijai ir (arba) teismui. Jeigu asmuo patiria žalą dėl nacionalinės teisės, kuria įgyvendinama direktyva, pažeidimo, jis turi teisę gauti kompensaciją iš duomenų valdytojo arba bet kurios kitos pagal valstybės narės teisę kompetentingos institucijos[782]. Apskritai duomenų subjektai turi turėti galimybę pasinaudoti teismine teisių gynimo priemone, jei pažeidžiamos jų teisės, garantuojamos nacionalinės teisės aktais, kuriais įgyvendinama direktyva[783].

779 *Ten pat*, 37 straipsnio 3 dalis.

780 *Ten pat*, 40 straipsnis.

781 *Ten pat*, 41 straipsnis.

782 *Ten pat*, 56 straipsnis.

783 *Ten pat*, 54 straipsnis.

8.3. Kiti specifiniai duomenų apsaugos teisės aktai, galiojantys teisėsaugos srityje

Be Duomenų apsaugos policijos ir baudžiamosios teisenos institucijoms tvarkant asmens duomenis direktyvos, keitimasis valstybių narių turima informacija konkrečiose srityse reglamentuojamas pagal įvairius teisės aktus, pavyzdžiui, Tarybos pamatinį sprendimą 2009/315/TVR dėl valstybių narių keitimosi informacija iš nuosprendžių registro organizavimo ir turinio, Tarybos sprendimą 2000/642/TVR dėl valstybių narių finansinės žvalgybos padalinių bendradarbiavimo susitarimų dėl keitimosi informacija ir 2006 m. gruodžio 18 d. Tarybos pamatinį sprendimą 2006/960/TVR dėl keitimosi informacija ir žvalgybos informacija tarp Europos Sąjungos valstybių narių teisėsaugos institucijų supaprastinimo[784].

Dar svarbiau tai, kad kompetentingų institucijų tarpvalstybinis bendradarbiavimas[785] vis dažniau apima keitimąsi imigracijos duomenimis. Ši teisės sritis nelaikoma policijos ir baudžiamosios teisenos klausimų dalimi, tačiau daugeliu atžvilgių ji yra svarbi policijos ir teisingumo institucijų darbui. Tą patį galima pasakyti apie į ES importuojamų arba iš ES eksportuojamų prekių duomenis. Panaikinus vidaus sienų kontrolę Šengeno erdvėje padidėjo sukčiavimo rizika, todėl būtina, kad valstybės narės intensyvintų bendradarbiavimą, visų pirma stiprindamos tarpvalstybinį keitimąsi informacija, kad veiksmingiau nustatytų nacionalinės ir ES muitų teisės pažeidimus ir patrauktų už juos baudžiamojon atsakomybėn. Be to, pastaraisiais metais pasaulyje padaugėjo sunkių formų ir organizuoto nusikalstamumo bei terorizmo atvejų, kurie gali būti susiję su tarptautinėmis kelionėmis, ir paaiškėjo, kad daugeliu atvejų reikia intensyvesnio policijos ir teisėsaugos institucijų tarpvalstybinio bendradarbiavimo[786].

784 Europos Sąjungos Taryba (2009 m.), 2009 m. vasario 26 d. Tarybos pamatinis sprendimas 2009/315/TVR dėl valstybių narių keitimosi informacija iš nuosprendžių registro organizavimo ir turinio, OL L 93, 2009; Europos Sąjungos Taryba (2000 m.), 2000 m. spalio 17 d. Tarybos sprendimas 2000/642/TVR dėl valstybių narių finansinės žvalgybos padalinių bendradarbiavimo susitarimų dėl keitimosi informacija, OL L271, 2000; 2006 m. gruodžio 18 d. Tarybos pamatinis sprendimas 2006/960/TVR dėl keitimosi informacija ir žvalgybos informacija tarp Europos Sąjungos valstybių narių teisėsaugos institucijų supaprastinimo, OL L 386.

785 Europos Komisija (2012 m.), *Komisijos komunikatas Europos Parlamentui ir Tarybai „Bendradarbiavimo teisėsaugos srityje stiprinimas ES: Europos keitimosi informacija modelis (EKIM)“*, COM(2012) 735 *final*, Briuselis, 2012 m. gruodžio 7 d.

786 Žr. Europos Komisijos (2011 m.) Pasiūlymą dėl Europos Parlamento ir Tarybos direktyvos dėl keleivio duomenų įrašo duomenų naudojimo teroristinių nusikaltimų ir sunkių nusikaltimų prevencijos, nustatymo, tyrimo ir patraukimo už juos baudžiamojon atsakomybėn tikslais, COM(2011) 32 *final*, Briuselis, 2011 m. vasario 2 d., p. 1.

Priumo sprendimas

Svarbus institucionalizuoto tarpvalstybinio bendradarbiavimo keičiantis nacionaliniu lygmeniu turimais duomenimis pavyzdys yra Tarybos sprendimas 2008/615/TVR ir jo įgyvendinimo nuostatos Sprendime 2008/615/TVR dėl tarpvalstybinio bendradarbiavimo gerinimo, visų pirma kovos su terorizmu ir tarpvalstybiniu nusikalstamumu srityje (Priumo sprendimas), kuriuo Priumo sutartis į ES teisę buvo įtraukta 2008 m.[787] Priumo sutartis buvo tarptautinė policijos bendradarbiavimo sutartis, ją 2005 m. pasirašė Austrija, Belgija, Prancūzija, Vokietija, Liuksemburgas, Nyderlandai ir Ispanija[788].

Priumo sprendimu siekiama padėti susitariančiosioms valstybėms narėms pagerinti dalijimąsi informacija siekiant užkirsti kelią nusikaltimams trijose srityse ir su jais kovoti: tai terorizmas, tarpvalstybiniai nusikaltimai ir neteisėta migracija. Šiuo tikslu sprendime įtvirtintos nuostatos, susijusios su:

- automatine prieiga prie DNR charakteristikų, pirštų atspaudų duomenų ir tam tikrų nacionalinių transporto priemonių registracijos duomenų;
- duomenų, susijusių su didelio masto tarpvalstybinio pobūdžio renginiais, teikimu;
- informacijos teikimu siekiant užkirsti kelią teroristiniams nusikaltimams;
- kitomis priemonėmis, kurias taikant pradedamas tarpvalstybinis policijos bendradarbiavimas.

Duomenų bazėms, kuriomis galima naudotis pagal Priumo sprendimą, taikoma tik nacionalinė teisė, tačiau keitimasis duomenimis taip pat reglamentuojamas sprendimu, kurio suderinamumas su Duomenų apsaugos direktyva, skirta policijos ir baudžiamosios teisenos institucijoms, turės būti įvertintas. Už tokių duomenų srautų priežiūrą atsakingos kompetentingos įstaigos yra nacionalinės duomenų apsaugos priežiūros institucijos.

787 Europos Sąjungos Taryba (2008 m.), 2008 m. birželio 23 d. Tarybos sprendimas 2008/615/TVR dėl tarpvalstybinio bendradarbiavimo gerinimo, visų pirma kovos su terorizmu ir tarpvalstybiniu nusikalstamumu srityje, OL L 210, 2008.

788 Belgijos Karalystės, Vokietijos Federacinės Respublikos, Ispanijos Karalystės, Prancūzijos Respublikos, Liuksemburgo Didžiosios Hercogystės, Nyderlandų Karalystės ir Austrijos Respublikos konvencija dėl tarpvalstybinio bendradarbiavimo gerinimo, pirmiausia kovos su terorizmu, tarpvalstybiniu nusikalstamumu ir neteisėta migracija srityje.

Pamatinis sprendimas 2006/960/TVR – Švedijos iniciatyva

Pamatinis sprendimas 2006/960/TVR (Švedijos iniciatyva)[789] yra kitas tarpvalstybinio bendradarbiavimo atsižvelgiant į teisėsaugos institucijų vykdomą keitimąsi turimais duomenimis tarptautiniu lygmeniu pavyzdys. Švedijos iniciatyva yra orientuota būtent į keitimąsi žvalgybos duomenimis ir informacija, o jos 8 straipsnyje nustatytos konkrečios duomenų apsaugos taisyklės.

Pagal šį dokumentą informacija ir žvalgybos duomenys, kuriais keičiamasi, turi būti naudojami laikantis informaciją gaunančios valstybės narės nacionalinių duomenų apsaugos nuostatų pagal tas pačias taisykles, kurios būtų taikomos tuo atveju, jei informacija ir žvalgybos duomenys būtų surinkti toje valstybėje narėje. 8 straipsnyje taip pat nurodyta, kad teikdama informaciją ir žvalgybos informaciją kompetentinga teisėsaugos institucija gali nustatyti sąlygas, kurios atitiktų jos nacionalinę teisę, dėl gaunančiosios kompetentingos teisėsaugos institucijos naudojimosi ta informacija ir žvalgybos duomenimis. Šios sąlygos taip pat gali būti taikomos pranešimui apie nusikalstamos veikos tyrimo rezultatus arba kriminalinės žvalgybos operacijoms, dėl kurių reikėjo keistis informacija ir žvalgybos duomenimis. Tačiau kai nacionalinėje teisėje numatytos naudojimo apribojimų išimtys (pavyzdžiui, teisminėms institucijoms, teisėkūros institucijoms ir kt.), informacija ir žvalgybos duomenys gali būti naudojami tik iš anksto pasikonsultavus su perduodančiąja valstybe nare.

Pateikta informacija ir žvalgybos duomenys gali būti naudojami:

- tikslais, kuriais ji buvo suteikta, arba
- užkertant kelią tiesioginei ir rimtai grėsmei visuomenės saugumui.

Tvarkyti duomenis kitais tikslais gali būti leidžiama, tačiau tik gavus išankstinį perduodančiosios valstybės narės leidimą.

Švedijos iniciatyvoje taip pat nurodyta, kad tvarkomi asmens duomenys turi būti apsaugoti pagal tokias tarptautines priemones, kaip:

789 Europos Sąjungos Taryba (2006 m.), 2006 m. gruodžio 18 d. Tarybos pamatinis sprendimas 2006/960/TVR dėl keitimosi informacija ir žvalgybos informacija tarp Europos Sąjungos valstybių narių teisėsaugos institucijų supaprastinimo, OL L 386/89, 2006 m. gruodžio 29 d.

- Europos Tarybos Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu[790];

- tos Konvencijos 2001 m. lapkričio 8 d. Papildomas protokolas dėl priežiūros institucijų ir tarpvalstybinio duomenų judėjimo[791];

- Europos Tarybos Rekomendacija Nr. R(87) 5, reglamentuojanti asmens duomenų naudojimą policijos sektoriuje[792].

ES PNR direktyva

Keleivio duomenų įrašo (PNR) duomenys yra susiję su informacija apie oro transporto keleivius, kuri renkama ir laikoma vežėjų bilietų užsakymo ir išvykimo kontrolės sistemose jų pačių komerciniais tikslais. Šie duomenys apima kelių rūšių skirtingą informaciją, pavyzdžiui, kelionių datas, kelionės maršrutą, bilietų informaciją, kontaktinius duomenis, kelionių agentūrą, kurioje buvo užsakytas skrydis, naudoto mokėjimo priemones, vietą lėktuve ir informaciją apie bagažą[793]. PNR duomenų tvarkymas gali padėti teisėsaugos institucijoms nustatyti žinomus arba potencialius įtariamuosius ir, remiantis kelionių modeliais ir kitais rodikliais, kurie paprastai susiję su nusikalstama veika, atlikti vertinimus. PNR duomenų analizė taip pat sudaro sąlygas atgaline data stebėti kelionės maršrutus ir asmenų, kurie, kaip įtariama, dalyvavo nusikalstamoje veikoje, kontaktus, o tai gali padėti teisėsaugos institucijoms išaiškinti nusikaltėlių tinklus[794]. ES sudarė keletą susitarimų su trečiosiomis valstybėmis dėl keitimosi PNR duomenimis, kaip paaiškinta 7 skirsnyje. Be to, Direktyvoje (ES) 2016/681 dėl keleivio duomenų įrašo (PNR) duomenų naudojimo teroristinių nusikaltimų ir sunkių nusikaltimų prevencijos, nustatymo, tyrimo ir patraukimo už

790 Europos Taryba (1981 m.), Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu, ETS Nr. 108.

791 Europos Taryba (2001 m.), Konvencijos dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu papildomas protokolas dėl priežiūros institucijų ir tarpvalstybinio duomenų judėjimo, CETS Nr. 108.

792 Europos Taryba (1987 m.), Ministrų Komiteto rekomendacija Nr. R (87) 15 valstybėms narėms, reglamentuojanti asmens duomenų naudojimą policijos sektoriuje (1987 m. rugsėjo 17 d. priėmė Ministrų Komitetas 410-ajame ministrų pavaduotojų susitikime).

793 Europos Komisija (2011 m.), Pasiūlymas dėl Europos Parlamento ir Tarybos direktyvos dėl keleivio duomenų įrašo duomenų naudojimo teroristinių nusikaltimų ir sunkių nusikaltimų prevencijos, nustatymo, tyrimo ir patraukimo už juos baudžiamojon atsakomybėn tikslais, COM(2011) 32 *final*, Briuselis, 2011 m. vasario 2 d., p. 1.

794 Europos Komisija (2015 m.), Faktų dėl kovos su terorizmu ES lygmeniu suvestinė, Komisijos veiksmų, priemonių ir iniciatyvų apžvalga, Briuselis, 2015 m. sausio 11 d.

juos baudžiamojon atsakomybėn tikslais (ES PNR direktyva)[795] ji nustatė PNR duomenų tvarkymo ES tvarką. Šioje direktyvoje nustatytos oro vežėjų prievolės perduoti PNR duomenis kompetentingoms institucijoms, taip pat griežtos su tokių duomenų tvarkymu ir rinkimu susijusios apsaugos priemonės. ES PNR direktyva taikoma tarptautiniams skrydžiams į ES ir iš ES, taip pat skrydžiams ES viduje, jei taip nusprendžia valstybė narė[796].

Surinktuose PNR duomenyse turi būti tik ta informacija, kuri yra leidžiama pagal ES PNR direktyvą. Ji turi būti saugoma viename informacijos skyriuje saugioje vietoje kiekvienoje valstybėje narėje. PNR duomenys turi būti nuasmeninti praėjus šešiems mėnesiams nuo momento, kai juos perdavė oro vežėjas, ir saugomi ne ilgiau kaip penkerius metus[797]. PNR duomenimis keičiasi valstybės narės, valstybės narės ir Europolas, ir kiekvienu konkrečiu atveju jais keičiamasi su trečiosiomis šalimis.

PNR duomenų perdavimas ir tvarkymas ir duomenų subjektų saugomos teisės privalo derėti su Duomenų apsaugos policijos ir baudžiamosios teisenos institucijoms tvarkant asmens duomenis direktyva, be to, būtina užtikrinti aukšto lygio privatumo ir asmens duomenų apsaugą, kaip to reikalaujama pagal Chartiją, atnaujintą 108-ąją konvenciją ir EŽTK.

Nepriklausomos nacionalinės priežiūros institucijos, kurios turi kompetenciją pagal Duomenų apsaugos policijos ir baudžiamosios teisenos institucijoms tvarkant asmens duomenis direktyvą, taip pat privalo patarti, kaip pagal ES PNR direktyvą taikyti valstybių narių priimtas nuostatas ir stebėti jų taikymą.

Telekomunikacijos duomenų saugojimas

Duomenų saugojimo direktyvoje[798], kuri paskelbta negaliojančia 2014 m. balandžio 8 d. Sprendime *Digital Rights Ireland*, ryšių paslaugų teikėjai privalėjo konkrečiu tikslu, susijusiu su kova su sunkiais nusikaltimais, ne trumpiau kaip šešis, bet ne

795 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/681 dėl keleivio duomenų įrašo (PNR) duomenų naudojimo teroristinių nusikaltimų ir sunkių nusikaltimų prevencijos, nustatymo, tyrimo ir patraukimo už juos baudžiamojon atsakomybėn tikslais, OL L 119, 2016, p. 132.

796 PNR direktyvos, L 119, p. 132, 1 straipsnio 1 dalis ir 2 straipsnio 1 dalis.

797 *Ten pat*, 12 straipsnio 1 dalis ir 12 straipsnio 2 dalis.

798 2006 m. kovo 15 d. Europos Parlamento ir Tarybos direktyva 2006/24/EB dėl duomenų, generuojamų arba tvarkomų teikiant viešai prieinamas elektroninių ryšių paslaugas arba viešuosius ryšių tinklus, saugojimo ir iš dalies keičianti Direktyvą 2002/58/EB, OL L 105, 2006.

ilgiau kaip 24 mėnesius saugoti metaduomenis, nepaisant to, ar paslaugų teikėjui šių duomenų dar reikia sąskaitų išrašymo tikslais arba paslaugai techniškai teikti.

Akivaizdu, kad saugant telekomunikacijos duomenis ribojama teisė į duomenų apsaugą[799]. Klausimas, ar šis apribojimas yra pagrįstas, buvo ginčijamas keliuose ES valstybių narių teisminiuose procesuose[800].

Pavyzdys. Byloje *Digital Rights Ireland* ir *Kärntner Landesregierung ir kt.*[801], *Digital Rights group* ir M. Seitlinger pareiškė ieškinį atitinkamai Airijos aukštajame teisme ir Austrijos Konstituciniame Teisme ginčydamas nacionalinių priemonių, kuriomis leidžiama saugoti elektroninių telekomunikacijų duomenis, teisėtumą. *Digital Rights* prašė Airijos teismo paskelbti negaliojančia Direktyvą 2006/24/EB ir tam tikras nacionalinės baudžiamosios teisės nuostatas, susijusias su teroristinėmis nusikalstamomis veikomis. Panašiai M. Seitlinger ir daugiau nei 11 000 kitų pareiškėjų ginčijo ir prašė panaikinti Austrijos teisės akto dėl telekomunikacijų nuostatą, kuria į nacionalinę teisę buvo perkelta Direktyva 2006/24/EB.

Nagrinėdamas šiuos prašymus priimti prejudicinį sprendimą, ESTT paskelbė Duomenų saugojimo direktyvą negaliojančia. Pasak ESTT, duomenyse, kuriuos buvo galima saugoti pagal direktyvą, atsižvelgiant į visas jos nuostatas, buvo numatyta tiksli informacija apie asmenis. Be to, ESTT nagrinėjo, kiek rimtai buvo apribotos pagrindinės teisės į privatų gyvenimą ir asmens duomenų apsaugą. Jis nustatė, kad saugojimas atitinka viešojo intereso tikslą, t. y. kovoti su sunkiais nusikaltimais ir taip užtikrinti visuomenės saugumą. Vis dėlto ESTT nurodė, kad ES teisės aktų leidėjas, priimdamas direktyvą, pažeidė proporcingumo principą. Net jeigu direktyva gali būti tinkama siekiant reikiamo tikslo, „plataus masto ir ypač rimtas direktyvoje nustatytas

799 EDAPP (2011 m.), *2011 m. gegužės 31 d. nuomonė dėl Duomenų saugojimo direktyvos (Direktyva 2006/24/EB) taikymo vertinimo ataskaitos, kurią Komisija pateikė Tarybai ir Europos Parlamentui*, 2011 m. gegužės 31 d.

800 Vokietija, Federalinis Konstitucinis Teismas (*Bundesverfassungsgericht*), 1 BvR 256/08, 2010 m. kovo 2 d.; Rumunija, Federalinis Konstitucinis Teismas (*Curtea Constituţională a României*), Nr. 1258, 2009 m. spalio 8 d.; Čekijos Respublika, Konstitucinis Teismas (Ústavní soud České republiky), 94/2011 rinkinys, 2011 m kovo 22 d.

801 ESTT, sujungtos bylos C-293/12 ir C-594/12, *Digital Rights Ireland Ltd prieš Minister for Communications, Marine and Natural Resources ir kt.* ir *Kärntner Landesregierung ir kt.* (DK), 2014 m. balandžio 8 d., 65 punktas.

pagrindinių teisių į privat[ų] gyvenim[ą] ir asmens duomenų apsaugą apribojimas nėra pakankamai apibrėžtas siekiant užtikrinti, kad apribojimas iš tikrųjų būtų susijęs su tuo, kas yra griežtai būtina“.

Jeigu nėra konkrečių duomenų saugojimą reglamentuojančių teisės aktų, duomenis leidžiama saugoti taikant telekomunikacijų duomenų konfidencialumo išimtį pagal Direktyvą 2002/58/EB (Direktyva dėl privatumo ir elektroninių ryšių)[802] ir tai turi būti prevencinė priemonė, kuria siekiama tik kovoti su sunkiais nusikaltimais. Toks saugojimas turi būti susijęs tik su tuo, kas yra griežtai būtina atsižvelgiant į saugomų duomenų kategorijas, susijusias ryšių priemones, atitinkamus asmenis ir pasirinktą saugojimo trukmę. Nacionalinės institucijos gali turėti galimybę susipažinti su saugomais duomenimis griežtomis sąlygomis, įskaitant išankstinę nepriklausomos institucijos peržiūrą. Duomenys turi būti saugomi ES.

Pavyzdys. Po sprendimo *Digital Rights Ireland* ir *Kärntner Landesregierung ir kt.*[803] bylose ESTT buvo iškeltos dar dvi bylos, susijusios su Švedijoje ir Jungtinėje Karalystėje nustatyta bendro pobūdžio elektroninių ryšių paslaugų teikėjų prievole saugoti telekomunikacijų duomenis, kaip to buvo reikalaujama pagal negaliojančia pripažintą Duomenų saugojimo direktyvą. Byloje *Tele2 Sverige* ir *Home Department prieš Tom Watson ir kt.*[804] ESTT nusprendė, kad nacionalinės teisės aktai, kuriais nustatomas bendras duomenų saugojimas be atrankos ir nereikalaujant nustatyti kokio nors santykio tarp duomenų, kurie turi būti saugomi, ir grėsmės visuomenės saugumui, taip pat nenurodant jokių konkrečių sąlygų, pavyzdžiui, saugojimo laikotarpio, geografinės vietos, asmenų, kurie gali dalyvauti darant sunkius nusikaltimus, grupės, viršija griežto būtinumo ribas ir negali būti laikomas pagrįstu demokratinėje visuomenėje, kaip to reikalaujama pagal Direktyvą 2002/58/EB, skaitant ją kartu su ES pagrindinių teisių chartija.

802 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių), OL L201, 2002.

803 ESTT, sujungtos bylos C-293/12 ir C-594/12, *Digital Rights Ireland Ltd prieš Minister for Communications, Marine and Natural Resources ir kt.* ir *Kärntner Landesregierung ir kt.* (DK), 2014 m. balandžio 8 d.

804 ESTT, sujungtos bylos C-203/15 ir C-698/15, *Tele2 Sverige AB prieš Post- och telestyrelsen* ir *Secretary of State for the Home Department prieš Tom Watson ir kt*. (DK), 2016 m. gruodžio 21 d.

Ateities perspektyvos

2017 m. sausio mėn. Europos Komisija paskelbė reglamento dėl teisės į privatų gyvenimą ir asmens duomenų apsaugos elektroninių ryšių sektoriuje pasiūlymą, kuriuo buvo siekiama panaikinti Direktyvą 2002/58/EB[805]. Pasiūlyme nėra jokių konkrečių nuostatų dėl duomenų saugojimo. Tačiau jame nustatyta, kad valstybės narės gali teisės aktais apriboti tam tikras prievoles ir teises pagal reglamentą, kai toks apribojimas yra būtina ir proporcinga priemonė siekiant apsaugoti konkrečius viešuosius interesus, įskaitant nacionalinį saugumą, gynybą, visuomenės saugumą ir nusikalstamų veikų prevenciją, tyrimą, nustatymą ar traukimą baudžiamojon atsakomybėn už jas arba baudžiamųjų sankcijų vykdymą[806]. Todėl valstybės narės galėtų išlaikyti arba sukurti nacionalines duomenų saugojimo sistemas, kuriose būtų numatytos tikslinės saugojimo priemonės, jei tokios sistemos atitinka Sąjungos teisę, atsižvelgiant į ESTT praktiką dėl E. privatumo direktyvos ir ES pagrindinių teisių chartijos aiškinimo[807]. Rengiant vadovą, vyko diskusijos dėl reglamento priėmimo.

ES ir JAV bendrasis susitarimas dėl asmens duomenų, kuriais keičiamasi teisėsaugos tikslais, apsaugos

2017 m. vasario 1 d. įsigaliojo ES ir JAV bendrasis susitarimas su JAV dėl asmens duomenų tvarkymo nusikalstamų veikų prevencijos, tyrimo, nustatymo ir baudžiamojo persekiojimo už jas tikslais[808]. ES ir JAV bendruoju susitarimu siekiama užtikrinti aukšto lygio ES piliečių duomenų apsaugą, kartu skatinant ES ir JAV teisėsaugos institucijų bendradarbiavimą. Jis papildo dabartinius ES ir JAV ir valstybių narių ir JAV susitarimus tarp teisėsaugos institucijų ir padeda nustatyti aiškias ir suderintas duomenų apsaugos taisykles, skirtas būsimiems šios srities susitarimams. Šiuo atžvilgiu susitarimu siekiama nustatyti ilgalaikį teisinį pagrindą, kuris palengvintų keitimąsi informacija.

Pačiame susitarime nenumatytas tinkamas keitimosi asmens duomenimis teisinis pagrindas, vietoje to, jame atitinkamiems asmenims pateikiamos tinkamos

805 Europos Komisija (2017 m.), *Pasiūlymas dėl Europos Parlamento ir Tarybos reglamento dėl teisės į privatų gyvenimą ir asmens duomenų apsaugos elektroninių ryšių sektoriuje, kuriuo panaikinama Direktyva 2002/58/EB (Reglamentas dėl privatumo ir elektroninių ryšių)*, COM(2017) 10 *final*, Briuselis, 2017 m. sausio 10 d.

806 *Ten pat*, 26 konstatuojamoji dalis.

807 Žr. Pasiūlymo dėl Reglamento dėl privatumo ir elektroninių ryšių aiškinamojo memorandumo COM(2017) 10 *final* 1.3 punktą.

808 Žr. ES Taryba (2016 m.), „*Enhanced data protection rights for EU citizens in law enforcement cooperation: EU and US sign Umbrella agreement*“, pranešimas spaudai 305/16, 2016 m. birželio 2 d.

duomenų apsaugos priemonės. Jis taikomas visoms asmens duomenų tvarkymo operacijoms, kurios yra būtinos nusikalstamų veikų, įskaitant terorizmą, prevencijos, tyrimo, nustatymo ir baudžiamojo persekiojimo už jas tikslais[809].

Susitarime nustatytos įvairios apsaugos priemonės, kuriomis užtikrinama, kad asmens duomenys būtų naudojami tik susitarime nurodytais tikslais. Visų pirma jame nustatyta tokia ES piliečių apsauga:

- asmens duomenys gali būti naudojami tik nusikalstamų veikų prevencijos, tyrimo, nustatymo ar traukimo baudžiamojon atsakomybėn už jas tikslais;
- apsauga nuo savavališkos ir nepateisinamos diskriminacijos;
- bet koks tolesnis duomenų perdavimas ne JAV, ne ES šaliai ar tarptautinei organizacijai turi būti vykdomas gavus išankstinį duomenis perdavusios šalies kompetentingos institucijos sutikimą;
- asmens duomenys turi būti saugomi atsižvelgiant į jų tikslumą, aktualumą, savalaikiškumą ir išsamumą;
- turi būti užtikrinamas duomenų tvarkymo saugumas, įskaitant pranešimą apie asmens duomenų saugumo pažeidimus;
- tvarkyti neskelbtinus duomenis leidžiama tik taikant tinkamas apsaugos priemones pagal teisės aktus;
- asmens duomenys negali būti saugomi ilgiau nei būtina ar tinkama;
- bet kuris asmuo turi teisę susipažinti su savo asmens duomenimis, laikydamasis tam tikrų sąlygų, ir galės prašyti, kad duomenys būtų ištaisyti, jei jie netikslūs;
- automatizuotiems sprendimams priimti reikia tinkamų apsaugos priemonių, įskaitant galimybę įsikišti žmogui;

809 2016 m. gegužės 18 d. Jungtinių Amerikos Valstijų ir Europos Sąjungos susitarimo dėl su nusikalstamų veikų prevencija, tyrimu, atskleidimu ir baudžiamuoju persekiojimu susijusios asmeninio pobūdžio informacijos apsaugos (originali versija anglų k.), 8557/16, 3 straipsnio 1 dalis. Taip pat žr. 2010 m. gegužės 26 d. Komisijos pranešimą apie ES ir JAV derybas dėl duomenų apsaugos susitarimo, MEMO/10/216, ir 2010 m. gegužės 26 d. ES Komisijos pranešimą spaudai (2010 m.) dėl aukštų privatumo standartų ES ir JAV duomenų apsaugos susitarime, IP/10/609.

- veiksminga priežiūra, įskaitant ES ir JAV priežiūros institucijų bendradarbiavimą, ir

- teisių gynimas teismine tvarka ir vykdytinumas: ES piliečiai turi teisę[810] kreiptis į JAV teismus dėl teisių gynimo tais atvejais, kai JAV valdžios institucijos atsisako leisti susipažinti su jų asmens duomenimis, juos ištaisyti arba neteisėtai atskleidžia.

Pagal bendrąjį susitarimą taip pat sukurta sistema, kurią naudojant valstybės narės, kurioje yra nukentėję asmenys, kompetentingai priežiūros institucijai prireikus pranešama apie bet kokius duomenų saugumo pažeidimus. Susitarime numatytomis teisinėmis apsaugos priemonėmis užtikrinamas vienodas požiūris į ES piliečius JAV tais atvejais, kai pažeidžiamas privatumas[811].

8.3.1. Duomenų apsauga ES teisminėse ir teisėsaugos agentūrose

Europolas

ES teisėsaugos institucijos Europolo būstinė yra Hagoje ir jis turi nacionalinius Europolo padalinius kiekvienoje valstybėje narėje. Europolas buvo įsteigtas 1998 m.; dabartinis jo, kaip ES institucijos, teisinis statusas yra pagrįstas Reglamentu dėl Europos Sąjungos teisėsaugos bendradarbiavimo agentūros (Europolo reglamentas)[812]. Europolo tikslas – padėti vykdyti organizuoto nusikalstamumo, terorizmo ir kitų sunkių nusikaltimų formų, išvardytų Europolo reglamento I priede ir darančių poveikį dviem ar daugiau valstybių narių, prevenciją ir tyrimą. Jis tai daro keisdamasis informacija ir veikdamas kaip ES informacijos centras, teikiantis žvalgybos analizę ir grėsmių vertinimą.

810 JAV teisminio teisių gynimo įstatymą 2016 m. vasario 24 d. pasirašė prezidentas B. Obama.

811 Europos duomenų apsaugos priežiūros pareigūnas priėmė nuomonę dėl ES ir JAV susitarimo, kurioje, be kita ko, rekomendavo atlikti šiuos pakeitimus: 1) įterpti straipsnį, susijusį su duomenų saugojimu ne ilgiau nei būtina ir tinkama, įterpti žodžius „konkrečiais tikslais, kuriais jie buvo perduoti“, ir 2) išskyrus didelio masto neskelbtinų duomenų perdavimą, kuris gali būti įmanomas. Žr. Europos duomenų apsaugos priežiūros pareigūno Nuomonės Nr. 1/2016, *Preliminari nuomonė dėl Jungtinių Amerikos Valstijų ir Europos Sąjungos susitarimo dėl asmeninės informacijos, susijusios su nusikalstamų veikų prevencija, tyrimu, nustatymu ir baudžiamuoju persekiojimu*, 35 punktą.

812 2016 m. gegužės 11 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/794 dėl Europos Sąjungos teisėsaugos bendradarbiavimo agentūros (Europolo), kuriuo pakeičiami ir panaikinami Tarybos sprendimai 2009/371/TVR, 2009/934/TVR, 2009/935/TVR, 2009/936/TVR ir 2009/968/TVR, OL L 135, 2016, p. 53.

Kad pasiektų savo tikslus, Europolas sukūrė Europolo informacinę sistemą, kuri suteikia valstybėms narėms duomenų bazę, kurioje jos gali keistis kriminalinės žvalgybos informacija ir informacija per savo nacionalinius padalinius. Europolo informacinė sistema gali būti naudojama duomenims, susijusiems su asmenimis, kurie yra įtariamieji arba kurie buvo nuteisti už Europolo kompetencijai priklausančią nusikalstamą veiką, arba asmenimis, dėl kurių yra faktinių požymių, kad jie padarys tokias nusikalstamas veikas. Europolas ir nacionaliniai Europolo padaliniai gali įvesti duomenis tiesiogiai į Europolo informacinę sistemą ir iš jos gauti duomenis. Duomenis keisti, taisyti arba ištrinti gali tik juos įrašiusi šalis. ES įstaigos, trečiosios šalys ir tarptautinės organizacijos taip pat gali teikti informaciją Europolui.

Informaciją, įskaitant asmens duomenis, Europolas taip pat gali gauti iš viešai prieinamų šaltinių, pavyzdžiui, interneto. Perduoti asmens duomenis ES įstaigoms leidžiama tik tuo atveju, jei tai būtina Europolo arba duomenis gaunančios ES įstaigos užduotims atlikti. Perduoti asmens duomenis trečiosioms šalims arba tarptautinėms organizacijoms leidžiama tik tuo atveju, jei Europos Komisija nusprendžia, kad atitinkama šalis arba tarptautinė organizacija užtikrina tinkamą duomenų apsaugos lygį (sprendimas dėl tinkamumo), arba jei yra sudarytas tarptautinis arba bendradarbiavimo susitarimas. Europolas gali gauti ir tvarkyti asmens duomenis iš privačių šalių ir privačių asmenų, laikydamasis griežtų sąlygų, kad tuos duomenis perduotų nacionalinis padalinys pagal savo nacionalinę teisę, trečiosios šalies kontaktinis asmuo arba tarptautinė organizacija, su kuria bendradarbiaujama pagal bendradarbiavimo susitarimą, arba trečiosios šalies institucija arba tarptautinė organizacija, su kuria priimtas sprendimas dėl tinkamumo arba su kuria ES yra sudariusi tarptautinį susitarimą. Visa informacija keičiamasi per Saugaus keitimosi informacija tinklo programą (SIENA).

Reaguojant į naujus pokyčius Europole įsteigti specializuoti centrai. 2013 m. Europole įsteigtas Europos kovos su elektroniniu nusikalstamumu centras[813]. Tai ES informacijos apie elektroninius nusikaltimus centras, kuris padeda greičiau reaguoti į internete daromus nusikaltimus, kurti ir diegti skaitmeninius teismo ekspertinius gebėjimus ir užtikrinti, kad tiriant elektroninius nusikaltimus būtų vadovaujamasi geriausia patirtimi. Centre daugiausia dėmesio skiriama elektroniniams nusikaltimams:

- kuriuos padaro organizuotos grupės, siekdamos gauti didelį nusikalstamą pelną, pavyzdžiui, sukčiavimas internetu;

813 Taip pat žr. EDAPP (2012 m.), *Duomenų apsaugos priežiūros pareigūno nuomonė dėl Europos Komisijos komunikato Tarybai ir Europos Parlamentui dėl Europos kovos su elektroniniu nusikalstamumu centro įsteigimo*, Briuselis, 2012 m. birželio 29 d.

- kurie sukelia didelę žalą aukai, pavyzdžiui, vaikų seksualinis išnaudojimas internetu;

- kurie daro poveikį ypatingos svarbos infrastruktūros objektams ar informacinėms sistemoms ES.

2016 m. sausio mėn. įsteigtas Europos kovos su terorizmu centras (ECTC), kurio paskirtis – teikti operatyvinę paramą valstybėms narėms atliekant su teroristiniais nusikaltimais susijusius tyrimus. Jis tiesiogiai sutikrina operatyvinius duomenis su Europolo jau turimais duomenimis, greitai atskleisdamas finansinę informaciją, ir analizuoja visus turimus tyrimo duomenis, kad padėtų susidaryti struktūruotą vaizdą apie teroristų tinklą[814].

Po 2015 m. lapkričio mėn. įvykusio Tarybos posėdžio 2016 m. vasario mėn. įsteigtas Europos kovos su neteisėtu migrantų gabenimu centras (EMSC), kurio tikslas – padėti valstybėms narėms kovoti su neteisėtu migrantų gabenimu užsiimančiais nusikaltėlių tinklais ir juos išardyti. Jis veikia kaip informacijos centras, teikiantis paramą ES regioniniams specialiosios paskirties biurams Katanijoje (Italijoje) ir Pirėjuje (Graikijoje), kurie padeda nacionalinėms valdžios institucijoms keliose srityse, įskaitant dalijimąsi žvalgybos informacija, nusikalstamų veikų tyrimus ir nusikaltėlių neteisėto žmonių gabenimo tinklų baudžiamąjį persekiojimą[815].

Duomenų apsaugos tvarka, kuria remiantis reglamentuojama Europolo veikla, sustiprinama ir grindžiama ES institucijų duomenų apsaugos reglamento[816] principais ir yra suderinama su Duomenų apsaugos policijos ir baudžiamosios teisenos institucijoms tvarkant asmens duomenis direktyva, atnaujinta 108-ąja konvencija ir Rekomendacija dėl policijos.

Tvarkyti nusikalstamos veikos aukų, liudytojų ar kitų asmenų, galinčių suteikti informacijos apie nusikalstamas veikas, arba jaunesnių nei 18 metų asmenų asmens duomenis leidžiama, jei tai tikrai būtina ir proporcinga nusikaltimų, patenkančių į Europolo tikslų sritį, prevencijai ir kovai su jais[817]. Neskelbtinų asmens duomenų tvarkymas draudžiamas, išskyrus atvejus, kai tai tikrai būtina ir proporcinga

814 Žr. Europolo svetainės tinklalapį apie ECTC.

815 Žr. Europolo svetainės tinklalapį apie EMSC.

816 2000 m. gruodžio 18 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 45/2001 dėl asmenų apsaugos Bendrijos institucijoms ir įstaigoms tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo, OL L 8, 2001.

817 Europolo reglamento 30 straipsnio 1 dalis.

nusikaltimų, patenkančių į Europolo tikslų sritį, prevencijos ir kovos su jais tikslais ir kai tie duomenys papildo kitus Europolo tvarkomus asmens duomenis[818]. Abiem šiais atvejais su atitinkamais duomenimis gali susipažinti tik Europolas[819].

Duomenis saugoti leidžiama tik būtiną ir proporcingą laikotarpį, o tolesnis duomenų saugojimas peržiūrimas kas trejus metus, be to, duomenys automatiškai ištrinami[820].

Tam tikromis sąlygomis Europolui leidžiama perduoti asmens duomenis ES įstaigai arba trečiosios šalies institucijai, arba tiesiogiai tarptautinei organizacijai[821]. Apie duomenų saugumo pažeidimus, jeigu tikėtina, kad jie turės rimtą neigiamą poveikį atitinkamų duomenų subjektų teisėms ir laisvėms, duomenų subjektus reikia informuoti nepagrįstai nedelsiant[822]. Valstybės narės lygmeniu bus paskirta nacionalinė priežiūros institucija, kuri stebės, kaip Europolas tvarko asmens duomenis[823].

EDAPP yra atsakingas už fizinių asmenų pagrindinių teisių ir laisvių apsaugos Europolui tvarkant asmens duomenis stebėseną ir užtikrinimą, taip pat už Europolo ir duomenų subjektų konsultavimą visais su asmens duomenų tvarkymu susijusiais klausimais. Šiuo tikslu EDAPP veikia kaip tyrimo ir skundų įstaiga ir glaudžiai bendradarbiauja su nacionalinėmis priežiūros institucijomis[824]. EDAPP ir nacionalinės priežiūros institucijos susitinka ne rečiau kaip du kartus per metus bendradarbiavimo valdyboje, kurioje atlieka patariamąją funkciją[825]. Valstybės narės yra įpareigotos įstatymu įsteigti priežiūros instituciją, kuri turėtų kompetenciją vykdyti valstybės narės vykdomo asmens duomenų perdavimo, išgavimo ir pateikimo Europolui teisėtumo stebėseną[826]. Valstybių narių taip pat reikalaujama užtikrinti, kad nacionalinė priežiūros institucija, vykdydama savo užduotis ir pareigas pagal Europolo reglamentą, galėtų veikti visiškai nepriklausomai[827]. Siekdamas patikrinti duomenų tvarkymo teisėtumą, savarankiškai stebėti savo veiklą ir užtikrinti duomenų vientisumą ir saugumą, Europolas saugo savo duomenų tvarkymo veiklos registracijos įrašus arba dokumentus.

818 *Ten pat*, 30 straipsnio 2 dalis.
819 *Ten pat*, 30 straipsnio 3 dalis.
820 *Ten pat*, 31 straipsnis.
821 *Ten pat*, atitinkamai 24 ir 25 straipsniai.
822 *Ten pat*, 35 straipsnis.
823 Europolo reglamento 42 straipsnis.
824 *Ten pat*, 43 ir 44 straipsniai.
825 *Ten pat*, 45 straipsnis.
826 *Ten pat*, 42 straipsnio 1 punktas.
827 *Ten pat*, 42 straipsnio 1 punktas.

Šiuose registracijos įrašuose pateikiama informacija apie duomenų tvarkymo operacijas automatizuotose duomenų tvarkymo sistemose, susijusiose su duomenų rinkimu, keitimu, paieška, atskleidimu, sujungimu ir ištrynimu[828].

EDAPP sprendimas gali būti apskųstas ESTT[829]. Bet kuris asmuo, kuris dėl neteisėto duomenų tvarkymo operacijos patyrė žalos, turi teisę gauti kompensaciją už patirtą žalą iš Europolo arba kitos atsakingos valstybės narės, šiuo tikslu pirmuoju atveju pareikšdamas ieškinį ESTT arba antruoju atveju kompetentingame nacionaliniame teisme[830]. Be to, Europolo veiklą gali tikrinti specializuota nacionalinių parlamentų ir Europos Parlamento jungtinė parlamentinės kontrolės grupė (JPKG)[831]. Kiekvienas asmuo turi teisę susipažinti su bet kuriais asmens duomenimis, kuriuos apie jį gali turėti Europolas, be to, kiekvienas asmuo turi teisę prašyti, kad šie asmens duomenys būtų patikrinti, ištaisyti arba ištrinti. Šioms teisėms gali būti taikomos išimtys ir apribojimai.

Eurojustas

2002 m. įsteigtas Eurojustas yra ES įstaiga, jos būstinė yra Hagoje. Jis skatina teisminį bendradarbiavimą tiriant sunkius nusikaltimus, susijusius su bent dviem valstybėmis narėmis, ir vykdant baudžiamąjį persekiojimą[832]. Eurojustui suteikiama kompetencija:

- skatinti ir gerinti įvairių valstybių narių kompetentingų institucijų vykdomus tyrimus ir baudžiamuosius persekiojimus;

- palengvinti su teisminiu bendradarbiavimu susijusių prašymų ir sprendimų vykdymą.

Eurojusto funkcijas vykdo nacionaliniai nariai. Kiekviena valstybė narė į Eurojustą deleguoja vieną teisėją arba prokurorą, kuriam taikoma nacionalinė teisė ir

828 *Ten pat*, 40 straipsnis.

829 *Ten pat*, 48 straipsnis.

830 *Ten pat*, 50 straipsnis.

831 *Ten pat*, 51 straipsnis.

832 Europos Sąjungos Taryba (2002 m.), 2002 m. vasario 28 d. Tarybos sprendimas 2002/187/TVR, įkuriantis Eurojustą siekiant sustiprinti kovą su sunkiais nusikaltimais, OL L 63, 2002; Europos Sąjungos Taryba (2003 m.), 2003 m. birželio 18 d. Tarybos sprendimas 2003/659/TVR, iš dalies keičiantis Sprendimą 2002/187/TVR, įkuriantį Eurojustą siekiant sustiprinti kovą su sunkiais nusikaltimais, OL L 44, 2003; Europos Sąjungos Taryba (2009 m.), 2008 m. gruodžio 16 d. Tarybos sprendimas 2009/426/EB dėl Eurojusto stiprinimo ir iš dalies keičiantis Sprendimą 2002/187/TVR, įkuriantį Eurojustą siekiant sustiprinti kovą su sunkiais nusikaltimais, OL L 138, 2009 (Sprendimai dėl Eurojusto).

suteikiama būtina kompetencija atlikti užduotis, kurios yra būtinos siekiant skatinti ir gerinti teisminį bendradarbiavimą. Be to, nacionaliniai nariai kartu veikia kaip kolegija, vykdanti specialias Eurojusto užduotis.

Eurojustas asmens duomenis gali tvarkyti tiek, kiek tai būtina jo tikslams pasiekti. Tačiau toks tvarkymas apima tik konkrečią informaciją apie asmenis, kurie įtariami padarę, dalyvavę padarant nusikalstamą veiką, kuri priklauso Eurojusto kompetencijai, arba už ją nuteisti. Eurojustas taip pat gali tvarkyti tam tikrą informaciją, susijusią su Eurojusto kompetencijai priklausančių nusikalstamų veikų liudytojais arba aukomis[833]. Išimtinėmis aplinkybėmis Eurojustas ribotą laikotarpį gali tvarkyti daugiau asmens duomenų, susijusių su nusikalstamos veikos aplinkybėmis, kai tokie duomenys yra tiesiogiai susiję su vykdomu tyrimu. Atsižvelgdamas į savo kompetenciją, Eurojustas gali bendradarbiauti su kitomis ES institucijomis, įstaigomis ir agentūromis ir keistis su jomis informacija. Eurojustas taip pat gali bendradarbiauti ir keistis duomenimis su trečiosiomis šalimis ir organizacijomis.

Duomenų apsaugos srityje Eurojustas privalo garantuoti tokį apsaugos lygį, kuris būtų bent jau lygiavertis atnaujintos Konvencijos Nr. 108 principams ir jos paskesniems pakeitimams. Jei keičiamasi duomenimis, privalu laikytis konkrečių taisyklių ir apribojimų, kurie nustatomi bendradarbiavimo susitarime arba darbo susitarime pagal Eurojusto tarybos sprendimus ir Eurojusto duomenų apsaugos taisykles[834].

Eurojuste sukurta nepriklausoma jungtinė priežiūros institucija (JSB), kurios užduotis – stebėti, kaip Eurojustas tvarko asmens duomenis. Asmenys jungtinei priežiūros institucijai gali pateikti skundus, jei jų netenkina Eurojusto sprendimas dėl prašymo leisti susipažinti su asmens duomenimis, juos ištaisyti, užblokuoti arba ištrinti. Jei Eurojustas asmens duomenis tvarko neteisėtai, jis laikomas atsakingu už bet kokią duomenų subjektui padarytą žalą pagal valstybės narės, kurioje yra jo būstinė, t. y. Nyderlandų, nacionalinę teisę.

Ateities perspektyvos

2013 m. liepos mėn. Europos Komisija pateikė reglamento dėl Eurojusto reformos pasiūlymą. Prie pasiūlymo buvo pridėtas pasiūlymas įsteigti Europos prokuratūrą (žr. toliau). Šiuo reglamentu siekiama supaprastinti funkcijas ir struktūrą, kad jos atitiktų

833 Tarybos sprendimo 2002/187/TVR, iš dalies pakeisto Tarybos sprendimu 2003/659/TVR ir Tarybos sprendimu 2009/426/TVR, suvestinės redakcijos 15 straipsnio 2 dalis.

834 Asmens duomenų tvarkymo ir apsaugos Eurojuste darbo tvarkos taisyklės, OL C 68/01, 2005, 2005 m. kovo 19 d., p. 1.

Lisabonos sutartį. Be to, reformos tikslas – aiškiai atskirti Eurojusto kolegijos vykdomas Eurojusto veiklos užduotis ir jo administracines užduotis. Tai taip pat leis valstybėms narėms daugiau dėmesio skirti operatyvinėms užduotims. Bus įsteigta nauja vykdomoji valdyba, kuri padės kolegijai vykdyti administracines užduotis[835].

Europos prokuratūra

Valstybės narės turi išimtinę kompetenciją vykdyti baudžiamąjį persekiojimą už nusikalstamas veikas, susijusias su sukčiavimu ir netinkamu ES biudžeto vykdymu, kurie taip pat gali turėti tarpvalstybinį poveikį. Padidėjo tokių nusikaltimų vykdytojų tyrimo, baudžiamojo persekiojimo ir patraukimo baudžiamojon atsakomybėn svarba, ypač atsižvelgiant į tebesitęsiančią ekonomikos krizę[836]. Europos Komisija pasiūlė Reglamentą dėl nepriklausomos Europos prokuratūros[837] įsteigimo siekiant kovoti su ES finansiniams interesams kenkiančiomis nusikalstamomis veikomis. Europos prokuratūra bus įsteigta taikant tvirtesnio bendradarbiavimo procedūrą, pagal kurią ne mažiau kaip devynios valstybės narės galės pradėti pažangų bendradarbiavimą tam tikroje srityje ES struktūrose, nedalyvaujant kitoms ES šalims[838]. Prie tvirtesnio bendradarbiavimo prisijungė Belgija, Bulgarija, Čekija, Estija, Graikija, Ispanija, Kipras, Kroatija, Latvija, Lietuva, Liuksemburgas, Portugalija, Prancūzija, Rumunija, Slovėnija, Slovakija, Suomija ir Vokietija; Austrija ir Italija išreiškė ketinimą prisijungti[839].

Europos prokuratūra bus kompetentinga tirti ES sukčiavimo ir kitus ES finansiniams interesams kenkiančius nusikaltimus ir vykdyti baudžiamąjį persekiojimą už juos, siekdama veiksmingai koordinuoti tyrimus ir baudžiamąjį persekiojimą įvairiose nacionalinėse teisinėse sistemose ir gerinti išteklių naudojimą bei keitimąsi informacija Europos lygmeniu[840].

835 Žr. Europos Komisijos svetainės tinklalapį apie Eurojustą.

836 Žr. Europos Komisijos (2013 m.) Pasiūlymą dėl Tarybos reglamento dėl Europos prokuratūros įsteigimo, COM(2013) 534 *final*, Briuselis, 2013 m. liepos 17 d., p. 1, ir Komisijos svetainės tinklalapį apie Europos prokuratūrą.

837 Europos Komisija (2013), Pasiūlymas dėl Tarybos reglamento dėl Europos prokuratūros įsteigimo, COM(2013) 534 *final*, Briuselis, 2013 m. liepos 17 d.

838 Sutarties dėl ES veikimo 86 straipsnio 1 dalis ir 329 straipsnio 1 dalis.

839 Žr. Europos Sąjungos Tarybos (2017 m.) pranešimą spaudai *„20 valstybių narių susitarė dėl Europos prokuratūros įsteigimo konkrečių aspektų“*, 2017 m. birželio 8 d.

840 Europos Komisija (2013 m.), Pasiūlymas dėl Tarybos reglamento dėl Europos prokuratūros įsteigimo, COM(2013) 534 *final*, Briuselis, 2013 m. liepos 17 d., p. 1 ir 51. Taip pat žr. Komisijos svetainės tinklalapį apie Europos prokuratūrą.

Europos prokuratūrai vadovaus Europos prokuroras, o kiekvienoje valstybėje narėje bus bent vienas įgaliotasis Europos prokuroras, atsakingas už tyrimų ir baudžiamojo persekiojimo vykdymą toje valstybėje narėje.

Pasiūlyme nustatytos griežtos apsaugos priemonės, kuriomis užtikrinamos Europos prokuratūros tyrimuose dalyvaujančių asmenų teisės, kaip nustatyta nacionalinėje teisėje, ES teisėje ir ES pagrindinių teisių chartijoje. Tyrimo priemonėms, kurios iš esmės yra susijusios su pagrindinėmis teisėmis, būtina gauti išankstinį nacionalinio teismo leidimą[841]. Nacionaliniai teismai atliks Europos prokuratūros tyrimų teisminę peržiūrą[842].

ES institucijų duomenų apsaugos reglamentas[843] bus taikomas Europos prokuratūros atliekamam administraciniam asmens duomenų tvarkymui. Tvarkant su operatyviniais klausimais susijusius asmens duomenis, pavyzdžiui, tai Europolo duomenų tvarkymas, Europos prokuratūrai bus taikoma atskira duomenų apsaugos tvarka, panaši į tą, kuri taikoma Europolo ir Eurojusto veiklai, atsižvelgiant į tai, kad Europos prokuratūros funkcijų vykdymas apims asmens duomenų tvarkymą teisėsaugos ir baudžiamojo persekiojimo institucijose valstybių narių lygmeniu. Todėl Europos prokuratūros duomenų apsaugos taisyklės yra beveik identiškos Duomenų apsaugos policijos ir baudžiamosios teisenos institucijoms tvarkant asmens duomenis direktyvoje nustatytoms taisyklėms. Pagal pasiūlymą dėl Europos prokuratūros įsteigimo asmens duomenys turi būti tvarkomi laikantis teisėtumo ir sąžiningumo, tikslų apribojimo, duomenų kiekio mažinimo, tikslumo, vientisumo ir konfidencialumo principų. Europos prokuratūra turi kiek įmanoma aiškiai atskirti skirtingų rūšių duomenų subjektų, pavyzdžiui, asmenų, nuteistų už nusikalstamą veiką, asmenų, kurie yra tik įtariamieji, aukų ir liudytojų, asmens duomenis. Juo taip pat turi būti siekiama patikrinti tvarkomų asmens duomenų kokybę ir kuo labiau atskirti faktais pagrįstus asmens duomenis nuo asmeniniais vertinimais pagrįstų asmens duomenų.

Į pasiūlymą įtrauktos nuostatos dėl duomenų subjektų teisių, visų pirma teisės gauti informaciją, susipažinti su savo asmens duomenimis, juos ištaisyti, ištrinti ir apriboti jų tvarkymą, ir numatyta, kad tokiomis teisėmis taip pat gali būti naudojamasi netiesiogiai per EDAPP. Jame taip pat įtvirtinti duomenų tvarkymo saugumo ir

841 Pasiūlymas dėl Tarybos reglamento dėl Europos prokuratūros įsteigimo, COM(2013) 534 *final*, Briuselis, 2013 m. liepos 17 d., 26 straipsnio 4 dalis.

842 *Ten pat*, 36 straipsnis.

843 2000 m. gruodžio 18 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 45/2001 dėl asmenų apsaugos Bendrijos institucijoms ir įstaigoms tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo, OL L 8, 2001.

atskaitomybės principai, pagal kuriuos reikalaujama, kad Europos prokuratūra įgyvendintų tinkamas technines ir organizacines priemones, kad užtikrintų duomenų tvarkymo keliamą riziką atitinkantį saugumo lygį, registruotų visą duomenų tvarkymo veiklą ir prieš pradėdama tvarkyti duomenis atliktų poveikio duomenų apsaugai vertinimą, kai dėl tam tikros rūšies duomenų tvarkymo (pavyzdžiui, duomenų tvarkymo naudojant naujas technologijas) gali kilti didelis pavojus asmenų teisėms. Galiausiai pasiūlyme numatyta, kad kolegija paskiria duomenų apsaugos pareigūną, kuris turi tinkamai dalyvauti sprendžiant visus su asmens duomenų apsauga susijusius klausimus ir užtikrinti, kad Europos prokuratūra laikytųsi taikytinų duomenų apsaugos teisės aktų.

8.3.2. Duomenų apsauga ES lygmens bendrose informacinėse sistemose

Be valstybių narių keitimosi duomenimis ir specializuotų ES institucijų, kovojančių su tarpvalstybiniu nusikalstamumu, pavyzdžiui, Europolo, Eurojusto ir Europos prokuratūros, sukūrimo, ES lygmeniu sukurtos kelios bendros informacinės sistemos, kad būtų sudarytos sąlygos ir palengvintas kompetentingų nacionalinių ir ES institucijų bendradarbiavimas ir keitimasis duomenimis konkrečiais tikslais sienų apsaugos, imigracijos, prieglobsčio ir muitinės srityse. Kadangi Šengeno erdvė iš pradžių buvo sukurta tarptautiniu susitarimu, kuris veikė nepriklausomai nuo ES teisės, Šengeno informacinė sistema (SIS) buvo sukurta iš daugiašalių susitarimų ir vėliau įtraukta į ES teisę. Vizų informacinė sistema (VIS), sistema EURODAC, EUROSUR ir Muitinės informacinė sistema (MIS) buvo sukurtos kaip pagal ES teisę reglamentuojamos priemonės.

Šių sistemų bendrą priežiūrą vykdo nacionalinės priežiūros institucijos ir EDAPP. Siekdamos užtikrinti aukšto lygio apsaugą, šios institucijos bendradarbiauja priežiūros koordinavimo grupėse, kurios yra susijusios su šiomis didelės apimties IT sistemomis: 1) sistema EURODAC; 2) Vizų informacine sistema; 3) Šengeno informacine sistema; 4) Muitinės informacine sistema ir 5) Vidaus rinkos informacine sistema[844]. Priežiūros koordinavimo grupės paprastai posėdžiauja du kartus per metus, vadovaujant išrinktam pirmininkui, ir priima gaires, aptaria tarpvalstybinius atvejus arba patvirtina bendras patikrinimų sistemas.

844 Žr. Europos duomenų apsaugos priežiūros pareigūno svetainės tinklalapį apie priežiūros koordinavimą.

2012 m. įkurta Europos Sąjungos didelės apimties IT sistemų laisvės, saugumo ir teisingumo erdvėje operacijų valdymo agentūra (eu-LISA)[845] atsako už antrosios kartos Šengeno informacinės sistemos (SIS II), Vizų informacinės sistemos (VIS) ir sistemos EURODAC operacijų valdymą. Pagrindinė eu-LISA užduotis – užtikrinti veiksmingą, saugų ir nuolatinį informacinių technologijų sistemų valdymą. Ji taip pat yra atsakinga už būtinų priemonių nustatymą siekiant užtikrinti sistemų ir duomenų saugumą.

Šengeno informacinė sistema

1985 m. keletas buvusiosios Europos bendrijos valstybių narių sudarė Beniliukso ekonominės sąjungos valstybių, Vokietijos ir Prancūzijos susitarimą dėl laipsniško jų bendrų sienų kontrolės panaikinimo (Šengeno susitarimas), kuriuo siekiama sukurti laisvo asmenų judėjimo erdvę, kuriai netrukdytų sienų kontrolė Šengeno teritorijoje[846]. Siekiant atsverti grėsmę visuomenės saugumui, kuri gali kilti dėl atvirų sienų, buvo nustatyta sustiprinta sienų kontrolė prie Šengeno erdvės išorės sienų, taip pat glaudus nacionalinių policijos ir teisingumo institucijų bendradarbiavimas.

Prie Šengeno susitarimo prisijungus kitoms valstybėms, Amsterdamo sutartimi Šengeno sistema galiausiai buvo integruota į ES teisinę sistemą[847]. Šis sprendimas įgyvendintas 1999 m. Naujausia Šengeno informacinė sistema, vadinamoji SIS II, pradėjo veikti 2013 m. balandžio 9 d. Dabar ją naudoja dauguma ES valstybių narių[848], taip pat Islandija, Lichtenšteinas, Norvegija ir Šveicarija[849]. Europolas ir Eurojustas taip pat turi prieigą prie SIS II.

SIS II sudaro centrinė sistema (C-SIS), kiekvienos valstybės narės nacionalinė sistema (N-SIS) ir ryšių perdavimo tarp centrinės sistemos ir nacionalinių sistemų

845 2011 m. spalio 25 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 1077/2011, kuriuo įsteigiama didelės apimties IT sistemų laisvės, saugumo ir teisingumo erdvėje operacijų valdymo agentūra, OL L 286, 2011.

846 Susitarimas tarp Beniliukso ekonominės sąjungos valstybių, Vokietijos Federacinės Respublikos ir Prancūzijos Respublikos vyriausybių dėl laipsniško jų bendrų sienų kontrolės panaikinimo, OL L 239, 2000.

847 Europos Bendrijos (1997 m.), Amsterdamo sutartis, iš dalies keičianti Europos Sąjungos sutartį, Europos Bendrijų steigimo sutartis ir tam tikrus susijusius aktus, OL C 340, 1997.

848 Kroatija, Kipras ir Airija vykdo parengiamąją integravimo į SIS II veiklą, tačiau dar nėra prie jos prisijungę. Žr. informaciją apie Šengeno informacinę sistemą, kuri prieinama Europos Komisijos migracijos ir vidaus reikalų generalinio direktorato svetainėje.

849 2006 m. gruodžio 20 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 1987/2006 dėl antrosios kartos Šengeno informacinės sistemos (SIS II) sukūrimo, veikimo ir naudojimo, OL L 381, 2006, ir Europos Sąjungos Taryba (2007 m.), 2007 m. birželio 12 d. Tarybos sprendimas 2007/533/TVR dėl antrosios kartos Šengeno informacinės sistemos (SIS II) sukūrimo, veikimo ir naudojimo, OL L 205, 2007.

infrastruktūra. C-SIS sudaro tam tikri valstybių narių įrašyti duomenys apie asmenis ir objektus. SIS visoje Šengeno erdvėje naudojasi nacionalinės sienų kontrolės, policijos, muitinės, vizų ir teisminės institucijos. Kiekvienoje valstybėje narėje naudojama C-SIS nacionalinė kopija, vadinama nacionaline Šengeno informacine sistema (N-SIS), kuri nuolat atnaujinama, taigi kartu atnaujinama ir C-SIS. SIS naudojami įvairių rūšių perspėjimai:

- asmuo neturi teisės atvykti į Šengeno teritoriją ar joje būti arba
- asmens arba daikto ieško teisminės arba teisėsaugos institucijos (pavyzdžiui, išduoti Europos arešto orderiai, prašymai atlikti slaptus patikrinimus), arba
- pranešama, kad asmuo yra dingęs, arba
- paskelbta apie pavogtas arba prarastas prekes, pavyzdžiui, banknotus, automobilius, krovinines transporto priemones, šaunamuosius ginklus ir tapatybės dokumentus.

Jei yra perspėjimas, tolesni veiksmai turi būti inicijuojami per SIRENE biurus. SIS II įdiegtos naujos funkcijos, pavyzdžiui, galimybė įrašyti biometrinius duomenis, pavyzdžiui, pirštų atspaudus ir nuotraukas, arba naujos perspėjimų kategorijos, pavyzdžiui, pavogti laivai, orlaiviai, konteineriai arba mokėjimo priemonės; sugriežtinti perspėjimai dėl asmenų ir daiktų; ir Europos arešto orderių (EAO) dėl asmenų, ieškomų siekiant juos suimti, perduoti ar išduoti, kopijos.

SIS II grindžiama dviem vienas kitą papildančiais aktais: SIS II sprendimu[850] ir SIS II reglamentu[851]. ES teisės aktų leidėjas, priimdamas sprendimą ir reglamentą, rėmėsi skirtingu teisiniu pagrindu. Sprendimu reglamentuojamas SIS II naudojimas policijos ir teisminio bendradarbiavimo baudžiamosiose bylose tikslais (buvęs ES trečiasis ramstis). Reglamentas taikomas perspėjimo procedūroms, susijusioms su vizų, prieglobsčio, imigracijos ir kitomis politikos sritimis, susijusiomis su laisvu asmenų judėjimu (anksčiau – pirmasis ramstis). Perspėjimo procedūros kiekvienam ramsčiui turėjo būti reglamentuojamos atskirais aktais, atsižvelgiant į tai, kad abu teisės aktai buvo priimti prieš įsigaliojant Lisabonos sutarčiai ir panaikinus ramsčių struktūrą.

850 2007 m. birželio 12 d. Tarybos sprendimas 2007/533/TVR dėl antrosios kartos Šengeno informacinės sistemos (SIS II) sukūrimo, veikimo ir naudojimo, OL L 205, 2007 m. rugpjūčio 7 d.

851 2006 m. gruodžio 20 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 1987/2006 dėl antrosios kartos Šengeno informacinės sistemos (SIS II) sukūrimo, veikimo ir naudojimo, OL L 381, 2006 m. gruodžio 28 d.

Abiejuose teisės aktuose pateikiamos duomenų apsaugos taisyklės. Pagal SIS II sprendimą draudžiama tvarkyti neskelbtinus duomenis[852]. Asmens duomenų tvarkymui taikoma atnaujinta 108-oji konvencija[853]. Be to, asmenys turi teisę susipažinti su savo asmens duomenimis, kurie įrašomi į SIS II[854].

SIS II reglamentu reglamentuojamos perspėjimų, susijusių su atsisakymu leisti atvykti ar apsigyventi ne ES piliečiams, įvedimo ir tvarkymo sąlygos ir procedūros. Jame taip pat nustatytos keitimosi papildoma informacija atvykimo į valstybę narę ar buvimo joje tikslais taisyklės[855]. Šiame reglamente taip pat pateikiamos duomenų apsaugos taisyklės. Neskelbtinų duomenų kategorijų, nurodytų Bendrojo duomenų apsaugos reglamento 9 straipsnio 1 dalyje, tvarkyti neleidžiama[856]. SIS II reglamentu duomenų subjektui taip pat suteikiamos tam tikros teisės:

- teisė susipažinti su asmens duomenimis, susijusiais su duomenų subjektu[857];
- teisė ištaisyti faktiškai netikslius duomenis[858];
- teisė ištrinti neteisėtai saugomus duomenis[859] ir
- teisė būti informuotam, jeigu dėl duomenų subjekto parengiamas perspėjimas. Informacija pateikiama raštu, prie jos pridedama kopija arba nuoroda į nacionalinį sprendimą paskelbti perspėjimą[860].

Teisė būti informuotam nenumatoma, jeigu 1) asmens duomenys nebuvo gauti iš duomenų subjekto ir tos informacijos pateikti neįmanoma arba tam reikia neproporcingų pastangų, 2) duomenų subjektas jau turi informaciją arba 3) jeigu pagal nacionalinius įstatymus leidžiama nustatyti apribojimą, remiantis, be kita ko, nacionalinio saugumo užtikrinimu arba nusikalstamų veikų prevencija[861].

852 SIS II sprendimo 56 straipsnis; SIS II reglamento 40 straipsnis.
853 SIS II reglamento 57 straipsnis.
854 SIS II sprendimo 58 straipsnis; SIS II reglamento 41 straipsnis.
855 SIS II reglamento 2 straipsnis.
856 *Ten pat*, 40 straipsnis.
857 *Ten pat*, 41 straipsnio 1 dalis.
858 *Ten pat*, 41 straipsnio 5 dalis.
859 *Ten pat*, 41 straipsnio 5 dalis.
860 *Ten pat*, 42 straipsnio 1 dalis.
861 *Ten pat*, 42 straipsnio 2 punktas.

Tiek SIS II sprendimo, tiek SIS II reglamento atveju asmenų prieigos teisėmis, susijusiomis su SIS II, gali būti naudojamasi bet kurioje valstybėje narėje ir jos bus reglamentuojamos pagal tos valstybės narės nacionalinę teisę[862].

Pavyzdys. Byloje *Dalea prieš Prancūziją*[863] pareiškėjui buvo atsisakyta išduoti vizą leisti atvykti į Prancūziją, nes Prancūzijos valdžios institucijos pranešė Šengeno informacinei sistemai, kad jam turėtų būti neleista atvykti. Pareiškėjo bandymas Prancūzijos duomenų apsaugos komisijoje, o vėliau ir Valstybės Taryboje prašyti leisti susipažinti su duomenimis ir juos ištaisyti arba ištrinti buvo nesėkmingas. EŽTT nusprendė, kad įrašas į Šengeno informacinę sistemą buvo atliktas pagal įstatymą ir juo buvo siekiama teisėto tikslo, t. y. užtikrinti nacionalinį saugumą. Kadangi pareiškėjas neįrodė žalos, kurią patyrė atsisakius jam išduoti leidimą patekti į Šengeno erdvę, be to, jis galėjo pasinaudoti tinkamomis apsaugos nuo savavališkų sprendimų priėmimo priemonėmis, jo teisės į privatų gyvenimą apribojimas buvo proporcingas. Todėl pareiškėjo skundas pagal 8 straipsnį buvo paskelbtas nepriimtinu.

Kiekvienos valstybės narės kompetentinga nacionalinė priežiūros institucija prižiūri vidaus N-SIS. Nacionalinė priežiūros institucija privalo užtikrinti, kad vidaus N-SIS atliekamų duomenų tvarkymo operacijų auditas būtų atliekamas ne rečiau kaip kas ketverius metus[864]. Nacionalinės priežiūros institucijos ir EDAPP bendradarbiauja ir užtikrina koordinuotą N-SIS priežiūrą, o EDAPP atsako už C-SIS priežiūrą. Siekiant užtikrinti skaidrumą, kas dvejus metus Europos Parlamentui, Tarybai ir eu-LISA siunčiama bendra veiklos ataskaita. SIS priežiūros koordinavimo tikslais buvo įsteigta SIS II priežiūros koordinavimo grupė, kuri posėdžiauja ne daugiau kaip du kartus per metus. Šią grupę sudaro EDAPP ir SIS II įgyvendinusių valstybių narių, taip pat Islandijos, Lichtenšteino, Norvegijos ir Šveicarijos priežiūros institucijų atstovai, nes jiems taip pat taikoma SIS, atsižvelgiant į tai, kad jie yra Šengeno erdvės nariai[865]. Kipras, Kroatija ir Airija dar neprisijungė prie SIS II, todėl dalyvauja tik kaip stebėtojai priežiūros koordinavimo grupėje. Priežiūros koordinavimo grupėje EDAPP ir nacionalinės priežiūros institucijos aktyviai bendradarbiauja keisdamiesi informacija, padėdami vieni kitiems atlikti auditus ir patikrinimus, rengdami suderintus pasiūlymus

862 SIS II reglamento 41 straipsnio 1 dalis ir SIS II sprendimo 58 straipsnis.

863 EŽTT, *Dalea prieš Prancūziją*, Nr. 964/07, 2010 m. vasario 2 d.

864 SIS II reglamento 60 straipsnio 2 dalis.

865 Žr. Europos duomenų apsaugos priežiūros pareigūno svetainės tinklalapį apie Šengeno informacinę sistemą.

dėl bendrų galimų problemų sprendimų ir didindami informuotumą apie duomenų apsaugos teises[866]. SIS II priežiūros koordinavimo grupė taip pat priima gaires, kad padėtų duomenų subjektams. Vienas iš pavyzdžių – vadovas, skirtas padėti duomenų subjektams naudotis savo prieigos teisėmis[867].

Ateities perspektyvos

2016 m. Europos Komisija atliko SIS vertinimą[868], iš kurio matyti, kad buvo įdiegti nacionaliniai mechanizmai, suteikiantys duomenų subjektams prieigą prie jų asmens duomenų SIS II, galimybę juos ištaisyti ir ištrinti arba gauti kompensaciją už netikslius duomenis. Siekdama pagerinti SIS II veiksmingumą ir efektyvumą, Europos Komisija pateikė tris pasiūlymus dėl reglamentų:

- reglamentą dėl SIS sukūrimo, veikimo ir naudojimo patikrinimams kertant sieną, kuriuo bus panaikintas SIS II reglamentas;

- reglamentą dėl SIS sukūrimo, eksploatavimo ir naudojimo policijos bendradarbiavimui ir teisminiam bendradarbiavimui baudžiamosiose bylose, kuriuo, be kita ko, bus panaikintas SIS II sprendimas, ir

- reglamentą dėl SIS naudojimo neteisėtai esančių trečiųjų šalių piliečių grąžinimui.

Svarbu tai, kad pasiūlymuose leidžiama tvarkyti ne tik nuotraukas ir pirštų atspaudus, bet ir kitų kategorijų biometrinius duomenis, kurie jau yra dabartinės SIS II tvarkos dalis. Veido atvaizdai, delnų atspaudai ir DNR analitės taip pat bus saugomi SIS duomenų bazėje. Be to, nors SIS II reglamente ir SIS II sprendime numatyta galimybė atlikti paiešką pagal pirštų atspaudus siekiant nustatyti asmens tapatybę, pagal pasiūlymus tokia paieška yra privaloma, jei asmens tapatybės neįmanoma nustatyti kokiu nors kitu būdu. Veido atvaizdai, nuotraukos ir delnų atspaudai bus naudojami atliekant paiešką sistemoje ir nustatant žmonių tapatybę, kai tai taps techniškai įmanoma. Naujos taisyklės dėl biometrinių požymių kelia ypatingą pavojų asmenų

866 SIS II reglamento 46 straipsnis ir SIS II sprendimo 62 straipsnis.

867 Žr. SIS II priežiūros koordinavimo grupė, „Šengeno informacinė sistema. *Naudojimosi prieigos teise vadovas*“, skelbiamas EDAPP svetainėje.

868 Europos Komisija (2016 m.), Komisijos ataskaita Tarybai ir Europos Parlamentui dėl antrosios kartos Šengeno informacinės sistemos (SIS II) vertinimo pagal Reglamento (EB) Nr. 1987/2006 24 straipsnio 5 dalį, 43 straipsnio 3 dalį ir 50 straipsnio 5 dalį ir Sprendimo 2007/533/TVR 59 straipsnio 3 dalį ir 66 straipsnio 5 dalį, COM(2016) 880 *final*, Briuselis, 2016 m. gruodžio 21 d.

teisėms. Savo nuomonėje dėl Komisijos pasiūlymų[869] EDAPP pažymėjo, kad biometriniai duomenys yra labai slapti ir kad jų įtraukimas į tokią didelio masto duomenų bazę turėtų būti grindžiamas įrodymais pagrįstu poreikio įtraukti juos į SIS vertinimu. Kitaip tariant, turėtų būti įrodyta, kad reikia tvarkyti naujų požymių duomenis. EDAPP taip pat laikėsi nuomonės, kad reikia išsamiau paaiškinti, kokios rūšies informaciją galima įtraukti į DNR analitę. Kadangi DNR charakteristika gali apimti neskelbtiną informaciją (ryškiausias pavyzdys būtų informacija, atskleidžianti sveikatos problemas), SIS saugomose DNR charakteristikose turėtų būti „tik būtiniausia informacija, kuri yra griežtai būtina dingusių asmenų tapatybei nustatyti ir aiškiai neapima informacijos apie sveikatą, rasinę kilmę ir bet kokios kitos neskelbtinos informacijos“[870]. Tačiau pasiūlymuose nustatomos papildomos apsaugos priemonės, kuriomis siekiama, kad duomenys būtų renkami ir toliau tvarkomi tik tiek, kiek to tikrai reikia ir kiek tai yra būtina vykdant veiklą, o prieiga suteikiama tik asmenims, kurie privalo tvarkyti asmens duomenis vykdydami veiklą[871]. Pasiūlymais eu-LISA taip pat suteikiama teisė reguliariai rengti valstybėms narėms skirtas duomenų kokybės ataskaitas, kad būtų galima reguliariai peržiūrėti perspėjimus siekiant užtikrinti duomenų kokybę[872].

Vizų informacinė sistema

Vizų informacinė sistema (VIS), kurią taip pat valdo eu-LISA, buvo sukurta siekiant padėti įgyvendinti bendrą ES vizų politiką[873]. VIS leidžia Šengeno valstybėms keistis duomenimis apie prašymą išduoti vizą pateikiančius asmenis per visiškai centralizuotą sistemą, kuri sujungia ne ES šalyse esančius Šengeno valstybių konsulatus ir ambasadas su visų Šengeno valstybių išorės sienos perėjimo punktais. VIS tvarkomi

869 EDAPP (2017 m.), EDAPP nuomonė dėl naujo Šengeno informacinės sistemos teisinio pagrindo, nuomonė Nr. 7/2017, 2017 m. gegužės 2 d.

870 *Ten pat*, 22 punktas.

871 Europos Komisija (2016 m.), Pasiūlymas dėl Europos Parlamento ir Tarybos reglamento dėl Šengeno informacinės sistemos (SIS) sukūrimo, eksploatavimo ir naudojimo policijos bendradarbiavimui ir teisminiam bendradarbiavimui baudžiamosiose bylose, kuriuo iš dalies keičiamas Reglamentas (ES) Nr. 515/2014 ir panaikinamas Reglamentas (EB) Nr. 1986/2006, Tarybos sprendimas 2007/533/JHA ir Komisijos sprendimas 2010/261/ES, COM(2016) 883 *final*, Briuselis, 2016 m. gruodžio 21 d.

872 *Ten pat*, p. 15.

873 Europos Sąjungos Taryba (2004 m.), 2004 m. birželio 8 d. Tarybos sprendimas 2004/512/EB dėl Vizų informacinės sistemos (VIS) sukūrimo, OL L 213, 2004; 2008 m. liepos 9 d. Europos Parlamento ir Tarybos reglamentas dėl Vizų informacinės sistemos (VIS) ir apsikeitimo duomenimis apie trumpalaikes vizas tarp valstybių narių (VIS reglamentas), OL L2018, 2008; Europos Sąjungos Taryba (2008 m.), 2008 m. birželio 23 d. Tarybos sprendimas 2008/633/TVR dėl valstybių narių paskirtų institucijų ir Europolo prieigos prie Vizų informacinės sistemos (VIS) teroristinių ir kitų sunkių nusikaltimų prevencijos, atskleidimo ir tyrimo tikslais, OL L 218, 2008.

duomenys, susiję su prašymais dėl trumpalaikių vizų apsilankymo Šengeno erdvėje arba jos kirtimo tikslais. VIS suteikia galimybę sienos apsaugos institucijoms naudojantis biometriniais požymiais, visų pirma pirštų atspaudais, patikrinti, ar vizą pateikiantis asmuo yra teisėtas jos turėtojas, ar ne, ir nustatyti asmenų, neturinčių dokumentų arba turinčių suklastotus dokumentus, tapatybę.

Europos Parlamento ir Tarybos reglamentu (EB) Nr. 767/2008 dėl Vizų informacinės sistemos (VIS) ir apsikeitimo duomenimis apie trumpalaikes vizas tarp valstybių narių (VIS reglamentas) reglamentuojamos su prašymais išduoti trumpalaikes vizas susijusių asmens duomenų perdavimo sąlygos ir procedūros. Pagal jį taip pat tikrinami dėl prašymų priimti sprendimai, įskaitant sprendimus panaikinti, atšaukti arba pratęsti vizą[874]. VIS reglamentas iš esmės apima duomenis apie prašymą išduoti vizą pateikiantį asmenį, jo vizas, nuotraukas, pirštų atspaudus, nuorodas į ankstesnius prašymus ir jį lydinčių asmenų prašymų bylas, arba duomenis, susijusius su asmenų kvietimu[875]. Prieiga prie VIS, siekiant įvesti, pakeisti ar ištrinti duomenis, suteikiama tik vizų institucijoms, o prieiga prie duomenų suteikiama vizų institucijoms ir institucijoms, atsakingoms už patikrinimus išorės sienos perėjimo punktuose, imigracijos patikrinimus ir prieglobstį.

Tam tikromis sąlygomis kompetentingos nacionalinės policijos institucijos ir Europolas gali prašyti leisti susipažinti su į VIS įvestais duomenimis teroristinių ir nusikalstamų veikų prevencijos, atskleidimo ar tyrimo tikslais[876]. Kadangi VIS sukurta kaip priemonė, kuria remiamas bendros vizų politikos įgyvendinimas, tikslo apribojimo principas, pagal kurį, kaip paaiškinta 3.2 skyriuje, reikalaujama, kad asmens duomenys būtų tvarkomi tik dėl nurodytų, aiškiai apibrėžtų ir teisėtų asmenų ir kuris turi būti adekvatus, aktualus ir neviršijantis tikslų, dėl kurių duomenys tvarkomi, būtų pažeistas, jei VIS taptų teisėsaugos priemone. Dėl šios priežasties nacionalinėms teisėsaugos institucijoms ir Europolui nesuteikiama įprasta prieiga prie VIS duomenų bazės. Prieiga gali būti suteikiama tik konkrečiu atveju ir kartu taikant griežtas apsaugos priemones. Šių institucijų prieigos prie VIS ir naudojimosi ja sąlygos ir apsaugos priemonės reglamentuojamos Tarybos sprendimu 2008/633/TVR[877].

874 VIS reglamento 1 straipsnis.

875 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), OL L 218, 2008, 5 straipsnis.

876 Europos Sąjungos Taryba (2008 m.), 2008 m. birželio 23 d. Tarybos sprendimas 2008/633/TVR dėl valstybių narių paskirtų institucijų ir Europolo prieigos prie Vizų informacinės sistemos (VIS) teroristinių ir kitų sunkių nusikaltimų prevencijos, atskleidimo ir tyrimo tikslais, OL L 218, 2008.

877 *Ten pat*.

Be to, VIS reglamente numatytos duomenų subjektų teisės. Tai yra tokios teisės:

- teisė, kad atsakinga valstybė narė informuotų apie duomenų valdytojo, atsakingo už asmens duomenų tvarkymą toje valstybėje narėje, tapatybę ir kontaktinius duomenis, tikslus, kuriais jų asmens duomenys bus tvarkomi VIS, asmenų, kuriems gali būti perduodami duomenys (gavėjai), kategorijas ir duomenų saugojimo laikotarpį. Be to, prašymą išduoti vizą pateikiantys asmenys turi būti informuojami apie tai, kad jų asmens duomenis pagal VIS surinkti būtina siekiant išnagrinėti jų prašymą, be to, valstybės narės taip pat privalo juos informuoti apie jų teisę susipažinti su savo duomenimis, prašyti juos ištaisyti ar ištrinti ir apie procedūras, pagal kurias jie gali pasinaudoti šiomis teisėmis[878];

- teisė susipažinti su savo asmens duomenimis, kurie įrašyti į VIS[879];

- teisė ištaisyti netikslius duomenis[880];

- teisė ištrinti neteisėtai saugomus duomenis[881].

Siekiant užtikrinti VIS priežiūrą, buvo sudaryta VIS priežiūros koordinavimo grupė. Ją sudaro EDAPP ir nacionalinių priežiūros institucijų atstovai, jie susitinka du kartus per metus. Šią grupę sudaro 28 ES valstybių narių ir Islandijos, Lichtenšteino, Norvegijos bei Šveicarijos atstovai.

878 VIS reglamento 37 straipsnis.

879 *Ten pat*, 38 straipsnio 1 dalis.

880 *Ten pat*, 38 straipsnio 2 dalis.

881 *Ten pat*, 38 straipsnio 2 dalis.

Sistema EURODAC

EURODAC – tai Europos daktiloskopija[882]. Tai centralizuota sistema, kurioje saugomi trečiųjų šalių piliečių ir asmenų be pilietybės, kurie prašo prieglobsčio vienoje iš ES valstybių narių, pirštų atspaudų duomenys[883]. Sistema veikia nuo 2003 m. sausio mėn., priėmus Tarybos reglamentą Nr. 2725/2000; naujos redakcijos reglamentas pradėtas taikyti 2015 m. Jo pagrindinis tikslas – padėti nustatyti, kuri valstybė narė turėtų būti atsakinga už konkretaus prieglobsčio prašymo nagrinėjimą pagal Reglamentą (EB) Nr. 604/2013. Šiame reglamente nustatyti valstybės narės, atsakingos už trečiosios šalies piliečio arba asmens be pilietybės vienoje iš valstybių narių pateikto tarptautinės apsaugos prašymo nagrinėjimą, nustatymo kriterijai ir mechanizmai (reglamentas „Dublinas III“)[884]. Asmens duomenys sistemoje EURODAC iš esmės naudojami siekiant palengvinti reglamento „Dublinas III“ taikymą[885].

Nacionalinėms teisėsaugos institucijoms ir Europolui leidžiama palyginti pirštų atspaudus, susijusius su nusikalstamų veikų tyrimais, su sistemoje EURODAC esančiais pirštų atspaudais, tačiau tik teroristinių ar kitų sunkių nusikalstamų veikų prevencijos, atskleidimo ar tyrimo tikslais. Kadangi sistema EURODAC sukurta kaip ES prieglobsčio politikos įgyvendinimo rėmimo priemonė, o ne kaip teisėsaugos priemonė, teisėsaugos institucijos turi prieigą prie duomenų bazės tik konkrečiais atvejais, konkrečiomis aplinkybėmis ir griežtomis sąlygomis[886]. Tolesniam duomenų naudojimui teisėsaugos tikslais taikoma Duomenų apsaugos policijos ir baudžiamosios

882 Žr. Europos duomenų apsaugos priežiūros pareigūno svetainės tinklalapį apie sistemą EURODAC.

883 2000 m. gruodžio 11 d. Tarybos reglamentas (EB) Nr. 2725/2000 dėl „Eurodac“ sistemos sukūrimo pirštų atspaudams lyginti siekiant veiksmingiau taikyti Dublino konvenciją, OL L 316, 2000; 2002 m. vasario 28 d. Tarybos reglamentas (EB) Nr. 407/2002, nustatantis tam tikras taisykles įgyvendinant Reglamentą (EB) Nr. 2725/2000 dėl „Eurodac“ sistemos sukūrimo pirštų atspaudams lyginti, siekiant veiksmingiau taikyti Dublino konvenciją, OL L 62, 2002 (EURODAC reglamentai), 2013 m. birželio 26 d. Reglamentas (ES) Nr. 603/2013 dėl „Eurodac“ sistemos pirštų atspaudams lyginti sukūrimo siekiant veiksmingai taikyti Reglamentą (ES) Nr. 604/2013, kuriuo išdėstomi valstybės narės, atsakingos už trečiosios šalies piliečio arba asmens be pilietybės vienoje iš valstybių narių pateikto tarptautinės apsaugos prašymo nagrinėjimą, nustatymo kriterijai ir mechanizmai, ir dėl valstybių narių teisėsaugos institucijų bei Europolo teisėsaugos tikslais teikiamų prašymų palyginti duomenis su „Eurodac“ sistemos duomenimis ir kuriuo iš dalies keičiamas Reglamentas (ES) Nr. 1077/2011, kuriuo įsteigiama Europos didelės apimties IT sistemų laisvės, saugumo ir teisingumo erdvėje operacijų valdymo agentūra, OL L 180, 2013, p. 1 (naujos redakcijos EURODAC reglamentas).

884 2013 m. birželio 26 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 603/2013 dėl „Eurodac“ sistemos pirštų atspaudams lyginti sukūrimo siekiant veiksmingai taikyti Reglamentą (ES) Nr. 604/2013, kuriuo išdėstomi valstybės narės, atsakingos už trečiosios šalies piliečio arba asmens be pilietybės vienoje iš valstybių narių pateikto tarptautinės apsaugos prašymo nagrinėjimą, nustatymo kriterijai ir mechanizmai, OL L 180, 2013 (reglamentas „Dublinas III“).

885 Naujos redakcijos sistemos EURODAC reglamento, OL L 180, 2013, p. 1, 1 straipsnio 1 dalis.

886 *Ten pat*, 1 straipsnio 2 dalis.

teisenos institucijoms tvarkant asmens duomenis direktyva, o duomenys, kurie naudojami siekiant pagrindinio tikslo – palengvinti reglamento „Dublinas III“ įgyvendinimą, saugomi pagal Bendrąjį duomenų apsaugos reglamentą. Draudžiama toliau perduoti asmens duomenis, kuriuos valstybė narė arba Europolas gavo pagal naujos redakcijos EURODAC reglamentą, bet kuriai trečiajai šaliai, tarptautinei organizacijai arba privačiam subjektui, įsisteigusiam ES arba už jos ribų[887].

Sistemą EURODAC sudaro eu-LISA valdomas centrinis padalinys, skirtas pirštų atspaudams saugoti ir lyginti, ir elektroninių duomenų perdavimo tarp valstybių narių ir centrinės duomenų bazės sistema. Valstybės narės ima ir perduoda kiekvieno ne jaunesnio kaip 14 metų asmens, prašančio prieglobsčio jų teritorijoje, ir kiekvieno ne jaunesnio kaip 14 metų ne ES piliečio arba asmens be pilietybės, sulaikyto dėl neteisėto jų išorės sienos kirtimo, pirštų atspaudus. Valstybės narės taip pat gali paimti ir perduoti jų teritorijoje be leidimo esančių ne ES piliečių arba asmenų be pilietybės pirštų atspaudus.

Nors bet kuri valstybė narė gali naudotis sistema EURODAC ir prašyti palyginti duomenis su pirštų atspaudų duomenimis, tik pirštų atspaudus surinkusi ir juos centriniam padaliniui perdavusi valstybė narė turi teisę keisti duomenis juos taisydama, papildydama arba ištrindama[888]. eu-LISA saugo įrašus apie visą duomenų tvarkymą, kad galėtų stebėti duomenų apsaugą ir užtikrinti duomenų saugumą[889]. Nacionalinės priežiūros institucijos padeda duomenų subjektams naudotis savo teisėmis ir juos konsultuoja[890]. Pirštų atspaudų duomenų rinkimą ir perdavimą tikrina nacionaliniai teismai[891]. ES institucijų duomenų apsaugos reglamentas[892] ir EDAPP vykdoma priežiūra taikomi centrinėje sistemoje, kurią, kiek tai susiję su sistema EURODAC, valdo eu-LISA, vykdomai duomenų tvarkymo veiklai[893]. Jeigu asmuo patiria žalą dėl neteisėtos duomenų tvarkymo operacijos ar bet kokio veiksmo, nesuderinamo su EURODAC reglamentu, šis asmuo turi teisę gauti kompensaciją iš žalą padariusios valstybės narės[894]. Tačiau reikėtų pabrėžti, kad prieglobsčio prašytojai yra ypač

887 *Ten pat*, 35 straipsnis.

888 *Ten pat*, 27 straipsnis.

889 *Ten pat*, 28 straipsnis.

890 *Ten pat*, 29 straipsnis.

891 *Ten pat*, 29 straipsnis.

892 2000 m. gruodžio 18 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 45/2001 dėl asmenų apsaugos Bendrijos institucijoms ir įstaigoms tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo, OL L 8, 2001.

893 Naujos redakcijos EURODAC reglamentas, OL L 180, 2013, p. 1, 31 straipsnis.

894 *Ten pat*, 37 straipsnis.

pažeidžiama asmenų, kurie dažnai keliauja ilgai ir rizikingai, grupė. Dėl pažeidžiamumo ir nesaugios padėties, kurioje jie dažnai atsiduria, kol nagrinėjamas jų prieglobsčio prašymas, praktiškai gali būti sunku pasinaudoti savo teisėmis, įskaitant teisę į kompensaciją.

Kad galėtų naudotis sistema EURODAC teisėsaugos tikslais, valstybės narės turi paskirti institucijas, kurios turės teisę prašyti prieigos, taip pat institucijas, kurios tikrins, ar prašymai palyginti duomenis yra teisėti[895]. Nacionalinių institucijų ir Europolo prieigai prie sistemos EURODAC pirštų atspaudų duomenų taikomos labai griežtos sąlygos. Prašančioji institucija turi pateikti motyvuotą elektroninį prašymą tik palyginusi duomenis su duomenimis kitose prieinamose informacinėse sistemose, pavyzdžiui, nacionalinėse pirštų atspaudų duomenų bazėse ir VIS. Turi būti viršesnis susirūpinimas dėl visuomenės saugumo, todėl palyginimas yra proporcingas. Palyginimas turi būti tikrai būtinas, susijęs su konkrečiu atveju ir turi būti pagrįstų priežasčių manyti, kad palyginimas iš esmės padės užkirsti kelią bet kuriai nagrinėjamai nusikalstamai veikai, ją atskleisti ar tirti, ypač kai yra pagrįstų įtarimų, kad teroristinio nusikaltimo arba kitos sunkios nusikalstamos veikos padarymu įtariamas asmuo, nusikaltimo vykdytojas arba auka patenka į kategoriją, kuriai taikomas pirštų atspaudų rinkimas sistemoje EURODAC. Duomenys turi būti lyginami tik su pirštų atspaudų duomenimis. Europolas taip pat privalo gauti pirštų atspaudų duomenis surinkusios valstybės narės leidimą.

Su prieglobsčio prašytojais susiję sistemoje EURODAC esantys asmens duomenys saugomi 10 metų nuo pirštų atspaudų paėmimo dienos, išskyrus atvejus, kai duomenų subjektas įgyja ES valstybės narės pilietybę. Šiuo atveju duomenis privaloma ištrinti nedelsiant. Duomenys, susiję su užsieniečiais, sulaikytais dėl neteisėto išorės sienos kirtimo, saugomi 18 mėnesių. Šiuos duomenis privaloma nedelsiant ištrinti, jei duomenų subjektas gauna leidimą gyventi, išvyksta iš ES teritorijos arba įgyja valstybės narės pilietybę. Asmenų, kuriems buvo suteiktas prieglobstis, duomenis galima palyginti teroristinių ir kitų sunkių nusikaltimų prevencijos, atskleidimo ir tyrimo tikslais trejus metus.

Sistemoje EURODAC, be visų ES valstybių narių, taip pat pagal tarptautinius susitarimus dalyvauja Islandija, Norvegija, Lichtenšteinas ir Šveicarija.

895 L. Roots (2015 m.) *The New EURODAC Regulation: Fingerprints as a Source of Informal Discrimination*, *Baltic Journal of European Studies Tallinn University of Technology*, 5 t., Nr. 2, p. 108–129.

Siekiant užtikrinti sistemos EURODAC priežiūrą, sukurta sistemos EURODAC priežiūros koordinavimo grupė. Ją sudaro EDAPP ir nacionalinių priežiūros institucijų atstovai, kurie susitinka du kartus per metus. Šią grupę sudaro 28 ES valstybių narių ir Islandijos, Lichtenšteino, Norvegijos bei Šveicarijos atstovai[896].

Ateities perspektyvos

Vykdydama reformą, kuria siekiama pagerinti bendros Europos prieglobsčio sistemos (BEPS) veikimą, 2016 m. gegužės mėn. Komisija pateikė pasiūlymą dėl naujos EURODAC reglamento redakcijos[897]. Siūloma nauja redakcija yra svarbi, nes ja bus gerokai praplėsta pirminės EURODAC duomenų bazės taikymo sritis. Sistema EURODAC iš pradžių buvo sukurta siekiant padėti įgyvendinti BEPS, suteikiant pirštų atspaudų įrodymus, kad būtų galima nustatyti, kuri valstybė narė yra atsakinga už ES pateikto prieglobsčio prašymo nagrinėjimą. Siūloma nauja redakcija bus praplėsta duomenų bazės taikymo sritis, kad būtų sudarytos palankesnės sąlygos neteisėtų migrantų grąžinimui[898]. Nacionalinės valdžios institucijos galės naudotis duomenų baze siekdamos nustatyti neteisėtai ES esančių arba neteisėtai į ES atvykusių trečiųjų šalių piliečių tapatybę ir gauti įrodymų, kurie padėtų valstybėms narėms grąžinti šiuos asmenis. Be to, nors pagal šiuo metu galiojančią teisinę tvarką reikalaujama tik rinkti ir saugoti pirštų atspaudus, pasiūlyme numatyta rinkti asmenų veido atvaizdus[899], kurie yra kitos rūšies biometriniai duomenys. Pasiūlymu taip pat būtų sumažintas minimalus vaikų, kurių biometrinius duomenis galima rinkti, amžius iki šešerių[900], o ne 14 metų (minimalus amžius pagal 2013 m. reglamentą). Praplėtus

896 Žr. Europos duomenų apsaugos priežiūros pareigūno svetainės tinklalapį apie sistemą EURODAC.

897 Europos Komisija, Pasiūlymas dėl Europos Parlamento ir Tarybos reglamento dėl pirštų atspaudų lyginimo sistemos EURODAC sukūrimo siekiant veiksmingai taikyti [Reglamentą (ES) Nr. 604/2013, kuriuo išdėstomi valstybės narės, atsakingos už trečiosios šalies piliečio arba asmens be pilietybės vienoje iš valstybių narių pateikto tarptautinės apsaugos prašymo nagrinėjimą, nustatymo kriterijai ir mechanizmai], siekiant nustatyti neteisėtai esančius trečiųjų šalių piliečius ar asmenis be pilietybės, ir dėl valstybių narių teisėsaugos institucijų bei Europolo teisėsaugos tikslais teikiamų prašymų palyginti duomenis su sistemos EURODAC duomenimis (nauja redakcija), COM(2016) 272 *final*, 2016 m. gegužės 4 d.

898 Žr. pasiūlymo aiškinamąjį memorandumą, p. 3.

899 Europos Komisija, Pasiūlymas dėl Europos Parlamento ir Tarybos reglamento dėl pirštų atspaudų lyginimo sistemos EURODAC sukūrimo siekiant veiksmingai taikyti [Reglamentą (ES) Nr. 604/2013, kuriuo išdėstomi valstybės narės, atsakingos už trečiosios šalies piliečio arba asmens be pilietybės vienoje iš valstybių narių pateikto tarptautinės apsaugos prašymo nagrinėjimą, nustatymo kriterijai ir mechanizmai], siekiant nustatyti neteisėtai esančius trečiųjų šalių piliečius ar asmenis be pilietybės, ir dėl valstybių narių teisėsaugos institucijų bei Europolo teisėsaugos tikslais teikiamų prašymų palyginti duomenis su sistemos EURODAC duomenimis (nauja redakcija), COM(2016) 272 *final*, 2016 m. gegužės 4 d., 2 straipsnio 1 dalis.

900 *Ten pat*, 2 straipsnio 2 dalis.

pasiūlymo taikymo sritį bus apribotos daugiau asmenų, kurie gali būti įtraukti į duomenų bazę, teisės į privatumą ir duomenų apsaugą. Siekiant atsverti šį ribojimą, pasiūlymu ir Europos Parlamento Piliečių laisvių, teisingumo ir vidaus reikalų komiteto[901] siūlomais pakeitimais siekiama sugriežtinti duomenų apsaugos reikalavimus. Rengiant vadovą, Parlamente ir Taryboje vyko diskusijos dėl pasiūlymo priėmimo.

EUROSUR

Europos sienų stebėjimo sistema (EUROSUR)[902] sukurta siekiant sustiprinti Šengeno išorės sienų kontrolę nustatant neteisėtos imigracijos ir tarpvalstybinio nusikalstamumo atvejus, užkertant jiems kelią ir su jais kovojant. Jis padeda stiprinti nacionalinių koordinavimo centrų ir *Frontex*, ES agentūros, atsakingos už naujos integruoto sienų valdymo koncepcijos kūrimą ir taikymą, keitimąsi informacija ir operatyvinį bendradarbiavimą[903]. Bendrieji jos tikslai yra:

- sumažinti nenustatytų neteisėtų migrantų, atvykstančių į ES, skaičių;
- sumažinti neteisėtų migrantų mirčių skaičių išsaugant daugiau gyvybių jūroje;
- didinti visos ES vidaus saugumą prisidedant prie tarpvalstybinio nusikalstamumo prevencijos[904].

901 Europos Parlamentas, *Pranešimas* dėl pasiūlymo dėl Europos Parlamento ir Tarybos reglamento dėl pirštų atspaudų lyginimo sistemos EURODAC sukūrimo siekiant veiksmingai taikyti Reglamentą (ES) Nr. 604/2013, kuriuo išdėstomi valstybės narės, atsakingos už trečiosios šalies piliečio arba asmens be pilietybės vienoje iš valstybių narių pateikto tarptautinės apsaugos prašymo nagrinėjimą, nustatymo kriterijai ir mechanizmai, siekiant nustatyti neteisėtai esančius trečiųjų šalių piliečius ar asmenis be pilietybės, ir dėl valstybių narių teisėsaugos institucijų bei Europolo teisėsaugos tikslais teikiamų prašymų palyginti duomenis su sistemos EURODAC duomenimis (nauja redakcija), PE 597.620v03-00, 2017 m. birželio 9 d.

902 2013 m. spalio 22 d. Europos Parlamento Tarybos reglamentas (ES) Nr. 1052/2013, kuriuo sukuriama Europos sienų stebėjimo sistema (EUROSUR), OL L 295, 2013.

903 2016 m. rugsėjo 14 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 206/1624 dėl Europos sienų ir pakrančių apsaugos pajėgų, kuriuo iš dalies keičiamas Europos Parlamento ir Tarybos reglamentas (ES) 2016/399 ir panaikinami Europos Parlamento ir Tarybos reglamentas (EB) Nr. 863/2007, Tarybos reglamentas (EB) Nr. 2007/2004 ir Tarybos sprendimas 2005/267/EB, OL L 251.

904 Taip pat žr.: Europos Komisija (2008 m.), *2015 m. gegužės 13 d. Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui: Europos sienų stebėjimo sistemos (EUROSUR) sukūrimo nagrinėjimas*, COM(2008) 68 *final*, Briuselis, 2008 m. vasario 13 d.; Europos Komisija (2011 m.), *Poveikio vertinimas, pridedamas prie pasiūlymo dėl Europos Parlamento ir Tarybos reglamento, kuriuo sukuriama Europos sienų stebėjimo sistema (EUROSUR)*, tarnybų darbinis dokumentas, SEC(2011) 1536 *final*, Briuselis, 2011 m. gruodžio 12 d., p. 18.

EUROSUR savo veiklą visose išorės sienas turinčiose valstybėse narėse pradėjo 2013 m. gruodžio 2 d., o kitose – 2014 m. gruodžio 1 d. Reglamentas taikomas valstybių narių išorės sausumos, jūrų ir oro sienų stebėjimui. EUROSUR labai ribotai keičiasi asmens duomenimis ir juos tvarko, nes valstybės narės ir *Frontex* turi teisę keistis tik laivų identifikavimo numeriais. EUROSUR keičiasi operatyvine informacija, pavyzdžiui, apie patruliavimo ir incidentų vietą, ir paprastai informacija, kuria keičiamasi, negali apimti asmens duomenų[905]. Išskirtiniais atvejais, kai asmens duomenimis keičiamasi naudojantis EUROSUR, reglamente numatyta, kad visapusiškai taikoma bendra ES duomenų apsaugos teisinė sistema[906].

Taip EUROSUR užtikrina teisę į duomenų apsaugą, būtent nurodydamas, kad keitimasis duomenimis turi atitikti Duomenų apsaugos policijos ir baudžiamosios teisenos institucijoms tvarkant asmens duomenis direktyvoje ir Bendrajame duomenų apsaugos reglamente numatytus kriterijus ir apsaugos priemones[907].

Muitinės informacinė sistema

Kita svarbi ES lygmeniu nustatyta informacinė sistema yra Muitinės informacinė sistema (MIS)[908]. Kuriant vidaus rinką buvo panaikinti visi ES teritorijoje vežamų prekių patikrinimai ir formalumai, todėl padidėjo sukčiavimo rizika. Ši rizika buvo mažinama intensyvesniu valstybių narių muitinių administracijų bendradarbiavimu. MIS tikslas – padėti valstybėms narėms užkirsti kelią nacionalinių ir ES muitinės ir žemės ūkio įstatymų pažeidimams, juos tirti ir patraukti už juos baudžiamojon atsakomybėn. MIS sukurta dviem teisės aktais, priimtais remiantis skirtingais teisiniais pagrindais: Tarybos reglamentas (EB) Nr. 515/97 susijęs su įvairių nacionalinių administracinių institucijų bendradarbiavimu kovojant su sukčiavimu muitų sąjungos ir bendros žemės ūkio politikos srityse, o Tarybos sprendimu 2009/917/TVR siekiama padėti užkirsti kelią sunkiems muitų teisės aktų pažeidimams, juos tirti ir patraukti už juos baudžiamojon atsakomybėn. Tai reiškia, kad MIS naudojama ne tik teisėsaugos tikslais.

905 Europos Komisija, „*EUROSUR: Šengeno išorės sienų apsauga – migrantų gyvybių apsauga. Trumpai apie EUROSUR*“, 2013 m. lapkričio 29 d.

906 Reglamento Nr. 1052/2013 13 konstatuojamoji dalis ir 13 straipsnis.

907 *Ten pat*, 13 konstatuojamoji dalis ir 13 straipsnis.

908 Europos Sąjungos Taryba (1995 m.), Tarybos aktas dėl Konvencijos dėl informacijos technologijų naudojimo muitinės tikslais parengimo, OL L 316, 1995, iš dalies pakeistas Europos Sąjungos Tarybos (2009 m.) 1997 m. kovo 13 d. Reglamentu Nr. 515/97 dėl valstybių narių administracinių institucijų tarpusavio pagalbos ir dėl pastarųjų bei Komisijos bendradarbiavimo, siekiant užtikrinti teisingą muitinės ir žemės ūkio teisės aktų taikymą, 2009 m. lapkričio 30 d. Tarybos sprendimas 2009/917/TVR dėl informacijos technologijų naudojimo muitinės tikslais (MIS sprendimas), OL L 323, 2009.

MIS saugoma informacija apima asmens duomenis, susijusius su prekėmis, transporto priemonėmis, įmonėmis, asmenimis, prekėmis ir grynaisiais pinigais, kurie laikomi, areštuojami ar konfiskuojami. Duomenų, kuriuos galima tvarkyti, kategorijos yra aiškiai apibrėžtos ir apima atitinkamų asmenų vardus ir pavardes, pilietybę, lytį, gimimo vietą ir datą, jų duomenų įtraukimo į sistemą priežastį ir transporto priemonės registracijos numerį[909]. Šią informaciją galima naudoti tik stebint ir vykdant konkrečius tyrimus arba teikiant apie juos ataskaitas, arba atliekant strateginę analizę, susijusią su muitinės nuostatų pažeidimu.

Prieiga prie MIS suteikiama nacionalinėms muitinės, mokesčių, žemės ūkio, visuomenės sveikatos ir policijos institucijoms, taip pat Europolui ir Eurojustui.

Asmens duomenys turi būti tvarkomi laikantis konkrečių taisyklių, nustatytų Reglamentu Nr. 515/97 ir Tarybos sprendimu 2009/917/TVR, taip pat Bendrojo duomenų apsaugos reglamento, ES institucijų duomenų apsaugos reglamento, atnaujintos 108-osios konvencijos ir Rekomendacijos dėl policijos nuostatų. EDAPP privalo prižiūrėti MIS atitiktį Reglamentui (EB) Nr. 45/2001. Jis bent kartą per metus sušaukia posėdį su visomis nacionalinėmis duomenų apsaugos priežiūros institucijomis, kurių kompetencijai priklauso su MIS susiję priežiūros klausimai.

ES informacinių sistemų sąveikumas

Migracijos valdymas, integruotas ES išorės sienų valdymas ir kova su terorizmu bei tarpvalstybiniu nusikalstamumu yra svarbūs uždaviniai, kurie globaliame pasaulyje tampa vis sudėtingesni. Pastaraisiais metais ES formavo naują visapusišką požiūrį į saugumo užtikrinimą ir palaikymą nepakenkiant ES vertybėms ir pagrindinėms laisvėms. Siekiant šių tikslų labai svarbu, kad nacionalinės teisėsaugos institucijos, taip pat valstybės narės ir atitinkamos ES agentūros veiksmingai keistųsi informacija[910]. Esamos ES sienų valdymo ir vidaus saugumo informacinės sistemos turi atitinkamus tikslus, institucinę struktūrą, duomenų subjektus ir naudotojus. ES stengiasi

909 Žr. MIS sprendimo 24, 25 ir 28 straipsnius.

910 Europos Komisija (2016 m.), Komisijos komunikatas Europos Parlamentui ir Tarybai: „Patikimesnės ir pažangesnės sienų ir saugumo informacinės sistemos“, COM(2016) 205 *final*, Briuselis, 2016 m. balandžio 6 d.; Europos Komisija (2016 m.), Komisijos komunikatas Europos Parlamentui, Europos Vadovų Tarybai ir Tarybai „Didesnis saugumas judžiame pasaulyje. Geresnis keitimasis informacija kovojant su terorizmu ir patikimesnės išorės sienos“, COM(2016) 602 *final*, Briuselis, 2016 m. rugsėjo 14 d.; Europos Komisija (2016 m.), Pasiūlymas dėl Europos Parlamento ir Tarybos reglamento dėl Šengeno informacinės sistemos naudojimo neteisėtai esančių trečiųjų šalių piliečių grąžinimo tikslams. Taip pat žr. Komisijos komunikatą Europos Parlamentui, Europos Vadovų Tarybai ir Tarybai „Septintoji pažangos, padarytos kuriant tikrą ir veiksmingą saugumo sąjungą, ataskaita“, COM(2017) 261 *final*, Briuselis, 2017 m. gegužės 16 d.

pašalinti trūkumus, susijusius su skirtingų informacinių sistemų, pavyzdžiui, SIS II, VIS ir sistemos EURODAC, suskaidyto ES duomenų valdymo funkcijomis, nagrinėdama sąveikumo galimybes[911]. Pagrindinis tikslas – užtikrinti, kad kompetentingos policijos, muitinės ir teisminės institucijos sistemingai gautų jų pareigoms atlikti būtiną informaciją, kartu išlaikant teisių į privatumą, duomenų apsaugos ir kitų pagrindinių teisių pusiausvyrą.

Sąveikumas yra „informacinių sistemų gebėjimas keistis duomenimis ir sudaryti sąlygas keistis informacija“[912]. Toks keitimasis neturi pažeisti būtinai griežtų prieigos ir naudojimo taisyklių, kurias garantuoja Bendrasis duomenų apsaugos reglamentas, Duomenų apsaugos direktyva, skirta policijos ir baudžiamosios teisenos institucijoms, ES pagrindinių teisių chartija ir visos kitos atitinkamos taisyklės. Bet koks integruotas duomenų valdymo sprendimas neturi daryti poveikio tikslų apribojimo, pritaikytosios duomenų apsaugos ar standartizuotosios duomenų apsaugos principams[913].

Komisija ne tik pagerino trijų pagrindinių informacinių sistemų – SIS II, VIS ir sistemos EURODAC – funkcijas, bet ir pasiūlė sukurti ketvirtą centralizuotą sienų valdymo sistemą, skirtą trečiųjų šalių piliečiams – atvykimo ir išvykimo sistemą (AIS)[914], kurią tikimasi įgyvendinti iki 2020 m.[915] Komisija taip pat pateikė pasiūlymą dėl Europos

911 Europos Sąjungos Taryba (2005 m.), Hagos programa „Laisvės, saugumo ir teisingumo stiprinimas Europos Sąjungoje“, OL C 53, 2005; Europos Komisija (2010 m.), Komisijos komunikatas Europos Parlamentui ir Tarybai „Informacijos valdymo laisvės, saugumo ir teisingumo erdvėje apžvalga“, COM(2010) 385 *final*, Europos Komisija (2016 m.), Komisijos komunikatas Europos Parlamentui ir Tarybai „Patikimesnės ir pažangesnės sienų ir saugumo informacinės sistemos“, COM(2016) 205 *final*, 2016 m. balandžio 6 d.; Europos Komisija (2016 m.), 2016 m. birželio 17 d. Komisijos sprendimas, kuriuo įsteigiama Aukšto lygio informacinių sistemų ir sąveikumo ekspertų grupė, OL C 257, 2016.

912 Europos Komisija (2016 m.), Komisijos komunikatas Europos Parlamentui ir Tarybai: „Patikimesnės ir pažangesnės sienų ir saugumo informacinės sistemos“, COM(2016) 205 *final*, 2016 m. balandžio 6 d., p. 14.

913 *Ten pat*, p. 4–5.

914 Europos Komisija (2016 m.), Pasiūlymas dėl Europos Parlamento ir Tarybos reglamento, kuriuo sukuriama atvykimo ir išvykimo sistema (AIS), kurioje registruojami trečiųjų šalių piliečių, kertančių Europos Sąjungos valstybių narių išorės sienas, atvykimo ir išvykimo bei atsisakymo leisti jiems atvykti duomenys, nustatomos prieigos prie AIS teisėsaugos tikslais sąlygos ir iš dalies keičiamas Reglamentas (EB) Nr. 767/2008 ir Reglamentas (ES) Nr. 1077/2011, COM(2016) 194 *final*, Briuselis, 2016 m. balandžio 6 d.

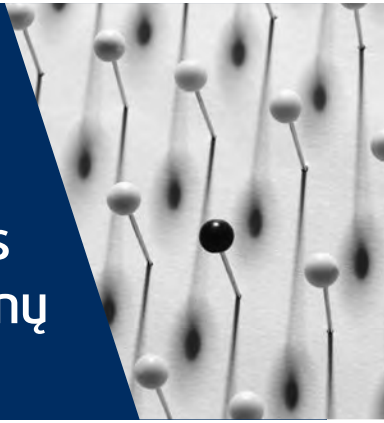
915 Europos Komisija (2016 m.), Komisijos komunikatas Europos Parlamentui ir Tarybai: „Patikimesnės ir pažangesnės sienų ir saugumo informacinės sistemos“, COM(2016) 205 *final*, 2016 m. balandžio 6 d., p. 5.

kelionių informacijos ir leidimų sistemos (ETIAS) sukūrimo[916], t. y. sistemos, kurioje bus renkama informacija apie asmenis, keliaujančius į ES be vizų, kad būtų galima atlikti išankstinius neteisėtos migracijos ir saugumo patikrinimus.

916 Europos Komisija (2016 m.), Pasiūlymas dėl Europos Parlamento ir Tarybos reglamento, kuriuo sukuriama Europos kelionių informacijos ir leidimų sistema (ETIAS) ir iš dalies keičiami reglamentai (ES) Nr. 515/2014, (ES) 2016/399, (ES) 2016/794 ir (ES) 2016/1624, COM(2016) 731 *final*, 2016 m. lapkričio 16 d.

9

Konkrečių rūšių duomenys ir su jais susijusios duomenų apsaugos taisyklės



ES	Reglamentuojami klausimai	ET
Bendrasis duomenų apsaugos reglamentas Direktyva dėl privatumo ir elektroninių ryšių	**Elektroniniai ryšiai**	Atnaujinta 108-oji konvencija Rekomendacija dėl telekomunikacijų paslaugų
Bendrojo duomenų apsaugos reglamento 88 straipsnis	**Darbo santykiai**	Atnaujinta 108-oji konvencija Rekomendacija dėl užimtumo EŽTT, *Copland prieš Jungtinę Karalystę*, Nr. 62617/00, 2007 m.
Bendrojo duomenų apsaugos reglamento 9 straipsnio 2 dalies h ir i punktai	**Medicininiai duomenys**	Atnaujinta 108-oji konvencija Rekomendacija dėl medicininių duomenų EŽTT, *Z prieš Suomiją*, Nr. 22009/93, 1997 m.
Klinikinių tyrimų reglamentas	**Klinikiniai tyrimai**	
Bendrojo duomenų apsaugos reglamento 6 straipsnio 4 dalis, 89 straipsnis	**Statistiniai duomenys**	Atnaujinta 108-oji konvencija Rekomendacija dėl statistinių duomenų

ES	Reglamentuojami klausimai	ET
Reglamentas (EB) Nr. 223/2009 dėl Europos statistikos ESTT, C-524/06, *Huber prieš Bundesrepublik Deutschland* (DK), 2008 m.	**Oficialūs statistiniai duomenys**	Atnaujinta 108-oji konvencija Rekomendacija dėl statistinių duomenų
Direktyva 2014/65/ES dėl finansinių priemonių rinkų Reglamentas (ES) Nr. 648/2012 dėl ne biržos išvestinių finansinių priemonių, pagrindinių sandorio šalių ir sandorių duomenų saugyklų Reglamentas (EB) Nr. 1060/2009 dėl kredito reitingų agentūrų Direktyva 2007/64/EB dėl mokėjimo paslaugų vidaus rinkoje	**Finansiniai duomenys**	Atnaujinta 108-oji konvencija Rekomendacija 90 (19), taikoma mokėjimams ir kitoms susijusioms operacijoms EŽTT, *Michaud prieš Prancūziją*, Nr. 12323/11, 2012 m.

Keliais atvejais Europos lygmeniu buvo priimtos specialios teisinės priemonės, kad būtų galima išsamiau konkrečioms situacijoms taikyti atnaujintos 108-osios konvencijos arba Bendrojo duomenų apsaugos reglamento bendrąsias taisykles.

9.1. Elektroniniai ryšiai

Pagrindiniai faktai

- Konkrečios duomenų apsaugos taisyklės telekomunikacijų srityje, visų pirma skirtos telefono ryšio paslaugoms, pateiktos 1995 m. ES rekomendacijoje.
- Asmens duomenų tvarkymas, susijęs su telekomunikacijų paslaugų teikimu ES lygmeniu, reglamentuojamas Direktyvoje dėl privatumo ir elektroninių ryšių.
- Elektroninių pranešimų konfidencialumas yra susijęs ne tik su pranešimo turiniu, bet ir su metaduomenimis, pavyzdžiui, informacija apie ryšio dalyvius, bendravimo laiką ir trukmę, taip pat buvimo vietos duomenimis, pavyzdžiui, kurioje vietoje buvo perduoti duomenys.

Ryšių tinkluose gali būti dažniau kišamasi į asmeninę naudotojų erdvę, nes juose yra didelės techninės galimybės klausytis ir stebėti tokiais tinklais siunčiamus pranešimus. Todėl buvo manoma, kad reikalingos specialios duomenų apsaugos taisyklės,

kad būtų galima pašalinti konkrečią elektroninių ryšių paslaugų naudotojams kylančią riziką.

1995 m. **ET** paskelbė rekomendaciją dėl duomenų apsaugos telekomunikacijų srityje, joje daugiausia dėmesio skiriama telefono ryšio paslaugoms[917]. Pagal šią rekomendaciją asmens duomenų rinkimo ir tvarkymo telekomunikacijų srityje tikslai turėtų apsiriboti naudotojo prijungimu prie tinklo, konkrečios telekomunikacijų paslaugos teikimu, sąskaitų išrašymu, tikrinimu, optimalaus techninio veikimo užtikrinimu ir tinklo bei paslaugos plėtojimu.

Ypatingas dėmesys taip pat buvo skiriamas ryšių tinklų naudojimui tiesioginės rinkodaros pranešimams siųsti. Paprastai tiesioginės rinkodaros pranešimai negali būti skirti jokiam abonentui, kuris aiškiai atsisakė jų gauti. Automatinė skambučių įranga, kurią naudojant perduodami iš anksto įrašyti reklamos pranešimai, gali būti naudojama tik tuo atveju, jeigu abonentas davė aiškų sutikimą. Nacionalinėje teisėje nustatomos išsamios šios srities taisyklės.

ES teisinėje sistemoje po pirmojo bandymo 1997 m. Direktyva dėl privatumo ir elektroninių ryšių buvo priimta 2002 m. ir iš dalies pakeista 2009 m. Tai buvo daroma siekiant papildyti ankstesnės Duomenų apsaugos direktyvos nuostatas ir jas pritaikyti prie telekomunikacijų sektoriaus[918].

Direktyva dėl privatumo ir elektroninių ryšių taikoma tik ryšių paslaugoms, kurios teikiamos naudojant viešus elektroninius tinklus.

Direktyvoje dėl privatumo ir elektroninių ryšių daromas skirtumas tarp trijų pagrindinių kategorijų duomenų, kurie buvo surinkti ryšių metu:

- duomenų, kurie sudaro ryšio metu išsiųstų pranešimų turinį, – šie duomenys yra griežtai konfidencialūs;

917 Europos Taryba, Ministrų Komitetas (1995 m.), Rekomendacija *Rec(95)4* valstybėms narėms dėl asmens duomenų apsaugos telekomunikacijų paslaugų srityje, ypač telefono ryšio paslaugų srityje, 1995 m. vasario 7 d.

918 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių), OL L 201, 2002, iš dalies pakeista 2009 m. lapkričio 25 d. Europos Parlamento ir Tarybos direktyva 2009/136/EB, iš dalies keičiančią Direktyvą 2002/22/EB dėl universaliųjų paslaugų ir paslaugų gavėjų teisių, susijusių su elektroninių ryšių tinklais ir paslaugomis, Direktyvą 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje ir Reglamentą (EB) Nr. 2006/2004 dėl nacionalinių institucijų, atsakingų už vartotojų apsaugos teisės aktų vykdymą, bendradarbiavimo, OL L 337, 2009.

- duomenų, būtinų ryšiui užmegzti ir palaikyti (vadinamieji metaduomenys, direktyvoje vadinami srauto duomenimis), pavyzdžiui, informacija apie ryšio šalis, ryšio laiką ir trukmę;

- metaduomenyse yra duomenų, konkrečiai susijusių su ryšio įrenginio buvimo vieta, vadinamųjų vietos nustatymo duomenų – šie duomenys kartu yra duomenys apie ryšio įrenginių naudotojų buvimo vietą, ypač kai tai susiję su judriojo ryšio įrenginių naudotojais.

Paslaugų teikėjas srauto duomenis gali naudoti tik išrašydamas sąskaitas ir užtikrindamas techninius paslaugos teikimo aspektus. Tačiau, duomenų subjektui sutikus, šie duomenys gali būti atskleisti kitiems duomenų valdytojams, teikiantiems pridėtinės vertės paslaugas, pavyzdžiui, atsižvelgiant į naudotojo buvimo vietą, teikiantiems informaciją apie kitą metro stotį ar vaistinę arba apie vietos orų prognozes.

Pagal E. privatumo direktyvos 15 straipsnį galimybė susipažinti su duomenimis apie ryšius elektroniniuose tinkluose turi atitikti reikalavimus dėl pagrįsto teisės į duomenų apsaugą apribojimo, kaip nustatyta EŽTK 8 straipsnio 2 dalyje ir patvirtinta ES pagrindinių teisių chartijos 8 ir 52 straipsniuose. Tokia galimybė gali apimti prieigą prie duomenų nusikaltimų tyrimo tikslais.

Direktyvos dėl privatumo ir elektroninių ryšių[919] 2009 m. pakeitimuose buvo įtvirtintos šios nuostatos:

- nustatyti apribojimai siunčiant tiesioginės rinkodaros e. laiškus, kurie pradėti taikyti trumpiesiems pranešimams, daugiaformačiams pranešimams ir kitokių rūšių panašioms priemonėms; rinkodaros e. laiškai draudžiami, išskyrus atvejus, kai buvo gautas išankstinis sutikimas. Be tokio sutikimo rinkodaros e. laiškai gali būti siunčiami tik ankstesniems klientams, jeigu jie nurodė savo e. pašto adresą ir sutinka gauti tokius laiškus.

- Valstybės narės privalėjo numatyti teismines teisių gynimo priemones už draudimo teikti neužsakytus pranešimus pažeidimus[920].

919 2009 m. lapkričio 25 d. Europos Parlamento ir Tarybos direktyva 2009/136/EB, iš dalies keičianti Direktyvą 2002/22/EB dėl universaliųjų paslaugų ir paslaugų gavėjų teisių, susijusių su elektroninių ryšių tinklais ir paslaugomis, Direktyvą 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje ir Reglamentą (EB) Nr. 2006/2004 dėl nacionalinių institucijų, atsakingų už vartotojų apsaugos teisės aktų vykdymą, bendradarbiavimo, OL L 337, 2009.

920 Žr. iš dalies pakeistą direktyvos 13 straipsnį.

- Be kompiuterio naudotojo sutikimo nebeleidžiama nustatyti slapukų – programinės įrangos, kuria stebimi ir įrašomi kompiuterio naudotojo veiksmai. Nacionalinėje teisėje turėtų būti išsamiau reglamentuota, kaip turėtų būti išreikštas ir gautas sutikimas, kad būtų suteikta pakankama apsauga[921].

Jeigu dėl neteisėtos prieigos padaromas duomenų saugumo pažeidimas, prarandami arba sunaikinami duomenys, apie tai nedelsiant būtina pranešti kompetentingai priežiūros institucijai. Abonentus privaloma informuoti tais atvejais, kai dėl duomenų saugumo pažeidimo jiems gali būti padaryta žala[922].

Pagal Duomenų saugojimo direktyvą[923] reikalaujama, kad ryšio paslaugų teikėjai saugotų metaduomenis. Tačiau šią direktyvą panaikino ESTT (daugiau informacijos žr. 8.3 skirsnyje).

Ateities perspektyvos

2017 m. sausio mėn. Europos Komisija priėmė naują pasiūlymą dėl E. privatumo reglamento, kuris pakeis senąją E. privatumo direktyvą. Apsaugos tikslas išlieka „fizinių ir juridinių asmenų pagrindinių teisių ir laisvių, visų pirma teisių į privatų gyvenimą ir komunikacijos slaptumą, apsaug[a] teikiant ir naudojant elektroninių ryšių paslaugas ir dėl fizinių asmenų apsaugos tvarkant asmens duomenis“. Kartu naujuoju pasiūlymu siekiama užtikrinti laisvą elektroninių ryšių duomenų ir elektroninių ryšių paslaugų judėjimą Sąjungoje[924]. Nors Bendrajame duomenų apsaugos reglamente visų pirma aptariamas ES pagrindinių teisių chartijos 8 straipsnis, siūlomu reglamentu siekiama į ES antrinę teisę įtraukti Chartijos 7 straipsnį.

Reglamentu ankstesnės direktyvos nuostatos būtų pritaikytos prie naujų technologijų ir rinkos realijų ir būtų sukurta išsami ir nuosekli sistema, atitinkanti Bendrąjį duomenų apsaugos reglamentą. Šia prasme E. privatumo reglamentas būtų

921 Žr. *ten pat*, 5 straipsnis.; taip pat žr. 29 straipsnio darbo grupės (2012 m.) *Nuomonę 04/2012 dėl slapukams taikomos reikalavimo gauti sutikimą išimties*, WP 194, Briuselis, 2012 m. birželio 7 d.

922 Taip pat žr. 29 straipsnio darbo grupės (2011 m.) *Darbo dokumentą Nr. 01/2011 dėl dabartinės ES asmens duomenų pažeidimo sistemos ir rekomendacijų dėl būsimų politikos pokyčių*, WP 184, Briuselis, 2011 m. balandžio 5 d.

923 2006 m. kovo 15 d. Europos Parlamento ir Tarybos direktyva 2006/24/EB dėl duomenų, generuojamų arba tvarkomų teikiant Viešai prieinamas elektroninių ryšių paslaugas arba viešuosius ryšių tinklus, saugojimo ir iš dalies keičianti Direktyvą 2002/58/EB, OL L 105, 2006.

924 Pasiūlymas dėl Europos Parlamento ir Tarybos reglamento dėl teisės į privatų gyvenimą ir asmens duomenų apsaugos elektroninių ryšių sektoriuje, kuriuo panaikinama Direktyva 2002/58/EB (Reglamentas dėl privatumo ir elektroninių ryšių) (COM(2017) 10 *final*), 1 straipsnis.

Bendrojo duomenų apsaugos reglamento *lex specialis*, kuriuo pastarasis reglamentas būtų pritaikytas prie elektroninių ryšių duomenų, kurie laikomi asmens duomenimis. Naujasis reglamentas apima „elektroninių ryšių duomenis“, įskaitant elektroninių ryšių turinį ir metaduomenis, kurie nebūtinai yra asmens duomenys. Teritorinė taikymo sritis apima tik ES, įskaitant atvejus, kai ES gauti duomenys tvarkomi už jos ribų, ir apima virštinklinių paslaugų teikėjus. Tai paslaugų teikėjai, teikiantys turinį, paslaugas ar taikomąsias programas internetu, tiesiogiai nedalyvaujant tinklo operatoriui ar interneto paslaugų teikėjui. Tokių paslaugų teikėjų pavyzdžiai: *Skype* (balso ir vaizdo skambučiai), *WhatsApp* (pranešimų siuntimas), *Google* (paieška), *Spotify* (muzika) arba *Netflix* (vaizdo turinys). Naujajam reglamentui būtų taikomi Bendrajame duomenų apsaugos reglamente nustatyti vykdymo užtikrinimo mechanizmai.

E. privatumo reglamentą numatyta priimti iki 2018 m. gegužės 25 d., nes iki šios datos Bendrasis duomenų apsaugos reglamentas bus taikomas visose 28 valstybėse narėse. Tačiau tam turi pritarti ir Europos Parlamentas, ir Taryba[925].

9.2. Įdarbinimo duomenys

Pagrindiniai faktai

- Konkrečios duomenų apsaugos darbo santykių srityje taisyklės išdėstytos ET rekomendacijoje dėl užimtumo duomenų.
- Bendrajame duomenų apsaugos reglamente darbo santykiai konkrečiai nurodomi tik tvarkant neskelbtinus duomenis.
- Sutikimo, kuris turi būti duotas laisva valia, kaip duomenų apie darbuotojus tvarkymo teisinio pagrindo, galiojimas gali būti abejotinas, atsižvelgiant į tai, kad darbdavio ir darbuotojų ekonominė galia nėra vienoda. Sutikimo aplinkybės turi būti atidžiai įvertintos.

Su darbo santykiais susijusiam duomenų tvarkymui taikomi bendrieji ES teisės aktai dėl asmens duomenų apsaugos. Tačiau viename reglamente[926] reglamentuojama būtent asmens duomenų apsauga, kai juos Europos institucijos tvarko (be kita ko)

925 Daugiau informacijos žr. Europos Komisijos (2017 m.) pranešime spaudai „Komisija siūlo visų tipų elektroniniams ryšiams taikyti griežtas privatumo taisykles ir atnaujina ES institucijoms taikomas duomenų apsaugos taisykles“, 2017 m. sausio 10 d.

926 2000 m. gruodžio 18 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 45/2001 dėl asmenų apsaugos Bendrijos institucijoms ir įstaigoms tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo, OL L 8, 2001.

įdarbindamos asmenis. Bendrajame duomenų apsaugos reglamente darbo santykiai konkrečiai minimi 9 straipsnio 2 dalyje, kurioje nurodyta, kad asmens duomenys gali būti tvarkomi duomenų valdytojui arba duomenų subjektui vykdant pareigas arba įgyvendinant konkrečias teises įdarbinimo srityje.

Pagal Bendrąjį duomenų apsaugos reglamentą darbuotojui turėtų būti suteikta galimybė aiškiai atskirti duomenis, dėl kurių jis savanoriškai sutinka, kad jie būtų tvarkomi ir (arba) saugomi, ir jų saugojimo tikslus. Darbuotojai taip pat turėtų būti informuoti apie jų teises ir duomenų saugojimo trukmę prieš duodant sutikimą. Jeigu tikėtina, kad dėl asmens duomenų saugumo pažeidimo kils didelis pavojus fizinių asmenų teisėms ir laisvėms, darbdavys privalo apie šį pažeidimą pranešti darbuotojui. Pagal reglamento 88 straipsnį valstybėms narėms leidžiama nustatyti konkretesnes taisykles, kuriomis užtikrinama darbuotojų teisių ir laisvių į pagarbą jų asmens duomenims apsauga.

Pavyzdys. Byloje *Worten*[927] duomenys buvo kaupiami darbo laiko apskaitos žiniaraštyje, kuriame nurodytas kasdienis darbas ir poilsio laikas, kurie yra asmens duomenys. Pagal nacionalinę teisę gali būti reikalaujama, kad darbdavys pateiktų darbo laiko apskaitos žiniaraščius nacionalinėms institucijoms, atsakingoms už darbo sąlygų stebėseną. Tai sudarytų sąlygas tiesiogiai susipažinti su atitinkamais asmens duomenimis. Tačiau galimybė susipažinti su asmens duomenimis yra būtina, kad nacionalinė institucija galėtų stebėti, kaip laikomasi darbo sąlygas reglamentuojančių teisės aktų[928].

Kalbant apie **ET**, pažymėtina, kad 1989 m. buvo paskelbta Rekomendacija dėl įdarbinimo duomenų, kuri buvo peržiūrėta 2015 m.[929] Rekomendacijoje aptariamas asmens duomenų tvarkymas įdarbinimo tikslais privačiajame ir viešajame sektoriuose. Duomenų tvarkymas turi atitikti tam tikrus principus ir apribojimus, pavyzdžiui, skaidrumo ir konsultavimosi su darbuotojų atstovais principą, prieš įdiegiant kontrolės sistemas darbo vietoje. Rekomendacijoje taip pat teigiama, kad darbdaviai turėtų taikyti prevencines priemones, pavyzdžiui, filtrus, o ne stebėti, kaip darbuotojai naudojasi internetu.

927 ESTT, C-342/12, *Worten – Equipamentos para o Lar SA prieš Autoridade para as Condições de Trabalho (ACT)*, 2013 gegužės 30 d., 19 punktas.

928 *Ten pat*, 43 punktas.

929 Europos Taryba, Ministrų Komitetas (2015 m.), Rekomendacija *Rec(2015)5* valstybėms narėms dėl asmens duomenų tvarkymo įdarbinimo srityje, 2015 m. balandžio mėn.

Dažniausiai pasitaikančių su užimtumu susijusių duomenų apsaugos problemų apžvalga pateikiama 29 straipsnio darbo grupės darbiniame dokumente[930]. Darbo grupė analizavo sutikimo, kaip teisinio įdarbinimo duomenų tvarkymo pagrindo svarbą[931]. Ji nustatė, kad ekonominės pusiausvyros nebuvimas tarp sutikimo prašančio darbdavio ir sutikimą duodančio darbuotojo dažnai kelia abejonių dėl to, ar sutikimas buvo duotas laisva valia. Todėl aplinkybės, kuriomis sutikimu remiamasi kaip duomenų tvarkymo teisiniu pagrindu, turėtų būti atidžiai apsvarstytos vertinant sutikimo galiojimą darbo santykių srityje.

Bendra duomenų apsaugos problema tipinėje šiandienos darbo aplinkoje yra darbuotojų elektroninių ryšių teisėtos stebėsenos mastas darbo vietoje. Dažnai teigiama, kad šią problemą galima lengvai išspręsti draudžiant darbe naudoti asmeninę ryšių įrangą. Tačiau toks bendras draudimas galėtų būti neproporcingas ir nerealus. Šiomis aplinkybėmis ypač svarbūs EŽTT sprendimai *Copland prieš Jungtinę Karalystę* ir *Bărbulescu prieš Rumuniją*.

Pavyzdys. Byloje *Copland prieš Jungtinę Karalystę*[932] nurodyta, kad buvo slapta stebima, kaip koledžo darbuotoja naudojasi telefonu, e. paštu ir internetu, siekiant nustatyti, ar ji ne per daug naudojasi koledžo infrastruktūra asmeniniais tikslais. EŽTT nusprendė, kad telefono skambučiams iš įmonės patalpų buvo taikomos privataus gyvenimo ir susirašinėjimo sąvokos. Todėl tokie iš darbo siunčiami kvietimai ir e. laiškai, taip pat informacija, gauta stebint asmeninį interneto naudojimą, buvo saugomi pagal EŽTK 8 straipsnį. Pareiškėjos byloje negaliojo jokios nuostatos, reglamentuojančios aplinkybes, kuriomis darbdaviai galėtų stebėti, kaip darbuotojai naudojasi telefonu, e. paštu ir internetu. Todėl apribojimas neatitiko įstatymo. Teismas padarė išvadą, kad buvo pažeistas EŽTK 8 straipsnis.

Pavyzdys. Byloje *Bărbulescu prieš Rumuniją*[933] pareiškėjas buvo atleistas iš darbo dėl to, kad darbo vietoje naudojosi internetu ir taip pažeidė nacionalines taisykles. Jo darbdavys stebėjo jo ryšius. Įrašai, kuriuose pateikiami grynai privataus pobūdžio pranešimai, buvo pateikti nagrinėjant nacionalinę

930 29 straipsnio darbo grupė (2017 m.), *Nuomonė Nr. 2/2017 dėl duomenų tvarkymo darbe*, WP 249, Briuselis, 2017 m. birželio 8 d.

931 29 straipsnio darbo grupė (2005 m.), *Darbo dokumentas dėl 1995 m. spalio 24 d. Direktyvos 95/46/EB 26 straipsnio 1 dalies vienodo aiškinimo*, WP 114, Briuselis, 2005 m. lapkričio 25 d.

932 EŽTT, *Copland prieš Jungtinę Karalystę*, Nr. 62617/00, 2007 m. balandžio 3 d.

933 EŽTT, *Bărbulescu prieš Rumuniją*(DK), Nr. 61496/08, 2017 m. rugsėjo 5 d., 121 punktas.

bylą. Prieidamas prie išvados, kad 8 straipsnis turi būti taikomas, EŽTT neatsakė į klausimą, ar dėl darbdavio ribojamųjų nuostatų pareiškėjas pagrįstai galėjo tikėtis privatumo, tačiau nusprendė, kad darbdavio nurodymai negali sumažinti privataus socialinio gyvenimo darbo vietoje iki nulio.

Iš esmės susitariančiosioms valstybėms turėjo būti suteikta plati veiksmų laisvė vertinant poreikį nustatyti teisinę sistemą, reglamentuojančią sąlygas, kuriomis darbdavys galėtų reguliuoti savo darbuotojų neprofesinius elektroninius ar kitokios formos ryšius darbo vietoje. Vis dėlto nacionalinės institucijos turėjo užtikrinti, kad darbdavio nustatytos susirašinėjimo ir kitų ryšių stebėsenos priemonės, nepaisant jų masto ir trukmės, taip pat apimtų tinkamas ir pakankamas apsaugos nuo piktnaudžiavimo priemones. Proporcingumas ir procedūrinės garantijos prieš savivalę buvo esminės ir EŽTT nustatė įvairius šiomis aplinkybėmis svarbius veiksnius. Tai, be kita ko, apėmė darbdavio vykdomos darbuotojų stebėsenos mastą ir darbuotojų privatumo apribojimo laipsnį, pasekmes darbuotojui ir tai, ar buvo numatytos tinkamos apsaugos priemonės. Be to, nacionalinės institucijos turėjo užtikrinti, kad darbuotojas, kurio ryšiai buvo stebimi, turėtų galimybę pasinaudoti teisių gynimo priemone teisminėje institucijoje, kuri turi jurisdikciją bent jau iš esmės nustatyti, kaip buvo laikomasi šių išdėstytų kriterijų ir ar ginčijamos priemonės buvo teisėtos.

Šioje byloje EŽTT nustatė, kad 8 straipsnis buvo pažeistas, nes nacionalinės institucijos nesuteikė pareiškėjo teisei į jo privatų gyvenimą ir susirašinėjimo slaptumą tinkamos apsaugos, taigi nesugebėjo nustatyti tinkamos aptariamų interesų pusiausvyros.

Pagal ET rekomendaciją dėl įdarbinimo surinkti asmens duomenys iš asmens turėtų būti gaunami tiesiogiai.

Įdarbinimo tikslu surinkti asmens duomenys turi apimti tik informaciją, kuri yra būtina siekiant įvertinti kandidatų tinkamumą ir jų karjeros potencialą.

Rekomendacijoje taip pat konkrečiai užsimenama apie kritinius duomenis, susijusius su atskirų darbuotojų darbu arba potencialu. Vertinamieji duomenys turi būti pagrįsti teisingais ir sąžiningais vertinimais ir jų formuluotė negali žeisti asmens. To reikalaujama pagal sąžiningo duomenų tvarkymo ir duomenų tikslumo principus.

Ypatingas duomenų apsaugos teisės aspektas, atsižvelgiant į darbdavio ir darbuotojo santykius, yra susijęs su darbuotojų atstovų vaidmeniu. Tokie atstovai gali gauti darbuotojų asmens duomenis tik tiek, kiek tai yra būtina, kad jie galėtų atstovauti darbuotojų interesams, arba jei tokie duomenys yra būtini kolektyvinėse sutartyse nustatytiems įpareigojimams vykdyti arba priežiūros tikslais.

Darbo tikslais surinkti neskelbtini asmens duomenys gali būti tvarkomi tik ypatingais atvejais ir laikantis nacionalinėje teisėje nustatytų apsaugos priemonių. Darbdaviai gali klausti darbuotojų arba darbo ieškančių asmenų apie jų sveikatos būklę arba juos mediciniškai apžiūrėti tik tada, kai tai būtina. Tai gali būti daroma siekiant nustatyti jų tinkamumą dirbti; įgyvendinti prevencinės medicinos reikalavimus; apsaugoti gyvybinius duomenų subjekto arba kitų darbuotojų ir asmenų interesus; sudaryti sąlygas mokėti socialines išmokas arba atsakyti į teisminius prašymus. Asmens sveikatos duomenys negali būti renkami iš kitų šaltinių nei atitinkamas darbuotojas, išskyrus atvejus, kai buvo gautas aiškus informuoto asmens sutikimas arba kai tai numatyta nacionalinės teisės aktuose.

Pagal Rekomendaciją dėl įdarbinimo darbuotojus reikėtų informuoti apie jų asmens duomenų tvarkymo tikslą, surinktų asmens duomenų rūšį, subjektus, kuriems duomenys reguliariai perduodami, ir tokio duomenų atskleidimo tikslą ir teisinį pagrindą. Prieiga prie elektroninių ryšių darbo vietoje gali būti suteikiama tik saugumo sumetimais arba dėl kitų teisėtų priežasčių, ir tokia prieiga leidžiama tik darbuotojus informavus, kad darbdavys gali naudotis tokios rūšies ryšiais.

Darbuotojams turi būti suteikiama teisė susipažinti su savo įdarbinimo duomenimis, taip pat teisė reikalauti, kad duomenys būtų ištaisyti arba sunaikinti. Jeigu tvarkomi vertinamieji duomenys, darbuotojai turi turėti teisę ginčyti vertinimą. Tačiau šios teisės laikinai gali būti ribojamos siekiant atlikti vidaus tyrimus. Jei atsisakoma darbuotojui leisti susipažinti su asmeniniais įdarbinimo duomenimis, juos ištaisyti arba sunaikinti, nacionalinėje teisėje turi būti numatytos tinkamos tokio atsisakymo ginčijimo procedūros.

9.3. Asmens sveikatos duomenys

Pagrindinis faktas

- Medicininiai duomenys yra neskelbtini duomenys, todėl jiems taikoma speciali apsauga.

Asmens duomenys, susiję su duomenų subjekto sveikata, laikomi neskelbtinais duomenimis pagal Bendrojo duomenų apsaugos reglamento 9 straipsnio 1 dalį ir atnaujintos 108-osios konvencijos 6 straipsnį. Atitinkamai su sveikata susijusiems duomenims taikoma griežtesnė duomenų tvarkymo tvarka, palyginti su įprastais duomenimis. Pagal Bendrąjį duomenų apsaugos reglamentą draudžiama tvarkyti „asmens sveikatos duomenis“ (kurie suprantami kaip „visi duomenys apie duomenų subjekto sveikatos būklę, kurie atskleidžia informaciją apie duomenų subjekto buvusią, esamą ar būsimą fizinę ar psichinę sveikatą“)[934], taip pat genetinius duomenis ir biometrinius duomenis, išskyrus atvejus, kai tai yra leidžiama pagal 9 straipsnio 2 dalį. Į „specialių kategorijų duomenų“ sąrašą įtraukti abiejų rūšių duomenys[935].

Pavyzdys. Byloje *Z prieš Suomiją*[936] buvęs pareiškėjos vyras, kuris buvo užsikrėtęs ŽIV, padarė keletą seksualinių nusikaltimų. Vėliau jis buvo nuteistas už žmogžudystę remiantis tuo, kad sąmoningai kėsinosi užkrėsti savo aukas ŽIV. Nacionalinis teismas nurodė, kad visas teismo sprendimas ir bylos dokumentai lieka konfidencialūs 10 metų, nepaisant pareiškėjos prašymų dėl ilgesnio konfidencialumo laikotarpio. Apeliacinis teismas atmetė šiuos prašymus ir savo sprendime nurodė pareiškėjos ir jos buvusio vyro vardus ir pavardes. EŽTT nusprendė, kad apribojimas nebuvo būtinas demokratinėje visuomenėje, nes medicininių duomenų apsauga turėjo esminę reikšmę galimybei naudotis teise į privatų ir šeimos gyvenimą, visų pirma kiek tai susiję su informacija apie ŽIV užkratą, atsižvelgiant į plačiai visuomenėje paplitusią su šia liga susijusią stigmą. Todėl EŽTT Teismas padarė išvadą, kad suteikus

934 Bendrojo duomenų apsaugos reglamento 35 konstatuojamoji dalis.

935 *Ten pat*, 2 straipsnis.

936 EŽTT, *Z prieš Suomiją*, Nr. 22009/93, 1997 m. vasario 25 d., 94 ir 112 punktai; taip pat žr. EŽTT, *M. S. prieš Švediją*, Nr. 20837/92, 1997 m. rugpjūčio 27 d.; EŽTT, *L. L. prieš Prancūziją*, Nr. 7508/02, 2006 m. spalio 10 d.; EŽTT, *I prieš Suomiją*, Nr. 20511/03, 2008 m. liepos 17 d.; EŽTT, *K. H. ir kt. prieš Slovakiją*, Nr. 32881/04, 2009 m. balandžio 28 d.; EŽTT, *Szuluk prieš Jungtinę Karalystę*, Nr. 36936/05, 2009 m. birželio 2 d.

galimybę susipažinti su apeliacinio teismo sprendimu, kuriame apibūdinama pareiškėjos tapatybė ir sveikatos būklė, vos po 10 metų nuo sprendimo priėmimo būtų pažeistas EŽTK 8 straipsnis.

Pagal **ES teisę**, t. y. Bendrojo duomenų apsaugos reglamento 9 straipsnio 2 dalies h punktą, medicininius duomenis leidžiama tvarkyti, jeigu to reikalaujama profilaktinės medicinos, medicinos diagnozės, priežiūros arba gydymo paslaugų teikimo arba sveikatos priežiūros paslaugų valdymo tikslais. Tačiau duomenis tvarkyti leidžiama, tik jeigu tai daro sveikatos priežiūros specialistas, kuris privalo saugoti profesinę paslaptį, arba kitas asmuo, kuriam galioja lygiavertė prievolė.

ET teisėje, t. y. 1997 m. ET rekomendacijoje dėl medicininių duomenų, išsamiau aptariamas 108-osios konvencijos principų taikymas tvarkant duomenis medicinos srityje[937]. Siūlomos taisyklės atitinka Bendrąjį duomenų apsaugos reglamentą tiek, kiek tai susiję su teisėtais medicininių duomenų tvarkymo tikslais, būtinomis asmens sveikatos duomenis naudojančių asmenų pareigomis saugoti profesinę paslaptį ir duomenų subjektų teisėmis į skaidrumą ir galimybe susipažinti su duomenimis, juos ištaisyti ir ištrinti. Be to, medicininiai duomenys, kuriuos teisėtai tvarko sveikatos priežiūros specialistai, negali būti perduoti teisėsaugos institucijoms, išskyrus atvejus, kai numatomos „pakankamos apsaugos priemonės, kuriomis užkertamas kelias tam, kad duomenys nebūtų atskleisti <...> negerbiant teisės į privat[ų] gyvenim[ą], kuri garantuojama pagal EŽTK 8 straipsnį“[938]. Nacionalinės teisės aktai taip pat turi būti „suformuluoti pakankamai tiksliai ir jiems turi būti suteikta tinkama teisinė apsauga nuo savivalės“[939].

Be to, Rekomendacijoje dėl medicininių duomenų pateikiamos specialios nuostatos dėl negimusių vaikų ir neįgaliųjų medicininių duomenų, taip pat dėl genetinių duomenų tvarkymo. Neabejotinai pripažįstama, kad moksliniai tyrimai yra tinkama priežastis saugoti duomenis ilgiau nei reikia, nors paprastai tokiu atveju duomenis reikalaujama anoniminti. Rekomendacijos dėl medicininių duomenų 12 straipsnyje siūlomos išsamios taisyklės, taikytinos tais atvejais, kai tyrėjams reikia asmens duomenų, o anonimintų duomenų nepakanka.

937 Europos Taryba, Ministrų Komitetas (1997 m.), Rekomendacija *Rec(97)5* valstybėms narėms dėl medicininių duomenų apsaugos, 1997 m. vasario 13 d. Pastaba. Ši rekomendacija dabar peržiūrima.

938 EŽTT, *Avilkina ir kt. prieš Rusiją*, Nr. 1585/09, 2013 m. birželio 6 d., 53 punktas. Taip pat žr. EŽTT, *Biriuk prieš Lietuvą*, Nr. 23373/03, 2008 m. lapkričio 25 d.

939 EŽTT, *L. H. prieš Latviją*, Nr. 52019/07, 2014 m. balandžio 29 d., 59 punktas.

Pseudonimų suteikimas gali būti tinkama priemonė moksliniams poreikiams patenkinti ir kartu apsaugoti susijusio paciento interesus. Pseudonimų suteikimo koncepcija atsižvelgiant į duomenų apsaugą išsamiau paaiškinta 2.1.1 skirsnyje.

2016 m. ET rekomendacija dėl duomenų, gautų atlikus genetinius bandymus, taip pat taikoma duomenų tvarkymui medicinos srityje[940]. Ši rekomendacija labai svarbi e. sveikatai, kurioje IRT naudojamos mediciniai priežiūrai palengvinti. Pavyzdžiui, vienas sveikatos priežiūros paslaugų teikėjas siunčia paciento tėvystės tyrimo rezultatus kitam sveikatos priežiūros paslaugų teikėjui. Šia rekomendacija siekiama apsaugoti asmenų, kurių asmens duomenys tvarkomi draudimo tikslais, teises siekiant apsidrausti nuo rizikos, susijusios su asmens sveikata, fizine neliečiamybe, amžiumi ar mirtimi. Draudikai turi pagrįsti su sveikata susijusių duomenų tvarkymą ir jis turėtų būti proporcingas svarstomos rizikos pobūdžiui ir svarbai. Šios rūšies duomenų tvarkymas priklauso nuo tiriamojo asmens sutikimo. Draudikai taip pat turėtų turėti su sveikata susijusių duomenų saugojimo apsaugos priemones.

Klinikiniai tyrimai, kurie apima naujų vaistų poveikio pacientams vertinimą dokumentais pagrįstoje mokslinių tyrimų aplinkoje, turi didelį poveikį duomenų apsaugai. Žmonėms skirtų vaistų klinikiniai bandymai reguliuojami pagal 2014 m. balandžio 16 d. Europos Parlamento ir Tarybos reglamentą (ES) Nr. 536/2014 dėl žmonėms skirtų vaistų klinikinių tyrimų, kuriuo panaikinama Direktyva 2001/20/EB (Klinikinių tyrimų reglamentas)[941]. Pagrindiniai Klinikinių tyrimų reglamento elementai yra:

- supaprastinta paraiškų teikimo per ES portalą procedūra[942];
- paraiškų dėl klinikinių tyrimų vertinimo terminai[943];
- etikos komitetas, kuris yra vertinimo dalis, pagal valstybių narių teisę (ir Europos teisę, kurioje apibrėžiami susiję laikotarpiai)[944] ir

940 Europos Taryba, Ministrų Komitetas (2016 m.), Rekomendacija *Rec(2016)8* valstybėms narėms dėl asmens sveikatos duomenų tvarkymo draudimo tikslais, įskaitant genetinių tyrimų duomenis, 2016 m. spalio 26 d.

941 2014 m. balandžio 16 d. Europos Parlamento ir Tarybose reglamentą (ES) Nr. 536/2014 dėl žmonėms skirtų vaistų klinikinių tyrimų, kuriuo panaikinama Direktyva 2001/20/EB (Klinikinių tyrimų reglamentas), OL L158, 2014.

942 Klinikinių tyrimų reglamento 5 straipsnio 1 dalis.

943 *Ten pat*, 5 straipsnio 2–5 dalys.

944 *Ten pat*, 2 straipsnio 2 dalies 11 punktas.

- didesnis klinikinių tyrimų ir jų rezultatų skaidrumas[945].

Bendrajame duomenų apsaugos reglamente nustatyta, kad sutikimo dalyvauti klinikinių tyrimų mokslinių tyrimų veikloje tikslais taikomas Reglamentas (ES) Nr. 536/2014[946].

Šiuo metu rengiama nemažai kitų teisėkūros ir kitų iniciatyvų, susijusių su asmens duomenimis sveikatos sektoriuje[947].

Elektroniniai sveikatos įrašai

Elektroniniai sveikatos įrašai apibūdinami kaip „išsam[ū]s elektronini[ai] medicinos įraša[i] ar panaš[ū]s dokumenta[i] apie buvusią ir esamą asmens fizinę ir psichinę sveikatos būklę, kuri[ų] duomenimis galima lengvai pasinaudoti medicininio gydymo ar kitais panašiais tikslais“[948]. Elektroniniai sveikatos įrašai – tai elektroninės pacientų sveikatos istorijos versijos, kuriose gali būti pateikiami klinikiniai duomenys, susiję su šiais asmenimis, pavyzdžiui, ankstesnė sveikatos istorija, problemos ir būklė, vaistai ir gydymas, taip pat tyrimų ir laboratorinių bandymų rezultatai ir pranešimai. Šios elektroninės rinkmenos gali apimti tiek išsamius įrašus, tiek trumpas ištraukas ar santraukas ir su jomis gali susipažinti bendrosios praktikos gydytojas, vaistininkas ir kiti sveikatos priežiūros specialistai. „E. sveikatos“ koncepcija taip pat apima šiuos sveikatos įrašus.

Pavyzdys. A sudarė draudimo sutartį su draudimo bendrove B. Pastaroji rinks iš A tam tikrą su sveikata susijusią informaciją, pavyzdžiui, apie sveikatos problemas ar ligas. Draudimo bendrovė turėtų saugoti su A sveikata susijusius asmens duomenis atskirai nuo kitų duomenų. Draudimo bendrovė taip pat turi saugoti su sveikata susijusius asmens duomenis atskirai nuo kitų asmens duomenų. Tai reiškia, kad tik A bylos tvarkytojas turės prieigą prie A sveikatos duomenų.

945 *Ten pat*, 9 straipsnio 1 punktas ir 67 konstatuojamoji dalis.

946 Bendrojo duomenų apsaugos reglamento 156 ir 161 konstatuojamosios dalys.

947 EDAPP (2013 m.), *Europos duomenų apsaugos priežiūros pareigūno nuomonė dėl Komisijos komunikato „2012–2020 m. e. sveikatos veiksmų planas. Novatoriška sveikatos priežiūra XXI amžiui“*, Briuselis, 2013 m. kovo 27 d.

948 2008 m. liepos 2 d. Komisijos rekomendacijos dėl tarpvalstybinio elektroninių sveikatos įrašų sistemų suderinamumo 3 dalies c punktas.

Vis dėlto elektroninės sveikatos bylos kelia tam tikrų duomenų apsaugos problemų, pavyzdžiui, dėl jų prieinamumo, tinkamo saugojimo ir duomenų subjekto prieigos.

Be elektroninių sveikatos įrašų, 2014 m. balandžio 10 d. Europos Komisija paskelbė Žaliąją knygą dėl mobiliosios sveikatos (m. sveikata), manydama, kad m. sveikata yra besiformuojanti ir sparčiai auganti sritis, galinti pakeisti sveikatos priežiūrą ir padidinti jos veiksmingumą bei kokybę. Terminas apima mobiliaisiais prietaisais, pavyzdžiui, mobiliaisiais telefonais, pacientų stebėjimo prietaisais, asmeniniais skaitmeniniais pagalbiniais prietaisais ir kitais belaidžiais prietaisais, taip pat taikomosiomis programomis (pavyzdžiui, gerovės taikomosiomis programomis), kurios gali būti prijungtos prie medicinos prietaisų ar jutiklių, palaikomą medicinos ir visuomenės sveikatos praktiką[949]. Dokumente išdėstomi pavojai teisei į asmens duomenų apsaugą, kurie galėtų kilti dėl m. sveikatos raidos, ir numatoma, kad, atsižvelgiant į sveikatos duomenų neskelbtiną pobūdį, kuriant duomenis turėtų būti numatytos konkrečios ir tinkamos pacientų duomenų apsaugos priemonės, pavyzdžiui, šifravimas, ir tinkami pacientų autentiškumo patvirtinimo mechanizmai, kad būtų sumažinta saugumo rizika. Siekiant didinti pasitikėjimą m. sveikatos sprendimais, labai svarbu laikytis asmens duomenų apsaugos taisyklių, įskaitant prievolę informuoti duomenų subjektą apie duomenų saugumą ir teisėto asmens duomenų tvarkymo principą[950]. Šiuo tikslu pramonės atstovai parengė elgesio kodeksą, grindžiamą įvairių suinteresuotųjų subjektų indėliu, į kurį įtraukti atstovai, turintys patirties duomenų apsaugos, savireguliavimo ir bendro reguliavimo, IRT ir sveikatos priežiūros srityse[951]. Tuo metu, kai buvo rengiamas vadovas, elgesio kodekso projektas buvo pateiktas 29 straipsnio duomenų apsaugos darbo grupei pastaboms pateikti, kol jis bus oficialiai patvirtintas.

949 Europos Komisija (2014 m.), Žalioji knyga dėl mobiliosios sveikatos (m. sveikata), COM(2014) 219 *final*, Briuselis, 2014 m. balandžio 10 d.

950 *Ten pat*, p. 8.

951 Elgesio kodekso dėl mobiliųjų sveikatos priežiūros programų privatumo projektas, 2016 m. birželio 7 d.

9.4. Duomenų tvarkymas moksliniais ir statistiniais tikslais

Pagrindiniai faktai

- Statistinių, mokslinių ar istorinių tyrimų tikslais surinkti duomenys negali būti naudojami jokiais kitais tikslais.
- Teisėtai bet kokiu tikslu surinkti duomenys gali būti toliau naudojami statistikos, mokslinių ar istorinių tyrimų tikslais, jei taikomos tinkamos apsaugos priemonės. Šiuo tikslu šias apsaugos priemones gali suteikti nuasmeninimas arba pseudonimų suteikimas prieš perduodant duomenis trečiosioms šalims.

Pagal **ES teisę** duomenis leidžiama tvarkyti statistiniais, mokslinių ar istorinių tyrimų tikslais, jei taikomos tinkamos duomenų subjektų teisių ir laisvių apsaugos priemonės. Šios priemonės gali apimti pseudonimų suteikimą[952]. ES teisėje arba nacionalinėje teisėje gali būti numatytos tam tikros nuo duomenų subjektų teisių nukrypti leidžiančios nuostatos, jei dėl šių teisių gali būti neįmanoma arba labai sukliudyta pasiekti teisėtą mokslinių tyrimų tikslą[953]. Gali būti nustatytos nuostatos, leidžiančios nukrypti nuo duomenų subjekto teisės susipažinti su duomenimis, teisės reikalauti ištaisyti duomenis, teisės apriboti duomenų tvarkymą ir teisės prieštarauti.

Nors duomenų valdytojas gali pakartotinai naudoti teisėtai bet kokiu tikslu surinktus duomenis savo statistikos, mokslinių ar istorinių tyrimų tikslais, duomenys turėtų būti nuasmeninti arba jiems turėtų būti taikomos tokios priemonės, kaip pseudonimų suteikimas, priklausomai nuo konteksto, prieš juos perduodant trečiajai šaliai statistinių, mokslinių ar istorinių tyrimų tikslais, išskyrus atvejus, kai duomenų subjektas su tuo sutiko arba tai konkrečiai numatyta nacionalinėje teisėje. Duomenims, kuriems taikomas pseudonimų suteikimas, priešingai nei anoniminiams duomenims, toliau taikomas Bendrasis duomenų apsaugos reglamentas[954].

Taigi reglamente moksliniams tyrimams nustatyta speciali tvarka, susijusi su bendrosiomis duomenų apsaugos taisyklėmis, siekiant išvengti mokslinių tyrimų plėtros apribojimų ir įgyvendinti tikslą sukurti Europos mokslinių tyrimų erdvę, kaip nustatyta SESV 179 straipsnyje. Jame numatytas platus asmens duomenų tvarkymo

952 Bendrojo duomenų apsaugos reglamento 89 straipsnio 1 punktas.

953 *Ten pat*, 89 straipsnio 2 dalis.

954 *Ten pat*, 26 konstatuojamoji dalis.

mokslinių tyrimų tikslais aiškinimas, įskaitant technologijų plėtrą ir demonstravimą, fundamentinius tyrimus, taikomuosius mokslinius tyrimus ir privačiai finansuojamus mokslinius tyrimus. Reglamente taip pat pripažįstama duomenų rinkimo registruose mokslinių tyrimų tikslais svarba ir tai, kad renkant duomenis gali būti sunku visapusiškai nustatyti vėlesnį asmens duomenų tvarkymo mokslinių tyrimų tikslais tikslą[955]. Dėl šios priežasties reglamentu leidžiama tvarkyti duomenis šiais tikslais be duomenų subjektų sutikimo, jei taikomos atitinkamos apsaugos priemonės.

Svarbus duomenų naudojimo statistikos tikslais pavyzdys yra oficiali statistika, kurią pagal nacionalinius ir ES teisės aktus dėl oficialios statistikos gauna nacionaliniai ir ES statistikos biurai. Pagal šiuos teisės aktus piliečiai ir įmonės paprastai privalo atskleisti duomenis atitinkamoms statistikos institucijoms. Statistikos biuruose dirbantiems pareigūnams taikomos specialios prievolės saugoti profesinę paslaptį, kurių turi būti tinkamai laikomasi, nes jos yra labai svarbios siekiant aukšto piliečių pasitikėjimo, kuris būtinas, kad duomenys būtų prieinami statistikos institucijoms[956].

Reglamente (EB) Nr. 223/2009 dėl Europos statistikos (Europos statistikos reglamente) nustatytos esminės duomenų apsaugos taisyklės, susijusios su oficialia statistika, todėl jis taip pat gali būti laikomas susijusiu su nuostatomis dėl oficialios statistikos nacionaliniu lygmeniu[957]. Reglamente išlaikomas principas, kad oficialiai statistikos veiklai reikalingas pakankamai aiškus teisinis pagrindas[958].

Pavyzdys. Byloje *Huber prieš Bundesrepublik Deutschland*[959] Austrijos verslininkas, persikėlęs į Vokietiją, skundėsi, kad Vokietijos valdžios institucijos, rinkdamos ir saugodamos užsienio piliečių asmens duomenis centriniame registre (AZR), taip pat statistiniais tikslais pažeidė jo teises pagal Duomenų

955 *Ten pat*, 33, 157 ir 159 konstatuojamosios dalys.

956 *Ten pat*, 90 straipsnis.

957 2009 m. kovo 11 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 223/2009 dėl Europos statistikos, panaikinantis Europos Parlamento ir Tarybos reglamentą (EB, Euratomas) Nr. 1101/2008 dėl konfidencialių statistinių duomenų perdavimo Europos Bendrijų statistikos tarnybai, Tarybos reglamentą (EB) Nr. 322/97 dėl Bendrijos statistikos ir Tarybos sprendimą 89/382/EEB, Euratomas, įsteigiantį Europos Bendrijų statistikos programų komitetą, OL L 87, 2009, su pakeitimais, padarytais 2015 m. balandžio 29 d. Europos Parlamento ir Tarybos reglamentu (ES) 2015/759, kuriuo iš dalies keičiamas Reglamentas (EB) Nr. 223/2009 dėl Europos statistikos, OL L 123, 2015.

958 Šis principas turi būti išsamiau apibūdintas Eurostato praktikos kodekse, kuriame pagal Europos statistikos reglamento 11 straipsnį pateikiamos etinės rekomendacijos, kaip rinkti oficialius statistinius duomenis, įskaitant atidų asmens duomenų naudojimą.

959 ESTT, C-524/06, *Heinz Huber prieš Bundesrepublik Deutschland* (DK), 2008 m. gruodžio 16 d.; visų pirma žr. 68 punktą.

apsaugos direktyvą. Atsižvelgdamas į tai, kad Direktyva 95/46/EB siekiama užtikrinti vienodą duomenų apsaugos lygį visose valstybėse narėse, ESTT nusprendė, kad, siekiant užtikrinti aukšto lygio apsaugą ES, 7 straipsnio e punkte vartojama būtinumo sąvoka negali turėti valstybėse narėse skirtingos prasmės. Taigi ši sąvoka Sąjungos teisėje turi savarankišką reikšmę ir turi būti aiškinama taip, kad visiškai atspindėtų Direktyvos 95/46/EB tikslą. ESTT, atkreipdamas dėmesį į tai, kad statistikos tikslais turėtų būti reikalaujama tik anoniminės informacijos, nusprendė, kad Vokietijos registras neatitinka 7 straipsnio e punkte nustatyto būtinumo reikalavimo.

ET kontekste tolesnis duomenų tvarkymas gali būti atliekamas moksliniais, istoriniais ar statistiniais tikslais, kai tai atitinka viešąjį interesą, ir jam turi būti taikomos tinkamos apsaugos priemonės[960]. Duomenų subjektų teisės taip pat gali būti apribotos, kai duomenys tvarkomi statistiniais tikslais, jei nėra akivaizdaus pavojaus, kad bus pažeistos jų teisės ir laisvės[961].

1997 m. paskelbtoje Rekomendacijoje dėl statistinių duomenų aptariami viešojo ir privačiojo sektorių statistinės veiklos rezultatai[962].

Duomenų valdytojas, kuris duomenis renka statistikos tikslais, negali jų naudoti kuriam nors kitam tikslui. Ne statistiniais tikslais surinkti duomenys gali būti naudojami tolesniam naudojimui statistikos tikslais. Pagal Rekomendaciją dėl statistinių duomenų taip pat leidžiama perduoti duomenis trečiosioms šalims, jei tai daroma tik statistikos tikslais. Tokiais atvejais šalys turėtų susitarime aprašyti teisėto tolesnio duomenų naudojimo statistiniais tikslais apimtį. Kadangi tai negali pakeisti duomenų subjekto sutikimo, jei reikia, nacionalinėje teisėje turi būti nustatytos tinkamos apsaugos priemonės, kad būtų kuo labiau sumažinta netinkamo asmens duomenų naudojimo rizika, pavyzdžiui, prievolė prieš atskleidžiant duomenis juos anoniminti arba pseudoniminti.

Statistikos srities mokslinių tyrimų specialistams pagal nacionalinę teisę turi būti taikomi specialūs profesinės paslapties saugojimo įpareigojimai, kaip paprastai daroma oficialios statistikos atveju. Tai turi būti taikoma ir apklausėjams bei kitiems asmens duomenų rinkėjams, jei jie dirba rinkdami duomenis iš duomenų subjektų ar kitų asmenų.

960 Atnaujintos 108-osios konvencijos 5 straipsnio 4 dalies b punktas.

961 *Ten pat*, 11 straipsnio 2 dalis.

962 Europos Taryba, Ministrų Komitetas (1997), Rekomendacija *Rec(97)18* valstybėms narėms dėl statistikos tikslais renkamų ir tvarkomų asmens duomenų apsaugos, 1997 m. rugsėjo 30 d.

Jeigu pagal įstatymą neleidžiama atlikti statistinio tyrimo naudojant asmens duomenis, duomenų subjektams gali tekti sutikti, kad jų duomenys būtų naudojami teisėtai, arba jiems gali reikėti suteikti galimybę nesutikti. Jei asmens duomenis statistiniais tikslais renka apklausėjai, jie turi būti aiškiai informuoti, ar pagal nacionalinę teisę duomenų teikimas yra privalomas.

Jei statistinio tyrimo negalima atlikti naudojant anoniminius duomenis ir yra reikalingi asmens duomenys, šiam tikslui surinkti duomenys turi būti kuo greičiau nuasmeninti. Statistinio tyrimo rezultatai turi būti tokie, kad bent jau nebūtų įmanoma nustatyti duomenų subjektų, išskyrus atvejus, kai tai akivaizdžiai nekelia jokio pavojaus.

Atlikus statistinę analizę, naudojami asmens duomenys turėtų būti ištrinti arba nuasmeninti. Tokiais atvejais Rekomendacijoje dėl statistinių duomenų rekomenduojama tapatybės nustatymo duomenis saugoti atskirai nuo kitų asmens duomenų. Tai reiškia, kad, pavyzdžiui, šifravimo raktas arba identifikavimo sinonimų sąrašas turi būti saugomi atskirai nuo kitų duomenų.

9.5. Finansiniai duomenys

Pagrindiniai faktai

- Nors finansiniai duomenys pagal atnaujintą 108-ąją konvenciją arba Bendrąjį duomenų apsaugos reglamentą nelaikomi neskelbtinais duomenimis, jiems tvarkyti reikalingos konkrečios apsaugos priemonės, kuriomis užtikrinamas tikslumas ir duomenų saugumas.
- Elektroninėse mokėjimo sistemose ypač reikalinga integruota duomenų apsauga, t. y. pritaikytoji arba standartizuotoji duomenų apsauga.
- Konkrečių duomenų apsaugos problemų šioje srityje gali kilti dėl būtinybės turėti tinkamus autentifikavimo mechanizmus.

Pavyzdys. Byloje *Michaud prieš Prancūziją*[963] ieškovas, Prancūzijos advokatas, ginčijo pagal Prancūzijos teisę jam tenkančią pareigą pranešti apie įtarimus dėl galimos jo klientų pinigų plovimo veiklos. EŽTT pažymėjo, kad

963 EŽTT, *Michaud prieš Prancūziją*, Nr. 12323/11, 2012 m. gruodžio 6 d. Taip pat žr. EŽTT, *Niemietz prieš Vokietiją*, Nr. 13710/88, 1992 m. gruodžio 16 d., 29 punktas, ir EŽTT, *Halford prieš Jungtinę Karalystę*, Nr. 20605/92, 1997 m. birželio 25 d., 42 punktas.

reikalavimas advokatams pateikti administracinėms institucijoms informaciją, susijusią su kitu asmeniu, kurią jie įgijo per savo profesinius mainus, yra advokato teisės į susirašinėjimą ir privatų gyvenimą pagal EŽTK 8 straipsnį apribojimas, nes ši sąvoka apima profesinio ar komercinio pobūdžio veiklą. Tačiau apribojimas atitiko įstatymą ir juo buvo siekiama teisėto tikslo, t. y. užkirsti kelią neramumams ir nusikaltimams. Atsižvelgdamas į tai, kad advokatai privalo pranešti apie įtartiną veiklą tik labai konkrečiomis aplinkybėmis, EŽTT nusprendė, kad ši pareiga yra proporcinga. EŽTT padarė išvadą, kad EŽTK 8 straipsnis nebuvo pažeistas.

Pavyzdys. Byloje *M. N. ir kiti prieš San Mariną*[964] pareiškėjas, Italijos pilietis, sudarė patikėtinio sutartį su bendrove, dėl kurios atliekamas tyrimas. Tai reiškė, kad bendrovėje buvo atlikta krata ir paimtos (elektroninių) dokumentų kopijos. Pareiškėjas San Marino teismui pateikė skundą, kuriame teigė, kad tarp jo ir įtariamų nusikaltimų nėra jokio ryšio. Tačiau teismas pripažino jo skundą nepriimtinu, nes jis nebuvo „suinteresuotoji šalis“. EŽTT nusprendė, kad pareiškėjas buvo labai nepalankioje padėtyje teisminės apsaugos atžvilgiu, palyginti su „suinteresuotąja šalimi“, tačiau jo duomenys vis dar buvo kratos ir poėmio operacijų objektas. Todėl EŽTT nusprendė, kad 8 straipsnis buvo pažeistas.

Pavyzdys. Byloje *G. S. B. prieš Šveicariją*[965] pareiškėjo banko sąskaitos duomenys buvo nusiųsti JAV mokesčių administratoriui remiantis Šveicarijos ir JAV administracinio bendradarbiavimo susitarimu. EŽTT nusprendė, kad perdavimas nepažeidžia EŽTK 8 straipsnio, nes pareiškėjo teisės į privatumą apribojimas buvo nustatytas įstatymu, juo buvo siekiama teisėto tikslo ir jis buvo proporcingas nagrinėjamam viešajam interesui.

Bendrosios teisinės duomenų apsaugos sistemos (išdėstytos 108-ojoje konvencijoje) taikymo mokėjimų srityje tvarka buvo išplėtota 1990 m. **ET** Rekomendacijoje *Rec(90)19*[966]. Šioje rekomendacijoje paaiškinama teisėto duomenų rinkimo ir naudojimo sritis mokėjimų srityje, ypač naudojant mokėjimo korteles. Joje taip pat pateikiamos išsamios rekomendacijos nacionalinės teisės aktų leidėjams dėl mokėjimo duomenų atskleidimo trečiosioms šalims taisyklių, duomenų saugojimo terminų, skaidrumo, duomenų saugumo ir tarpvalstybinių duomenų srautų, taip pat dėl

964 EŽTT, *M. N. ir kiti prieš San Mariną*, Nr. 28005/12, 2015 m. liepos 7 d.

965 EŽTT, *G. S. B. prieš Šveicariją*, Nr. 28601/11, 2015 m. gruodžio 22 d.

966 Europos Taryba, Ministrų Komitetas (1990 m.), Rekomendacija Nr. R(90)19 dėl mokėjimams ir kitoms susijusioms operacijoms naudojamų asmens duomenų apsaugos, 1990 m. rugsėjo 13 d.

priežiūros ir teisių gynimo priemonių. ET taip pat parengė nuomonę dėl mokesčių duomenų perdavimo[967], kurioje pateikiamos rekomendacijos ir klausimai, į kuriuos reikia atsižvelgti nagrinėjant mokesčių duomenų perdavimą.

EŽTT leidžia perduoti finansinius duomenis, visų pirma asmens banko sąskaitos duomenis, pagal EŽTK 8 straipsnį, jeigu tai numatyta teisės aktuose, jais siekiama teisėto tikslo ir jie yra proporcingi nagrinėjamam viešajam interesui[968].

Kalbant apie **ES teisę**, pažymėtina, kad elektroninio mokėjimo sistemos, kuriose tvarkomi asmens duomenys, turi atitikti Bendrąjį duomenų apsaugos reglamentą. Todėl šiose sistemose būtina užtikrinti pritaikytąją ir standartizuotąją duomenų apsaugą. Pagal pritaikytąją duomenų apsaugą duomenų valdytojas įpareigojamas nustatyti tinkamas technines ir organizacines priemones, kad įgyvendintų duomenų apsaugos principus. Standartizuotoji duomenų apsauga reiškia, kad duomenų valdytojas turi užtikrinti, kad standartizuotąja tvarka būtų galima tvarkyti tik tuos asmens duomenis, kurie yra būtini konkrečiam tikslui (žr. 4.4 skirsnį). Dėl finansinių duomenų pažymėtina, kad ESTT nusprendė, kad perduoti duomenys apie mokesčius gali reikšti asmens duomenis[969]. 29 straipsnio duomenų apsaugos darbo grupė parengė susijusias gaires valstybėms narėms, įskaitant kriterijus, kuriais užtikrinama, kad būtų laikomasi duomenų apsaugos taisyklių, kai automatiniu būdu automatiškai keičiamasi asmens duomenimis mokesčių tikslais[970]. Be to, priimta nemažai teisinių priemonių finansų rinkoms ir kredito įstaigų bei investicinių įmonių veiklai reguliuoti[971]. Kitos teisinės priemonės padeda kovoti su prekyba vertybiniais popieriais naudojantis

967 Europos Taryba, 108-osios konvencijos konsultacinis komitetas (2014 m.), Nuomonė dėl automatinio keitimosi duomenimis tarp valstybių mechanizmų poveikio duomenų apsaugai administravimo ir mokesčių tikslais, 2014 m. birželio 4 d.

968 EŽTT, *G. S. B. prieš Šveicariją*, Nr. 28601/11, 2015 m. gruodžio 22 d.

969 ESTT, C-201/14, *Smaranda Bara ir kt. prieš. Casa Națională de Asigurări de Sănătate ir kt.*, 2015 m. spalio 1 d., 29 punktas.

970 29 straipsnio duomenų apsaugos darbo grupė (2015 m.), 29 straipsnio darbo grupės pareiškimas dėl automatinio tarpvalstybinio keitimosi asmens duomenimis mokesčių tikslais, 14/EN WP 230.

971 2014 m. gegužės 15 d. Europos Parlamento ir Tarybos direktyva 2014/65/ES dėl finansinių priemonių rinkų, kuria iš dalies keičiamos Direktyva 2002/92/EB ir Direktyva 2011/61/ES, OL L 173, 2014; 2014 m. gegužės 15 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 600/2014 dėl finansinių priemonių rinkų, kuriuo iš dalies keičiamas Reglamentas (ES) Nr. 648/2012, OL L 173, 2014; 2013 m. birželio 26 d. Europos Parlamento ir tarybos direktyva 2013/36/ES dėl galimybės verstis kredito įstaigų veikla ir dėl riziką ribojančios kredito įstaigų ir investicinių įmonių priežiūros, kuria iš dalies keičiama Direktyva 2002/87/EB ir panaikinamos direktyvos 2006/48/EB bei 2006/49/EB, OL L 176, 2013.

viešai neatskleista informacija ir manipuliavimu rinka[972]. Pagrindinės sritys, kurios turi poveikį duomenų apsaugai, yra:

- finansinių sandorių įrašų saugojimas;
- asmens duomenų perdavimas trečiosioms šalims;
- pokalbių telefonu arba elektroninių ryšių įrašinėjimas, įskaitant kompetentingų institucijų įgaliojimus prašyti pateikti telefono ir srauto duomenų įrašus;
- asmeninės informacijos atskleidimas, įskaitant sankcijų paskelbimą;
- kompetentingų institucijų priežiūros ir tyrimų įgaliojimai, įskaitant patikrinimus vietoje ir patekimą į privačias patalpas siekiant paimti dokumentus;
- pranešimo apie pažeidimus mechanizmai, t. y. informavimo apie pažeidimus sistemos, ir
- valstybių narių kompetentingų institucijų ir Europos vertybinių popierių ir rinkos institucijos (EVPRI) bendradarbiavimas.

Taip pat konkrečiai aptariami kiti šios srities klausimai, įskaitant duomenų apie duomenų subjektų finansinę padėtį[973] arba tarpvalstybinius mokėjimus atliekant bankinius pavedimus rinkimą, kuris neišvengiamai yra susijęs su asmens duomenų judėjimu[974].

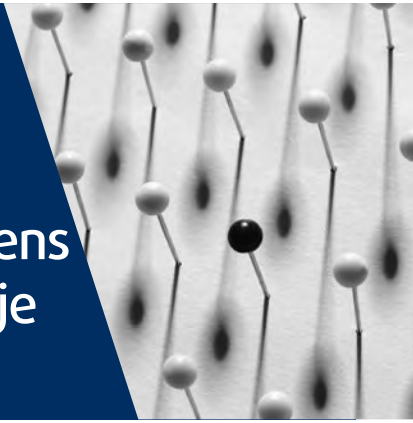
---

972 2014 m. balandžio 16 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 596/2014 dėl piktnaudžiavimo rinka (Piktnaudžiavimo rinka reglamentas) ir kuriuo panaikinama Europos Parlamento ir Tarybos direktyva 2003/6/EB ir Komisijos direktyvos 2003/124/EB, 2003/125/EB ir 2004/72/EB, OL L 173, 2014.

973 2009 m. rugsėjo 16 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 1060/2009 dėl kredito reitingų agentūrų, OL L 302, 2009, paskutinį kartą iš dalies pakeista 2014 m. balandžio 16 d. Europos Parlamento ir Tarybos direktyva, kuria iš dalies keičiamos direktyvų 2003/71/EB ir 2009/138/EB bei reglamentų (EB) Nr. 1060/2009, (ES) Nr. 1094/2010 bei (ES) Nr. 1095/2010 nuostatos, kiek tai susiję su Europos priežiūros institucijos (Europos draudimo ir profesinių pensijų institucijos) ir Europos priežiūros institucijos (Europos vertybinių popierių ir rinkų institucijos) įgaliojimais, OJ 2014 L 153; 2013 m. gegužės 21 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 462/2013, kuriuo iš dalies keičiamas Reglamentas (EB) Nr. 1060/2009 dėl kredito reitingų agentūrų, OL L 146, 2013.

974 2007 m. lapkričio 13 d. Europos Parlamento ir Tarybos direktyva 2007/64/EB dėl mokėjimo paslaugų vidaus rinkoje, iš dalies keičianti direktyvas 97/7/EB, 2002/65/EB, 2005/60/EB ir 2006/48/EB ir panaikinanti Direktyvą 97/5/EB, OL L 319, 2007, su pakeitimais, padarytais 2009 m. rugsėjo 16 d. Europos Parlamento ir Tarybos direktyva 2009/111/EB, iš dalies keičiančia direktyvas 2006/48/EB, 2006/49/EB ir 2007/64/EB dėl centrinių įstaigų kontroliuojamų bankų, tam tikrų nuosavų lėšų straipsnių, didelių pozicijų, priežiūros priemonių ir krizių valdymo, OL L 302, 2009.

10 Šiuolaikiniai iššūkiai asmens duomenų apsaugos srityje



Skaitmeniniame, arba informacinių technologijų, amžiuje plačiai naudojami kompiuteriai, internetas ir skaitmeninės technologijos. Tai apima didžiųjų duomenų, įskaitant asmens duomenis, rinkimą ir tvarkymą. Dėl asmens duomenų rinkimo ir tvarkymo globalizuotoje ekonomikoje daugėja tarpvalstybinių duomenų srautų. Toks duomenų tvarkymas gali duoti daug pastebimos naudos kasdieniame gyvenime: paieškos sistemos palengvina prieigą prie didelės apimties informacijos ir žinių, socialinių tinklų paslaugos suteikia galimybę viso pasaulio žmonėms bendrauti, reikšti nuomonę ir sutelkti paramą socialinėms, aplinkosaugos ir politinėms idėjoms, o įmonės ir vartotojai gauna naudos iš veiksmingų ir efektyvių rinkodaros metodų, kurie skatina ekonomiką. Technologijos ir asmens duomenų tvarkymas taip pat yra būtinos priemonės valstybės institucijoms kovojant su nusikalstamumu ir terorizmu. Be to, didieji duomenys – didelio kiekio informacijos rinkimas, saugojimas ir analizė siekiant nustatyti modelius ir prognozuoti elgseną – „gali būti didelės vertės visuomenei šaltinis, didinantis našumą, viešojo sektoriaus veiklos rezultatus ir socialinį dalyvavimą“[975].

Nepaisant daugialypės skaitmeninio amžiaus naudos, jis taip pat kelia privatumo ir duomenų apsaugos problemų, nes daugybė asmens duomenų renkama ir tvarkoma vis sudėtingesniais ir neskaidriais būdais. Dėl technologinės pažangos buvo sukurti didžiuliai duomenų rinkiniai, kuriuos galima lengvai sutikrinti ir toliau analizuoti ieškant modelių arba priimant algoritmais grindžiamus sprendimus, kurie gali suteikti precedento neturintį supratimą apie žmogaus elgesį ir asmeninį gyvenimą[976].

975 Europos Taryba, 108-osios konvencijos konsultacinis komitetas, *Gairės dėl asmenų apsaugos tvarkant asmens duomenis didžiųjų duomenų pasaulyje*, T-PD(2017)01, Strasbūras, 2017 m. sausio 23 d.

976 Europos Parlamentas (2017 m.), Rezoliucija „Didelių duomenų kiekių poveikis pagrindinėms teisėms: privatumas, duomenų apsauga, nediskriminavimas, saugumas ir teisėsauga“ (P8_TA-PROV(2017)0076, Strasbūras, 2017 m. kovo 14 d.

Naujos technologijos yra galingos ir gali būti ypač pavojingos, jei patektų į netinkamas rankas. Didelio poveikio, kurį šios technologijos gali daryti asmenų teisėms, pavyzdys – masinio sekimo veiklą vykdančios valstybės institucijos, kurios gali pasinaudoti šiomis technologijomis. 2013 m. Edwardo Snowdeno atskleista informacija apie žvalgybos agentūrų vykdomas didelio masto interneto ir telefoninių pokalbių sekimo programas kai kuriose valstybėse sukėlė didelį susirūpinimą dėl sekimo veiklos keliamo pavojaus privatumui, demokratiniam valdymui ir saviraiškos laisvei. Masinis sekimas ir technologijos, sudarančios sąlygas globalizuotai saugoti ir tvarkyti asmens duomenis bei suteikti plačią prieigą prie duomenų, gali pakenkti pačiai teisės į privatumą esmei[977]. Be to, jie gali turėti neigiamą poveikį politinei kultūrai ir atgrasomąjį poveikį demokratijai, kūrybiškumui ir inovacijoms[978]. Vien nuogąstavimai, kad valstybė gali nuolat sekti ir analizuoti piliečių elgesį ir veiksmus, gali atgrasyti juos reikšti savo nuomonę tam tikrais klausimais ir lemti apdairumą bei atsargumą[979]. Šios problemos paskatino keletą valdžios institucijų, mokslinių tyrimų centrų ir pilietinės visuomenės organizacijų analizuoti galimą naujų technologijų poveikį visuomenei. 2015 m. Europos duomenų apsaugos priežiūros pareigūnas pradėjo keletą iniciatyvų, kuriomis siekiama įvertinti didžiųjų duomenų ir daiktų interneto poveikį etikai. Visų pirma jis įsteigė Etikos patariamąją grupę, kurios tikslas – skatinti „atvirą informuotų asmenų diskusiją apie skaitmeninę etiką, leisiančią ES geriau suvokti technologijų naudą visuomenei ir ekonomikai ir kartu sustiprinti asmenų teises ir laisves, ypač jų teises į privatumą ir duomenų apsaugą“[980].

Asmens duomenų tvarkymas taip pat yra galinga priemonė korporacijų rankose. Šiandien ji gali atskleisti išsamią informaciją apie asmens sveikatos būklę ar finansinę padėtį, informaciją, kuria vėliau korporacijos naudojasi priimdamos asmenims svarbius sprendimus, pavyzdžiui, nustatydamos sveikatos draudimo įmoką, kuri jiems turi būti taikoma, arba jų kreditingumą. Duomenų tvarkymo metodai taip pat gali turėti įtakos demokratiniams procesams, kai politikai ar korporacijos daro įtaką rinkimams, pavyzdžiui, rinkėjų komunikacijai taikant „mikrotikslinius“ metodus. Kitaip tariant, nors privatumas iš pradžių buvo suvokiamas kaip teisė apsaugoti

977 Žr. JT Generalinė Asamblėja, *Specialiojo pranešėjo žmogaus teisių ir pagrindinių laisvių skatinimo ir apsaugos kovojant su terorizmu klausimais ataskaitos*, Ben Emmerson, A/69/397, 2014 m. rugsėjo 23 d., 59 punktas. Taip pat žr. EŽTT, *Informacijos apie masinį sekimą suvestinė*, 2017 m. liepos mėn.

978 EDAPP (2015 m.), *Pasitinkant didžiųjų duomenų iššūkius*, Nuomonė 7/2015, Briuselis, 2015 m. lapkričio 19 d.

979 Žr. visų pirma ESTT, sujungtos bylos C-293/12 ir C-594/12, *Digital Rights Ireland Ltd prieš Minister for Communications, Marine and Natural Resources ir kt.* ir *Kärntner Landesregierung ir kt.* (DK), 2014 m. balandžio 8 d., 37 punktas.

980 EDAPP, 2015 m. gruodžio 3 d. Sprendimo dėl duomenų apsaugos etinių aspektų išorės patariamosios grupės (toliau – Etikos patariamoji grupė) įsteigimo, 2015 m. gruodžio 3 d., 5 konstatuojamoji dalis.

asmenis nuo nepagrįsto valdžios institucijų kišimosi, šiuolaikiniame pasaulyje jam taip pat gali kelti grėsmę privačių subjektų įtaka. Tai kelia klausimų dėl technologijų naudojimo ir prognozuojamosios analizės priimant sprendimus, kurie daro poveikį asmenų kasdieniam gyvenimui, ir sustiprina poreikį užtikrinti, kad tvarkant asmens duomenis būtų laikomasi pagrindinių teisių reikalavimų.

Duomenų apsauga yra glaudžiai susijusi su technologiniais, socialiniais ir politiniais pokyčiais. Todėl būtų neįmanoma parengti išsamaus būsimų uždavinių sąrašo. Šiame skyriuje nagrinėjamos tam tikros sritys, susijusios su didžiaisiais duomenimis, interneto socialiniais tinklais ir ES bendrąja skaitmenine rinka. Tai ne išsamus šių sričių vertinimas duomenų apsaugos požiūriu, o įvairios galimos naujos ar peržiūrėtos žmogaus veiklos ir duomenų apsaugos sąsajos.

10.1. Didieji duomenys, algoritmai ir dirbtinis intelektas

Pagrindiniai faktai

- Radikalios IRT inovacijos formuoja naują gyvenimo būdą, kai socialiniai ryšiai, verslas, privačiosios ir viešosios paslaugos yra tarpusavyje susiję skaitmeniniu būdu, todėl gaunama vis daugiau duomenų, kurių dauguma yra asmens duomenys.
- Vyriausybės, įmonės ir piliečiai vis dažniau veikia duomenimis grindžiamoje ekonomikoje, kurioje patys duomenys tapo vertingu turtu.
- Didžiųjų duomenų sąvoka susijusi tiek su duomenimis, tiek su jų analize.
- Asmens duomenys, tvarkomi atliekant didžiųjų duomenų analizę, patenka į ES ir ET teisės aktų taikymo sritį.
- Nuo duomenų apsaugos taisyklių ir teisių nukrypti leidžiančios nuostatos taikomos tik tam tikroms teisėms ir konkretiems atvejams, kai užtikrinti teisės vykdymą būtų neįmanoma arba reikėtų neproporcingų duomenų valdytojų pastangų.
- Visiškai automatizuotas sprendimų priėmimas paprastai draudžiamas, išskyrus konkrečius atvejus.
- Asmenų informuotumas ir kontrolė yra labai svarbūs siekiant užtikrinti teisių įgyvendinimą.

Vis labiau skaitmenizuotame pasaulyje kiekviena veikla palieka skaitmeninį pėdsaką, kurį galima rinkti, tvarkyti, vertinti ar analizuoti. Naudojant naujas informacines ir ryšių technologijas renkama ir registruojama vis daugiau duomenų[981]. Dar visai neseniai nė viena technologija negalėjo analizuoti ar įvertinti duomenų masės ar padaryti naudingų išvadų. Duomenų paprasčiausiai buvo per daug, kad būtų galima juos įvertinti, jie buvo pernelyg sudėtingi, prastai struktūrizuoti ir greitai kintantys, kad būtų galima nustatyti tendencijas ir įpročius.

10.1.1. Didžiųjų duomenų, algoritmų ir dirbtinio intelekto apibūdinimas

Didieji duomenys

Sąvoka „didieji duomenys“ yra populiarus terminas, kuris, priklausomai nuo konteksto, gali reikšti keletą koncepcijų. Jis paprastai apima „didėjantį technologinį pajėgumą rinkti proceso duomenis ir gauti naujų ir prognozuojamų žinių iš didelio duomenų kiekio, greičio ir įvairovės“[982]. Todėl pati didžiųjų duomenų sąvoka apima tiek pačius duomenis, tiek duomenų analitiką.

Duomenų šaltiniai yra įvairių rūšių ir apima žmones ir jų asmens duomenis, įrenginius arba jutiklius, informaciją apie klimatą, palydovų atvaizdus, skaitmenines nuotraukas ir vaizdo medžiagą arba GPS signalus. Vis dėlto daug duomenų ir informacijos yra asmens duomenys, pavyzdžiui, vardas, pavardė, nuotrauka, e. pašto adresas, banko duomenys, GPS sekimo duomenys, socialinių tinklų interneto svetainių adresai, medicininė informacija ar kompiuterio IP adresas[983].

Didieji duomenys taip pat reiškia **duomenų tvarkymą**, duomenų masės ir prieinamos informacijos analizę ir vertinimą, t. y. siekiant gauti naudingos informacijos didžiųjų duomenų analizės tikslais. Tai reiškia, kad surinkti duomenys ir informacija

981 Europos Komisija, Komisijos komunikatas Europos Parlamentui, Tarybai, Ekonomikos ir socialinių reikalų komitetui „Kuriame klestinčią duomenimis grindžiamą ekonomiką“, COM(2014) 442 *final*, Briuselis, 2014 m. liepos 2 d.

982 Europos Taryba, 108-osios konvencijos konsultacinis komitetas, Gairės dėl asmenų apsaugos tvarkant asmens duomenis didžiųjų duomenų pasaulyje, 2017 m. sausio 23 d., p. 2; Europos Komisija, Komisijos komunikatas Europos Parlamentui, Tarybai, Ekonomikos ir socialinių reikalų komitetui „Kuriame klestinčią duomenimis grindžiamą ekonomiką“, COM(2014) 442 *final*, Briuselis, 2014 m. liepos 2 d., p. 4; Tarptautinė telekomunikacijų sąjunga (2015 m.), Rekomendacija Y.3600. Didieji duomenys – debesijos kompiuterija grindžiami reikalavimai ir pajėgumai.

983 ES Komisijos faktų apie ES duomenų apsaugos reformą ir didžiuosius duomenis suvestinė; Europos Taryba, 108-osios konvencijos konsultacinis komitetas, Gairės dėl asmenų apsaugos tvarkant asmens duomenis didžiųjų duomenų pasaulyje, 2017 m. sausio 23 d., p. 2.

gali būti naudojami kitiems tikslams, nei buvo numatyta iš pradžių, pavyzdžiui, statistinėms tendencijoms arba labiau pritaikytoms paslaugoms, pavyzdžiui, reklamai. Iš tiesų, jei egzistuoja didžiųjų duomenų rinkimo, tvarkymo ir vertinimo technologijos, bet kokia informacija gali būti derinama ir iš naujo vertinama, t. y. finansiniai sandoriai, kreditingumas, medicininis gydymas, asmeninis vartojimas, profesinė veikla, sekimas ir naudojami maršrutai, naudojimasis internetu, elektroninės kortelės ir išmanieji telefonai, vaizdo ar ryšių stebėsena. Didžiųjų duomenų analizė suteikia naują kiekybinį duomenų aspektą, kurį galima įvertinti ir naudoti tikruoju laiku, pavyzdžiui, teikiant vartotojams pritaikytas paslaugas.

Algoritmai ir dirbtinis intelektas

Dirbtinis intelektas (DI) – tai mašinų, kurios veikia kaip „išmanieji agentai“, intelektas. Kaip išmanusis agentas tam tikri prietaisai su programine įranga gali suvokti savo aplinką ir imtis veiksmų pagal algoritmus. Terminas „dirbtinis intelektas“ taikomas, kai mašina imituoja „kognityvines“ funkcijas, tokias kaip mokymasis ir problemų sprendimas, kurios paprastai būtų susijusios su fiziniais asmenimis[984]. Siekiant imituoti sprendimų priėmimą, šiuolaikinėse technologijose ir programinėje įrangoje naudojami algoritmai „automatizuotiems sprendimams“ priimti. Algoritmą geriausia apibūdinti kaip laipsnišką skaičiavimo, duomenų tvarkymo, vertinimo, automatinio pagrindimo ir sprendimų priėmimo procedūrą.

Panašiai kaip ir didžiųjų duomenų analizės atveju, dirbtinis intelektas ir jo kuriamas automatizuotas sprendimų priėmimas reiškia poreikį rinkti ir tvarkyti didžiuosius duomenis. Šie duomenys gali būti gaunami iš paties įrenginio (stabdžių šilumos, kuro ir kt.) arba iš supančios aplinkos. Pavyzdžiui, profiliavimas yra procesas, kuris gali būti grindžiamas automatizuotu sprendimų priėmimu pagal iš anksto nustatytus modelius ar veiksnius.

Pavyzdys. Profiliavimas ir tikslinė reklama

Didžiaisiais duomenimis grindžiamas profiliavimas reiškia, kad reikia ieškoti modelių, kurie atspindėtų „asmens rūšies savybes“, pavyzdžiui, kai internetu prekiaujančios įmonės siūlo produktus „jums taip pat gali patikti“, remdamosi informacija, surinkta iš produktų, kurie anksčiau buvo pateikti į kliento

984 Stuart Russel ir Peter Norvig, *Artificial Intelligence: A Modern Approach* (2-as leid.), 2003 m., *Upper Saddle River*, Naujasis Džersis: *Prentice Hall*, p. 27, 32–58, 968–972; Stuart Russel ir Peter Norvig, *Artificial Intelligence: A Modern Approach* (3-ias leid.), 2009 m., *Upper Saddle River*, Naujasis Džersis: *Prentice Hall*, p. 2.

pirkinių krepšelį. Kuo daugiau duomenų, tuo aiškesnė mozaika. Pavyzdžiui, išmanusis telefonas yra galingas klausimynas, kurį kiekvienas naudotojas pildo sąmoningai ir nesąmoningai.

Šiuolaikinėje psichografijoje – asmenybės ypatybių studijavimo mokslo srityje – naudojamas metodas „OCEAN“, pagal kurį nustatomos nagrinėjamų požymių rūšys. „Big Five“ simbolių matmenys yra susiję su atvirumu (asmens atvirumas naujovėms), teisingumu (kiek asmuo yra panašus į asmens tobulumą), ekstravertiškumu (asmens socializacijos laipsniu), priimtinumu (kiek asmuo yra linkęs sutikti) ir neurotizmu (kiek asmuo yra pažeidžiamas). Ši informacija apibūdina atitinkamą asmenį, jo poreikius ir nuogąstavimus, tai, kaip jis elgsis, ir kt. Toliau ji papildoma kita informacija apie asmenį, gauta iš bet kokių prieinamų šaltinių, iš duomenų tarpininkų, socialinių tinklų (įskaitant paspaudimus „patinka“ po paskelbtais įrašais ir nuotraukomis), muzikos, kurios buvo klausomasi internete, arba GPS ir sekimo duomenų.

Profilių, sukurtų taikant didžiųjų duomenų analizės metodus, masė vėliau lyginama siekiant nustatyti panašius modelius ir sukurti asmenų grupes. Todėl informacija apie tam tikrų asmenų elgesį ir požiūrį yra nukreipta į juos pačius. Kalbant apie prieigą prie didžiųjų duomenų ir jų naudojimą, asmenybės testas apverčiamas, pasitelkiant informaciją apie elgesį ir požiūrį, kuri dabar naudojama asmens asmenybei apibūdinti. Turint bendrą informaciją apie „patiktukus“ socialiniuose tinkluose, sekimo duomenis, klausomą muziką ar žiūrimus filmus, galima susidaryti aiškų vaizdą apie asmens asmenybę, kad įmonės galėtų skleisti pritaikytą reklamą ir (arba) informaciją pagal to asmens asmenybę. Svarbiausia, kad ši informacija gali būti tvarkoma tikruoju laiku[985].

10.1.2. Didžiųjų duomenų naudos ir rizikos pusiausvyra

Taikant šiuolaikines duomenų tvarkymo technologijas galima tvarkyti masinį duomenų kiekį, greitai importuoti naujus duomenis, užtikrinti, kad informacija būtų apdorojama tikruoju laiku, t. y. per trumpą atsakymo laiką (net ir sudėtingų prašymų atveju), numatyti galimybę pateikti daug prašymų vienu metu ir analizuoti įvairių rūšių informaciją (nuotraukas, tekstus ar numerius). Šios technologinės naujovės suteikia galimybę tikruoju laiku susisteminti, tvarkyti ir įvertinti duomenų ir

985 Duomenų tvarkymo metodais ir nauja programine įranga vertinama informacija apie tai, ką asmuo mėgsta; žiūrima, kada apsiperka internetu arba tikruoju laiku prideda prie pirkinių internetu krepšelio, ir, remiantis surinkta informacija, gali siūlyti „produktus“, kurie gali būti įdomūs.

informacijos masę[986]. Eksponentiškai padidinus turimų ir analizuojamų duomenų kiekį, dabar galima pasiekti rezultatus, kurių būtų neįmanoma pasiekti atliekant mažesnio masto analizę. Didieji duomenys padėjo plėtoti naują verslo sritį, kurioje įmonėms ir vartotojams gali atsirasti naujų paslaugų. Iki 2020 m. ES piliečių asmens duomenų vertė gali pasiekti beveik 1 trln. EUR metinę vertę[987]. Todėl didieji duomenys gali suteikti naujų masinių duomenų vertinimo **galimybių** naujoms socialinėms, ekonominėms ar mokslinėms įžvalgoms, kurios gali būti naudingos tiek asmenims, tiek įmonėms ir vyriausybėms[988].

Didžiųjų duomenų analizė gali atskleisti įvairių šaltinių ir duomenų rinkinių modelius ir suteikti naudingų įžvalgų tokiose srityse, kaip mokslas ir medicina. Tai pasakytina, pavyzdžiui, apie sveikatą, aprūpinimą maistu, intelektines transporto sistemas, energijos vartojimo efektyvumą ar miestų planavimą. Ši informacijos analizė tikruoju laiku gali būti naudojama įdiegtoms sistemoms tobulinti. Mokslinių tyrimų srityje naujų įžvalgų galima gauti derinant didžiuosius duomenis ir statistinius vertinimus, ypač tose srityse, kuriose iki šiol daug duomenų buvo vertinami tik rankiniu būdu. Galima sukurti naujus gydymo būdus, pritaikytus atskiriems pacientams, remiantis palyginimais su daugybe turimos informacijos. Bendrovės tikisi, kad didžiųjų duomenų analizė suteiks joms galimybę įgyti konkurencinį pranašumą, sutaupyti lėšų ir sukurti naujas verslo sritis teikiant tiesiogines individualizuotas klientų aptarnavimo paslaugas. Vyriausybės agentūros tikisi pagerinti baudžiamąją teiseną. Komisijos Europos bendrosios skaitmeninės rinkos strategijoje pripažįstamas duomenimis grindžiamų technologijų, paslaugų ir didžiųjų duomenų potencialas skatinti ekonomikos augimą, inovacijas ir skaitmeninimą ES[989].

---

986 Didiesiems duomenims tvarkyti skirta programinė įranga dar tik pradedama kurti. Nepaisant to, neseniai buvo parengtos analitinės programos, visų pirma skirtos masinei duomenų ir informacijos, susijusių su asmenų veikla, analizei realiuoju laiku. Galimybė struktūriškai analizuoti ir tvarkyti didžiuosius duomenis suteikė naujų profiliavimo ir tikslinės reklamos priemonių. Komisijos komunikatas Europos Parlamentui, Tarybai, Ekonomikos ir socialinių reikalų komitetui „Kuriame klestinčią duomenimis grindžiamą ekonomiką“, COM(2014) 442 *final*, Briuselis, 2014 m. liepos 2 d.; Europos Taryba, 108-osios konvencijos konsultacinis komitetas, Gairės dėl asmenų apsaugos tvarkant asmens duomenis didžiųjų duomenų pasaulyje, 2017 m. sausio 23 d., p. 2.

987 ES Komisijos faktų apie ES duomenų apsaugos reformą ir didžiuosius duomenis suvestinė.

988 Tarptautinė už duomenų apsaugą ir privatumą atsakingų Komisijos narių konferencija (2014), Rezoliucija dėl didžiųjų duomenų; Komisijos komunikatas Europos Parlamentui, Tarybai, Ekonomikos ir socialinių reikalų komitetui „Kuriame klestinčią duomenimis grindžiamą ekonomiką“, COM(2014) 442 *final*, Briuselis, 2014 m. liepos 2 d., 2; Europos Taryba, 108-osios konvencijos konsultacinis komitetas, Gairės dėl asmenų apsaugos tvarkant asmens duomenis didžiųjų duomenų pasaulyje, 2017 m. sausio 23 d., p. 1.

989 2017 m. kovo 14 d. Europos Parlamento rezoliucija „Didžiųjų duomenų poveikis pagrindinėms teisėms: privatumas, duomenų apsauga, nediskriminavimas, saugumas ir teisėsauga“ (2016/2225 (INI)).

Tačiau didieji duomenys taip pat kelia **riziką**, paprastai siejamą su tvarkomų duomenų apimtimi, greičiu ir įvairove. Apimtis reiškia tvarkomų duomenų kiekį, įvairovė – duomenų rūšių skaičių ir įvairovę, o greitis – duomenų tvarkymo greitį. Konkretūs duomenų apsaugos aspektai kyla visų pirma tada, kai didžiųjų duomenų analizė naudojama dideliems duomenų rinkiniams, siekiant gauti naujų ir prognozuojamų žinių sprendimų priėmimo tikslais, susijusiais su asmenimis ir (arba) grupėmis[990]. Su didžiaisiais duomenimis susijusi rizika duomenų apsaugai ir privatumui pabrėžta EDAPP ir 29 straipsnio darbo grupės nuomonėse, Europos Parlamento rezoliucijose ir Europos Tarybos politikos dokumentuose[991].

Rizika gali apimti tai, kad asmenys, turintys prieigą prie masinės informacijos, manipuliuodami, diskriminuodami asmenis ar konkrečias visuomenės grupes ar darydami joms spaudimą netinkamai tvarko didžiuosius duomenis[992]. Kai surenkama, tvarkoma ir vertinama daugybė asmens duomenų ar informacijos apie asmens elgesį, jų naudojimas gali lemti rimtus pagrindinių teisių ir laisvių pažeidimus, nesusijusius su teisės į privatumą apsauga. Neįmanoma tiksliai įvertinti, kokiu mastu gali būti daromas poveikis privatumui ir asmens duomenims. Europos Parlamentas nustatė, kad trūksta metodikos, kurią taikant būtų galima atlikti įrodymais pagrįstą bendro didžiųjų duomenų poveikio vertinimą, tačiau yra įrodymų, kad didžiųjų duomenų analizė gali turėti didelį horizontalųjį poveikį tiek viešajame, tiek privačiajame sektoriuose[993].

Bendrajame duomenų apsaugos reglamente yra nuostatų dėl teisės į tai, kad nebūtų taikomas automatizuotas sprendimų priėmimas, įskaitant profiliavimą[994]. Privatumo klausimas kyla tada, kai, norint pasinaudoti teise nesutikti, reikia žmogaus įsikišimo,

990 Europos Taryba, 108-osios konvencijos konsultacinis komitetas, Gairės dėl asmenų apsaugos tvarkant asmens duomenis didžiųjų duomenų pasaulyje, 2017 m. sausio 23 d., p. 2.

991 Žr., pvz., EDAPP (2015 m.), *Pasitinkant didžiųjų duomenų iššūkius*, Nuomonė 7/2015, 2015 m. lapkričio 19 d.; EDAPP (2016 m.), *Nuoseklus pagrindinių teisių įgyvendinimas didelių duomenų kiekių amžiuje*, Nuomonė 8/2016, 2016 m. rugsėjo 23 d.; Europos Parlamentas (2016 m.), Rezoliucija „Didelių duomenų kiekių poveikis pagrindinėms teisėms: privatumas, duomenų apsauga, nediskriminavimas, saugumas ir teisėsauga“, P8_TA(2017)0076, Strasbūras, 2017 m. kovo 14 d.; Europos taryba, 108-osios konvencijos konsultacinis komitetas, Gairės dėl asmenų apsaugos tvarkant asmens duomenis didžiųjų duomenų pasaulyje, T-PD (2017) 01, Strasbūras, 2017 m. sausio 23 d.

992 Tarptautinė duomenų apsaugos ir privatumo priežiūros pareigūnų konferencija (2014 m.), Rezoliucija dėl didžiųjų duomenų.

993 2017 m. kovo 14 d. Europos Parlamento rezoliucija „Didelių duomenų kiekių poveikis pagrindinėms teisėms: privatumas, duomenų apsauga, nediskriminavimas, saugumas ir teisėsauga“ (2016/2225 (INI)).

994 Bendrojo duomenų apsaugos reglamento 22 straipsnis.

kad duomenų subjektai galėtų pareikšti savo nuomonę ir užginčyti sprendimą[995]. Todėl gali kilti sunkumų užtikrinant tinkamą asmens duomenų apsaugos lygį, jei, pavyzdžiui, žmogus negali įsikišti arba algoritmai yra pernelyg sudėtingi, o susijusių duomenų kiekis yra per didelis, kad asmenys galėtų pagrįsti tam tikrus sprendimus ir (arba) gauti išankstinę informaciją, reikalingą duomenų subjekto sutikimui patvirtinti. Dirbtinio intelekto naudojimo ir automatizuoto sprendimų priėmimo pavyzdys yra naujausi pokyčiai, susiję su hipotekos prašymais arba įdarbinimo procesais. Paraiškos atmetamos arba atmetamos remiantis tuo, kad pareiškėjai neatitinka iš anksto nustatytų parametrų ar veiksnių.

10.1.3. Su duomenų apsauga susiję klausimai

Kalbant apie duomenų apsaugą, pažymėtina, kad pagrindiniai klausimai yra susiję, viena vertus, su tvarkomų asmens duomenų kiekiu ir įvairove, kita vertus, su tvarkymu ir jo rezultatais. Sudėtingų algoritmų ir programinės įrangos, skirtų masinius duomenis paversti ištekliumi sprendimų priėmimo tikslais, įdiegimas visų pirma daro poveikį asmenims ir grupėms, ypač profiliavimo ar ženklinimo atvejais, ir galiausiai kelia daug duomenų apsaugos problemų[996].

Duomenų valdytojų ir duomenų tvarkytojų nustatymas ir jų atsakomybė

Dėl didžiųjų duomenų ir dirbtinio intelekto kyla keletas klausimų, susijusių su duomenų valdytojų ir duomenų tvarkytojų nustatymu ir jų atsakomybe: kai surenkamas ir tvarkomas toks didelis duomenų kiekis, kas yra duomenų savininkas? Kai duomenis tvarko žvalgybos įranga ir programinė įranga, kas yra duomenų valdytojas? Kokia yra tiksli kiekvieno duomenų tvarkymo subjekto atsakomybė? Ir kokiais tikslais gali būti naudojami didieji duomenys?

Atsakomybės dirbtinio intelekto srityje klausimas taps dar sudėtingesnis, kai dirbtinis intelektas sugebės priimti sprendimą, pagrįstą jo paties plėtojamu duomenų tvarkymu. Bendrajame duomenų apsaugos reglamente nustatyta duomenų valdytojo ir tvarkytojo atsakomybės teisinė sistema. Dėl neteisėto asmens duomenų tvarkymo atsiranda duomenų valdytojo ir duomenų tvarkytojo atsakomybė[997]. Dėl dirbtinio

995 *Ten pat*, 22 straipsnio 3 dalis.

996 Europos Taryba, 108-osios konvencijos konsultacinis komitetas, Gairės dėl asmenų apsaugos tvarkant asmens duomenis didžiųjų duomenų pasaulyje, 2017 m. sausio 23 d., p. 2.

997 Bendrojo duomenų apsaugos reglamento 77–79 straipsniai ir 82 straipsnis.

intelekto ir automatizuoto sprendimų priėmimo kyla klausimų, kas yra atsakingas už pažeidimus, darančius poveikį duomenų subjektų privatumui, kai tvarkomų duomenų sudėtingumo ir kiekio negalima tiksliai nustatyti. Kai dirbtinis intelektas ir algoritmai laikomi produktais, kyla neatitikčių tarp asmeninės atsakomybės, kuri reglamentuojama pagal Bendrąjį duomenų apsaugos reglamentą, ir atsakomybės už gaminius, kuri nereglamentuojama[998]. Tam reikėtų nustatyti atsakomybės taisykles, kad būtų užpildytas atotrūkis tarp asmeninės atsakomybės ir atsakomybės už produktus robotikos ir dirbtinio intelekto srityje, įskaitant, pavyzdžiui, automatizuotą sprendimų priėmimą[999].

Poveikis duomenų apsaugos principams

Dėl pirmiau aprašytų didžiųjų duomenų pobūdžio, analizės ir naudojimo kyla sunkumų taikant kai kuriuos tradicinius pagrindinius Europos duomenų apsaugos teisės principus[1000]. Tokie sunkumai iš esmės yra susiję su teisėtumo, duomenų kiekio mažinimo, tikslų apribojimo ir skaidrumo principais.

Pagal duomenų kiekio mažinimo principą reikalaujama, kad asmens duomenys būtų adekvatūs, tinkami ir neviršytų to, kas būtina tikslams, dėl kurių jie tvarkomi, pasiekti. Tačiau didžiųjų duomenų verslo modelis gali būti duomenų kiekio mažinimo antitezė, nes jam reikia vis daugiau duomenų, dažnai netiksliai apibrėžtais tikslais.

Tą patį galima pasakyti apie tikslų apribojimo principą, pagal kurį reikalaujama, kad duomenys būtų tvarkomi konkrečiais tikslais ir negali būti naudojami su pradiniu duomenų rinkimo tikslu nesuderinamais tikslais, išskyrus atvejus, kai toks tvarkymas grindžiamas teisiniu pagrindu, pavyzdžiui, duomenų subjekto sutikimu, tačiau tuo neapsiribojant (žr. 4.1.1 skirsnį).

Galiausiai, didieji duomenys taip pat kelia pavojų duomenų tikslumo principui, nes didžiųjų duomenų taikomosios programos paprastai renka duomenis iš įvairių šaltinių ir neturi galimybės patikrinti ir (arba) išlaikyti surinktų duomenų tikslumo[1001].

998 Europos Parlamentas, Europos civilinės teisės taisyklės robotikoje, Vidaus politikos generalinis direktoratas (2016 m. spalio mėn.), p. 14.

999 Roberto Viola kalba Europos Parlamente vykusiame žiniasklaidos seminare dėl Europos robotikos teisės (SPEECH 16/02/2017); Europos Parlamento pranešimas dėl pasiūlymo dėl robotikai ir dirbtiniam intelektui taikomų civilinės atsakomybės taisyklių.

1000 Europos Taryba, *Gairės dėl asmenų apsaugos tvarkant asmens duomenis didžiųjų duomenų pasaulyje*, T-PD (2017) 01, Strasbūras, 2017 m. sausio 23 d.

1001 EDAPP (2016 m.), *Nuoseklus pagrindinių teisių įgyvendinimas didelių duomenų kiekių amžiuje*, Nuomonė 8/2016, 2016 m. rugsėjo 23 d., p. 8.

Konkrečios taisyklės ir teisės

Pagal bendrą taisyklę asmens duomenys, tvarkomi atliekant didžiųjų duomenų analizę, patenka į duomenų apsaugos teisės aktų taikymo sritį. Vis dėlto ES ir ET teisėje nustatytos specialios taisyklės ar nukrypti leidžiančios nuostatos, taikomos konkrečiais atvejais, susijusiais su algoritminiu sudėtingų duomenų tvarkymu.

ET teisėje atnaujintoje 108-ojoje konvencijoje duomenų subjektui suteikiamos naujos teisės, kad jis galėtų veiksmingiau kontroliuoti savo asmens duomenis didžiųjų duomenų eroje. Tai, pavyzdžiui, galima pasakyti būtent apie atnaujintos Konvencijos 9 straipsnio 1 dalies a, c ir d punktus dėl teisės į tai, kad duomenų subjektui nebūtų taikomas sprendimas, grindžiamas tik automatizuotu duomenų tvarkymu, neatsižvelgus į jo nuomonę; teisė paprašius gauti informacijos apie motyvus, kuriais grindžiamas duomenų tvarkymas tais atvejais, kai jam taikomi tokio tvarkymo rezultatai, taip pat teisė nesutikti. Kitos atnaujintos 108-osios konvencijos nuostatos, visų pirma susijusios su skaidrumu ir papildomomis pareigomis, yra papildomi apsaugos mechanizmo, sukurto atnaujintoje 108-ojoje konvencijoje, siekiant spręsti skaitmenines problemas, aspektai.

ES teisėje, be BDAR 23 straipsnyje išvardytų atvejų, **skaidrumą** privaloma užtikrinti visais atvejais tvarkant asmens duomenis. Tai ypač svarbu kalbant apie interneto paslaugas ir kitą sudėtingą automatizuotą duomenų tvarkymą, pavyzdžiui, sprendimų priėmimo algoritmų naudojimą. Šiuo atveju pažymėtina, kad dėl duomenų tvarkymo sistemų ypatumų duomenų subjektams turi būti įmanoma iš tikrųjų suprasti, kas daroma su jų duomenimis. Siekiant užtikrinti sąžiningą ir skaidrų duomenų tvarkymą, Bendrajame duomenų apsaugos reglamente reikalaujama, kad duomenų valdytojas pateiktų duomenų subjektui prasmingą informaciją apie logiką, susijusią su automatizuotu sprendimų priėmimu, įskaitant profiliavimą[1002]. Europos Tarybos Ministrų Komitetas savo rekomendacijoje dėl teisės į saviraiškos laisvę ir teisės į privatų gyvenimą apsaugos ir skatinimo, atsižvelgdamas į tinklo neutralumą, rekomendavo, kad interneto paslaugų teikėjai „teiktų naudotojams aiškią, išsamią ir viešai prieinamą informaciją apie bet kokią srauto valdymo praktiką, kuri gali turėti įtakos naudotojų prieigai prie turinio, taikomųjų programų ar paslaugų ir jų platinimui“[1003]. Visų valstybių narių kompetentingų institucijų parengtos interneto duo-

1002 Bendrojo duomenų apsaugos reglamento 13 straipsnio 2 dalies f punktas.

1003 Europos Taryba, Ministrų Komitetas (2016 m.), Ministrų Komiteto rekomendacija *CM/Rec(2016)1* valstybėms narėms dėl teisės į saviraiškos laisvę ir teisės į privatų gyvenimą apsaugos ir skatinimo atsižvelgiant į tinklo neutralumą, 2016 m. sausio 13 d., 5.1 punktas.

menų srautų valdymo praktikos ataskaitos turėtų būti rengiamos atvirai ir skaidriai ir turėtų būti nemokamai prieinamos visuomenei[1004].

Duomenų valdytojai, nepaisant to, ar iš duomenų subjektų renkami duomenys, ar ne, privalo **pateikti** jiems ne tik informaciją apie surinktus duomenis ir numatomą duomenų tvarkymą (žr. 6.1.1 skirsnį), bet ir, kai tinkama informuoti apie automatizuotą sprendimų priėmimo procesą, pateikdami jiems „prasmingą informaciją apie loginį jo pagrindimą“[1005], tikslus ir galimas tokio duomenų tvarkymo pasekmes. Bendrajame duomenų apsaugos reglamente taip pat paaiškinta (ne tik tais atvejais, kai asmens duomenys nebuvo gauti iš duomenų subjekto), kad duomenų valdytojas neprivalo duomenų subjektui pateikti tokios informacijos, kai „tokios informacijos pateikimas būtų neįmanomas arba pareikalautų neproporcingų pastangų“[1006]. Tačiau, kaip pažymėjo 29 straipsnio darbo grupė savo *Automatizuoto atskirų sprendimų priėmimo ir profiliavimo pagal Reglamentą 2016/679 gairėse*, duomenų tvarkymo sudėtingumas pats savaime neturėtų atimti duomenų valdytojui galimybės pateikti duomenų subjektui aiškių paaiškinimų apie duomenų tvarkymo veiklos tikslus ir joje naudojamas analitikos priemones[1007].

Duomenų subjektų teisei **susipažinti** su savo asmens duomenimis, juos **ištaisyti** ir **ištrinti**, taip pat jų teisei apriboti duomenų tvarkymą panaši išimtis netaikoma. Tačiau duomenų valdytojo pareiga pranešti duomenų subjektui apie jo asmens duomenų ištaisymą ar ištrynimą (žr. 6.1.4 skirsnį) taip pat gali būti panaikinta, kai toks pranešimas „pasirodytų neįmanomas arba pareikalautų neproporcingų pastangų“[1008].

Pagal BDAR 21 straipsnį (žr. 6.1.6 skirsnį) duomenų subjektai taip pat turi teisę **nesutikti**, kad jų asmens duomenys būtų tvarkomi, įskaitant didžiųjų duomenų analizės atvejus. Nors duomenų valdytojams ši prievolė gali būti netaikoma, jei jie gali įrodyti viršesnius teisėtus interesus, jie negali naudotis tokia išimtimi tvarkydami duomenis tiesioginės rinkodaros tikslais.

1004 *Ten pat*, 5.2 punktas.

1005 Bendrojo duomenų apsaugos reglamento 13 straipsnio 2 dalies f punktas ir 14 straipsnio 2 dalies g punktas.

1006 *Ten pat*, 14 straipsnio 5 dalies b punktas.

1007 29 straipsnio darbo grupė, *Automatizuoto atskirų sprendimų priėmimo ir profiliavimo pagal Reglamentą 2016/679 gairės*, WP 251, 2017 m. spalio 3 d., p. 14.

1008 Bendrojo duomenų apsaugos reglamento 19 straipsnis.

Duomenų valdytojai, tvarkydami asmens duomenis archyvavimo tikslais viešojo intereso labui, mokslinių ar istorinių tyrimų tikslais arba statistiniais tikslais, taip pat gali nustatyti konkrečias nuo šių teisių nukrypti leidžiančias nuostatas[1009].

BDAR nustatytos konkrečios **profiliavimo ir automatizuoto sprendimų priėmimo** taisyklės: 22 straipsnio 1 dalyje nustatyta, kad duomenų subjektas „turi teisę, kad jam nebūtų taikomas tik automatizuotu duomenų tvarkymu, įskaitant profiliavimą, grindžiamas sprendimas, dėl kurio jam kyla teisinės pasekmės“. Kaip pažymėta 29 straipsnio darbo grupės gairėse, šiame straipsnyje nustatytas bendras draudimas priimti visiškai automatizuotus sprendimus[1010]. Duomenų valdytojams toks draudimas gali būti netaikomas tik trimis konkrečiais atvejais: 1) būtini duomenų subjekto ir duomenų valdytojo sutarčiai vykdyti, 2) leidžiami pagal ES arba nacionalinę teisę arba 3) grindžiami aiškiu sutikimu[1011].

Individuali kontrolė

Dėl didžiųjų duomenų analizės sudėtingumo ir skaidrumo stokos gali prireikti persvarstyti individualios asmens duomenų kontrolės koncepcijas. Kontrolė turėtų būti pritaikyta prie konkrečių socialinių ir technologinių aplinkybių, atsižvelgiant į tai, kad asmenys neturi pakankamai žinių. Todėl duomenų apsauga, susijusi su didžiaisiais duomenimis, turėtų būti grindžiama platesne duomenų naudojimo kontrolės idėja, pagal kurią individuali kontrolė virsta sudėtingesniu daugialypių rizikos, susijusios su duomenų naudojimu, poveikio vertinimų procesu[1012].

Ar didžiųjų duomenų taikomoji programa yra tinkama, priklauso nuo to, kaip gerai ji gali nuspėti testuojamų asmenų (arba vartotojų) norus ar elgesį. Dabartiniai prognozavimo modeliai, pagrįsti didžiųjų duomenų analize, nuolat tobulinami. Naujausi patobulinimai apima ne tik duomenų naudojimą asmenybėms (t. y. elgsenai ir požiūriams) suskirstyti į kategorijas, bet ir elgsenos analizę analizuojant balso įpročius ir pranešimų intensyvumą arba kūno temperatūrą. Visa ši informacija gali būti naudojama tikruoju laiku, remiantis žiniomis, gautomis iš didžiųjų duomenų vertinimo, siekiant įvertinti kreditingumą, pavyzdžiui, susitikimo su banko atstovu metu. Vertinimas atliekamas atsižvelgiant ne į asmens, prašančio suteikti kreditą, privalumus, o į

1009 *Ten pat*, 89 straipsnio 2 ir 3 dalys.

1010 29 straipsnio darbo grupė, *Automatizuoto atskirų sprendimų priėmimo ir profiliavimo pagal Reglamentą 2016/679 gairės*, WP 251, 2017 m. spalio 3 d., p. 9.

1011 Bendrojo duomenų apsaugos reglamento 22 straipsnio 2 dalis.

1012 Europos Taryba, 108-osios konvencijos konsultacinis komitetas, *Gairės dėl asmenų apsaugos tvarkant asmens duomenis didžiųjų duomenų pasaulyje*, T-PD(2017)01, Strasbūras, 2017 m. sausio 23 d.

elgesio charakteristikas, nustatytas išanalizavus ir įvertinus informaciją apie didžiuosius duomenis, t. y. vertinant kandidato stiprų arba malonų balsą, kūno kalbą arba kūno temperatūrą.

Profiliavimas ir tikslinė reklama nebūtinai gali kelti problemų, jei asmenys **žino**, kad jiems skirta speciali reklama. Profiliavimas tampa problema, kai jis naudojamas manipuliuoti asmenimis, t. y. tam tikrų asmenų ar asmenų grupių paieškai politinėms kampanijoms. Pavyzdžiui, į neapsisprendusių rinkėjų grupes galima kreiptis politinėmis žinutėmis, pritaikytomis prie jų asmenybės ir požiūrio. Kitas klausimas galėtų būti tokio profiliavimo naudojimas siekiant neleisti tam tikriems asmenims naudotis prekėmis ir paslaugomis. Viena iš apsaugos priemonių, galinčių suteikti apsaugą nuo piktnaudžiavimo didžiaisiais duomenimis ir asmenine informacija, yra pseudonimų suteikimas (žr. 2.1.1 skirsnį)[1013]. Tais atvejais, kai asmens duomenys yra iš tiesų nuasmeninti, t. y. nėra informacijos, iš kurios būtų galima atsekti duomenų subjektą, šie atvejai nepatenka į Bendrojo duomenų apsaugos reglamento taikymo sritį. Duomenų subjektų ir asmenų sutikimo tvarkant didžiuosius duomenis reglamentavimas taip pat yra vienas iš duomenų apsaugos teisės uždavinių. Tai apima sutikimą taikyti specialiai pritaikytą reklamą ir profiliavimą, kurie gali būti pateisinami dėl priežasčių, susijusių su klientų patirtimi, ir sutikimą naudoti daugybę asmens duomenų siekiant tobulinti ir plėtoti informacija grindžiamas analitines priemones. Žinojimas arba nežinojimas apie didžiųjų duomenų tvarkymą kelia keletą klausimų, susijusių su būdais, kuriais duomenų subjektai gali naudotis savo teisėmis, atsižvelgiant į tai, kad didžiųjų duomenų tvarkymas gali būti grindžiamas ir pseudonimine, ir anonimine informacija, kuriai taikomi algoritmai. Nors pseudoniminiams duomenims taikomas Bendrasis duomenų apsaugos reglamentas, anoniminiams duomenims reglamentas netaikomas. Individuali duomenų subjektų asmens duomenų tvarkymo kontrolė ir informuotumas apie jį yra labai svarbūs atliekant didžiųjų duomenų analizę: be to, jie neturės aiškios informacijos apie tai, kas yra duomenų valdytojas arba tvarkytojas, todėl negalės veiksmingai pasinaudoti savo teisėmis.

1013 *Ten pat*, p. 2.

10.2. 2.0 ir 3.0 kartos žiniatinklis: socialiniai tinklai ir daiktų internetas

Pagrindiniai faktai

- Socialinių tinklų paslaugos (SNS) yra internetinės komunikacijos platformos, suteikiančios asmenims galimybę prisijungti prie panašiai mąstančių vartotojų tinklų arba juos kurti.
- Daiktų internetas – tai objektų prijungimas prie interneto ir objektų tarpusavio sujungimas.
- Duomenų subjektų sutikimas yra dažniausias teisinis pagrindas, kuriuo remdamiesi duomenų valdytojai gali teisėtai tvarkyti duomenis socialiniuose tinkluose.
- Socialinio tinklo naudotojai paprastai yra apsaugoti „namų ūkiams taikoma išimtimi“; tačiau tam tikromis aplinkybėmis ši nukrypti leidžianti nuostata gali būti panaikinta.
- Socialinių tinklų paslaugų teikėjai nėra apsaugoti „namų ūkio išimtimi“.
- Siekiant šioje srityje užtikrinti duomenų saugumą, esminę svarbą turi pritaikytoji ir standartizuotoji privatumo apsauga.

10.2.1. 2.0 ir 3.0 kartos žiniatinklio apibūdinimas

Socialinių tinklų svetainių paslaugų teikėjai

Iš pradžių internetas buvo sukurtas kaip tinklas, skirtas kompiuteriams sujungti ir perduoti pranešimams, turintiems ribotas galimybes keistis duomenimis, o interneto svetainėse asmenims tiesiog suteikta galimybė pasyviai peržiūrėti jų turinį[1014]. 2.0 kartos žiniatinklio epochoje internetas tapo forumu, kuriame naudotojai sąveikauja, bendradarbiauja ir kuria informaciją. Šiai erai būdinga didžiulė sėkmė ir plačiai naudojamos socialinių tinklų paslaugos, kurios dabar yra esminė milijonų žmonių kasdienio gyvenimo dalis.

Socialinio tinklo paslaugas (SNS) arba socialinius tinklus plačiąja prasme galima apibūdinti kaip „internetines ryšių platformas, leidžiančias žmonėms susisiekti arba kurti tų pačių pažiūrų vartotojų tinklus“[1015]. Norėdami prisijungti prie tinklo arba jį

1014 Europos Komisija (2016 m.), *Daiktų interneto tobulinimas Europoje*, SWD(2016) 110 *final*.

1015 29 straipsnio darbo grupė (2009 m.), *Nuomonė Nr. 5/2009 dėl socialinių tinklų internete*, WP 163, 2009 m. birželio 12 d., p. 4.

sukurti, asmenys kviečiami pateikti asmens duomenis ir susikurti savo profilį. SNS suteikia naudotojams galimybę kurti skaitmeninį „turinį“, pradedant nuotraukomis ir vaizdo įrašais, baigiant laikraščių nuorodomis ir asmeniniais įrašais, kuriuose jie gali pareikšti savo nuomonę. Naudodamiesi šiomis internetinėmis ryšių platformomis, naudotojai gali bendrauti ir palaikyti ryšį su keliais kitais naudotojais. Svarbu tai, kad daugumai populiariųjų SNS nereikia jokių registracijos mokesčių. Užuot reikalavę, kad naudotojai mokėtų už prisijungimą prie tinklo, SNS paslaugų teikėjai didžiąją dalį savo pajamų gauna iš tikslinės reklamos. Reklamuotojams gali būti labai naudinga šiose svetainėse kasdien atskleidžiama asmeninė informacija. Turėdami informacijos apie naudotojo amžių, lytį, buvimo vietą ir interesus, jie gali užsiimti tiksline reklama.

Europos Tarybos Ministrų Komitetas priėmė Rekomendaciją dėl žmogaus teisių, susijusių su socialinių tinklų paslaugomis, apsaugos[1016], kurios specialiame skirsnyje aptariama duomenų apsauga ir kurią 2018 m. papildė kita Rekomendacija dėl interneto tarpininkų vaidmens ir atsakomybės[1017].

Pavyzdys. Nora yra labai laiminga, nes jos partneris pasipiršo. Ji nori pasidalyti gera naujiena su savo draugais ir šeima ir nusprendžia socialiniame tinkle parašyti emocingą įrašą, kuriame išreiškia džiaugsmą, ir pakeisti savo santykių statusą į „susižadėjusi“. Artimiausiomis dienomis Nora, prisijungusi prie savo paskyros, mato reklaminius skelbimus apie vestuvines sukneles ir gėlių parduotuves. Kodėl taip yra?

Kurdamos reklaminį skelbimą socialiniame tinkle *Facebook*, vestuvinių suknelių ir gėlių bendrovės pasirinko tam tikrus parametrus, kad galėtų pasiekti tokius žmones kaip Nora. Kai Noros profilis rodo, kad ji yra moteris, aktyvi, gyvenanti Paryžiuje, netoli vietovės, kurioje yra įsikūrusios reklaminius skelbimus pateikiančios aprangos ir gėlių parduotuvės, ji iš karto mato reklaminius skelbimus.

Daiktų internetas

Daiktų internetas simbolizuoja kitą interneto plėtros etapą, t. y. 3.0 kartos žiniatinklį. Naudojant daiktų internetą, įrenginiai gali būti sujungiami ir sąveikauti su kitais

1016 Europos Taryba, Ministrų Komitetas, Ministrų Komiteto rekomendacija *CM/Rec(2012)4* dėl žmogaus teisių, susijusių su socialinių tinklų paslaugomis, apsaugos, 2012 m. balandžio 4 d.

1017 Europos Taryba, Ministrų Komitetas, Ministrų Komiteto rekomendacija *CM/Rec(2018)2* dėl interneto tarpininkų vaidmens ir atsakomybės, 2018 m. kovo 7 d.

įrenginiais internete. Tai suteikia galimybę per ryšių tinklus sujungti objektus ir žmones, pranešti apie jų būklę ir (arba) supančios aplinkos būklę[1018]. Daiktų internetas ir prijungti įrenginiai jau yra realybė ir tikimasi, kad per ateinančius kelerius metus jų gerokai padaugės, nes bus sukurti ir toliau plėtojami išmanieji įrenginiai, kurie padės sukurti pažangiuosius miestus, išmaniuosius namus ir pažangiąsias įmones.

Pavyzdys. Daiktų internetas gali būti ypač naudingas sveikatos priežiūros srityje. Įmonės jau yra sukūrusios prietaisų, jutiklių ir taikomųjų programų, kurios leidžia stebėti paciento sveikatą. Naudojant dėvimąjį pavojaus signalo mygtuką ir kitus belaidžius jutiklius aplink namus, galima sekti kasdienį vienišų pagyvenusių žmonių gyvenimą ir teikti perspėjimus, jei nustatoma rimtų jų kasdienės rutinos sutrikimų. Pavyzdžiui, kritimo aptikimo jutiklius plačiai naudoja vyresnio amžiaus žmonės. Šie jutikliai gali tiksliai nustatyti kritimą ir apie jį pranešti asmens gydytojui ir (arba) šeimai.

Pavyzdys. Barselona yra vienas iš žinomiausių pažangiojo miesto pavyzdžių. Nuo 2012 m. mieste diegiamos naujoviškos technologijos, kuriomis siekiama sukurti pažangią viešojo transporto, atliekų tvarkymo, automobilių stovėjimo ir gatvių apšvietimo sistemą. Pavyzdžiui, atliekų tvarkymui pagerinti miestas naudoja pažangiąsias šiukšlių dėžes. Tai leidžia stebėti atliekų kiekį, kad būtų galima optimizuoti surinkimo būdus. Kai šiukšlių dėžės yra beveik pilnos, jos judriojo ryšio tinklu perduoda signalus, jie siunčiami į atliekų tvarkymo įmonės naudojamą programinę įrangą. Taigi bendrovė gali planuoti geriausią atliekų surinkimo būdą, nustatyti prioritetus ir (arba) tik sutvarkyti šiukšlių dėžes, kurias iš tikrųjų reikia ištuštinti.

10.2.2. Privalumų ir rizikos pusiausvyra

Didelio masto socialinių tinklų paslaugų plėtra ir sėkmė per pastarąjį dešimtmetį rodo, kad šios paslaugos duoda **didelę naudą**. Pavyzdžiui, tikslinė reklama (kaip aprašyta paryškintame pavyzdyje) yra ypač novatoriškas būdas įmonėms pasiekti savo auditoriją, siūlant joms konkretesnę rinką. Vartotojams taip pat gali būti naudinga, kad jiems būtų pateikiami svarbesni ir įdomesni reklaminiai skelbimai. Vis dėlto dar svarbiau tai, kad socialinių tinklų paslaugos ir socialinė žiniasklaida gali turėti teigiamą poveikį visuomenei ir pokyčių įgyvendinimui. Jos suteikia

1018 Europos Komisija, Komisijos tarnybų darbinis dokumentas, *Daiktų interneto tobulinimas Europoje*, SWD (2016) 110, 2016 m. balandžio 19 d.

naudotojams galimybes bendrauti, sąveikauti, burtis į grupes ir rengti renginius jiems aktualiais klausimais.

Taip pat tikimasi, kad daiktų internetas bus labai naudingas ekonomikai, be to, jis yra ES bendrosios skaitmeninės rinkos kūrimo strategijos dalis. Apskaičiuota, kad 2020 m. Europos Sąjungoje daiktų interneto jungčių skaičius padidės iki šešių milijardų. Tikimasi, kad šis junglumo išplėtimas atneš didelės ekonominės naudos, nes bus kuriamos novatoriškos paslaugos ir taikomosios programos, užtikrinama geresnė sveikatos priežiūra, geriau suprantami vartotojų poreikiai ir didinamas veiksmingumas.

Be to, atsižvelgiant į didelį asmeninės informacijos, kurią sukaupia socialinių tinklų naudotojai ir kurią paskui tvarko paslaugų operatoriai, kiekį, socialinių tinklų paslaugų plėtra kelia **vis didesnį susirūpinimą** dėl būdų, kaip būtų galima apsaugoti privatumą ir asmens duomenis. Socialinių tinklų paslaugos kelia pavojų teisei į privatų gyvenimą ir teisei į saviraiškos laisvę. Toks pavojus gali apimti „teisinių ir procedūrinių apsaugos priemonių, susijusių su procesais, dėl kurių naudotojai gali būti pašalinti, trūkumą; nepakankamą vaikų ir jaunimo apsaugą nuo žalingo turinio ar elgesio; kitų asmenų teisių negerbimą; privatumui palankių nuostatų nebuvimą; skaidrumo apie asmens duomenų rinkimo ir tvarkymo tikslus nebuvimą“[1019]. Europos duomenų apsaugos teisėje pabandyta reaguoti į privatumo / duomenų apsaugos problemas, kurias sukėlė socialiniai tinklai. Tokie principai kaip sutikimas, privatumas / pritaikytoji ir standartizuotoji duomenų apsauga ir asmenų teisės yra ypač svarbūs atsižvelgiant į socialinius tinklus ir tinklų paslaugas.

Daiktų interneto srityje daugybė asmens duomenų, gautų iš įvairių tarpusavyje sujungtų įrenginių, taip pat kelia pavojų privatumui ir duomenų apsaugai. Nors skaidrumas yra svarbus Europos duomenų apsaugos teisės principas, dėl daugybės prijungtų įrenginių ne visada aišku, kas gali rinkti, gauti ir naudoti iš daiktų interneto įrenginių surinktus duomenis[1020]. Tačiau pagal ES ir ET teisę skaidrumo principu duomenų valdytojai įpareigojami aiškiai ir paprastai informuoti duomenų subjektus apie tai, kaip naudojami jų duomenys. Atitinkamiems asmenims turi būti aiškiai nurodyta su jų asmens duomenų tvarkymu susijusi rizika, taisyklės, apsaugos priemonės ir teisės. Prie daiktų interneto prijungti prietaisai ir daugialypės tvarkymo operacijos bei susiję duomenys taip pat galėtų prieštarauti reikalavimui gauti aiškų

1019 Europos Taryba, Rekomendacija *Rec(2012)4* valstybėms narėms dėl žmogaus teisių apsaugos teikiant socialinių tinklų paslaugas, 2012 m. balandžio 4 d.

1020 Europos duomenų apsaugos priežiūros pareigūnas (2017 m.), *Daiktų interneto supratimas.*

ir informacija pagrįstą sutikimą dėl duomenų tvarkymo, kai toks tvarkymas grindžiamas sutikimu. Asmenims dažnai trūksta žinių apie techninį tokio duomenų tvarkymo veikimą, taigi ir apie savo sutikimo pasekmes.

Kitas svarbus susirūpinimą keliantis klausimas yra saugumas, atsižvelgiant į tai, kad prijungti įrenginiai yra ypač neapsaugoti nuo saugumo rizikos. Prijungtiems prietaisams būdingas skirtingas saugumo lygis. Kadangi jie veikia ne tik standartinėje IT infrastruktūroje, jie gali neturėti tinkamos duomenų tvarkymo galios ir saugojimo pajėgumų, kad galėtų įdiegti saugumo programinę įrangą, arba naudotojų asmeninei informacijai apsaugoti naudoti tokius metodus, kaip šifravimas, pseudonimų suteikimas ar anoniminimas.

Pavyzdys. Vokietijoje reguliavimo institucijos nusprendė uždrausti žaislą, prijungtą prie interneto, atsižvelgdamos į didelį susirūpinimą dėl žaislo poveikio vaikų privačiam gyvenimui. Reguliavimo institucijos laikėsi nuomonės, kad prie interneto prijungta lėlė „Cayla“ iš tikrųjų yra paslėptas šnipinėjimo prietaisas. Lėlė veikė išsiųsdama su ja žaidžiančio vaiko garsinius klausimus į taikomąją programėlę skaitmeniniame įrenginyje, kuri ją vertė į tekstą ir ieškojo atsakymo internete. Tuomet programėlė siuntė atsakymą lėlei, kuri jį išsakė vaikui. Naudojant šią lėlę būtų galima užregistruoti ir į programėlę perduoti vaiko ir netoliese esančių suaugusiųjų pranešimus. Jei lėlių gamintojai nebūtų ėmęsi tinkamų saugumo priemonių, lėlę būtų buvę galima naudoti pokalbiams pasiklausyti.

10.2.3. Su duomenų apsauga susiję klausimai

Sutikimas

Europoje asmens duomenų tvarkymas yra teisėtas tik tuo atveju, jei tai leidžiama pagal Europos duomenų apsaugos teisę. Socialinių tinklų paslaugų teikėjams duomenų subjektų sutikimas paprastai yra teisėtas duomenų tvarkymo pagrindas. Sutikimas turi būti duotas laisva valia ir būti konkretus, pagrįstas informacija ir nedviprasmiškas (žr. 4.1.1 skirsnį)[1021]. „Laisvas“ sutikimas iš esmės reiškia, kad duomenų subjektams būtina suteikti galimybę priimti realų ir tikrą sprendimą. Sutikimas yra „konkretus“ ir „pagrįstas informacija“, kai jis yra suprantamas, aiškiai ir tiksliai susijęs

1021 Bendrojo duomenų apsaugos reglamento 4 ir 7 straipsniai; atnaujintos 108-osios konvencijos 5 straipsnis.

su visa duomenų tvarkymo apimtimi, tikslais ir pasekmėmis. Socialiniuose tinkluose gali būti abejojama, ar sutikimas yra laisvas, konkretus ir pagrįstas informacija dėl visų rūšių duomenų tvarkymo, kurį atlieka socialinių tinklų paslaugų operatorius ir trečiosios šalys.

Pavyzdys. Norėdami prisijungti ir gauti prieigą prie socialinių tinklų paslaugų, asmenys dažnai turi sutikti, kad jų asmens duomenys būtų tvarkomi įvairiais būdais, dažnai nenurodant būtinų sąlygų ar alternatyvių galimybių. Vienas iš pavyzdžių būtų poreikis sutikti gauti elgesiu grindžiamą reklamą, kad būtų galima užsiregistruoti socialinių tinklų paslaugai gauti. 29 straipsnio darbo grupė savo nuomonėje dėl sąvokos „sutikimas" apibrėžties pažymi, kad „[t]urint omenyje kai kurių socialinių tinklų įgytą svarbą, kai kurių kategorijų naudotojai (pavyzdžiui, paaugliai) sutiks gauti elgsena paremtą reklamą, kad išvengtų grėsmės būti iš dalies atskirti nuo socialinių santykių. Naudotojui turėtų būti sudaryta galimybė duoti savanorišką ir konkretų sutikimą gauti elgsena pagrįstą reklamą, nepaisant jo galimybės pasinaudoti socialinio tinklo paslauga"[1022].

Pagal Bendrąjį duomenų apsaugos reglamentą jaunesnių nei 16 metų vaikų asmens duomenys iš esmės negali būti tvarkomi remiantis jų sutikimu[1023]. Jeigu būtina duoti sutikimą tvarkyti duomenis, jį turi duoti vienas iš vaiko tėvų arba globėjas. Vaikams reikalinga ypatinga apsauga, nes jie gali mažiau suvokti su duomenų tvarkymu susijusią riziką ir pasekmes. Tai labai svarbu socialinės žiniasklaidos srityje, nes vaikai yra labiau pažeidžiami dėl tam tikro neigiamo poveikio, kurį gali sukelti naudojimasis tokiomis žiniasklaidos priemonėmis, pavyzdžiui, kibernetinis persekiojimas, persekiojimas internetu arba tapatybės vagystė.

Saugumas ir privatumas / pritaikytoji ir standartizuotoji duomenų apsauga

Asmens duomenų tvarkymas savaime kelia pavojų saugumui, atsižvelgiant į nuolatinę saugumo pažeidimo galimybę, dėl kurios tvarkomi asmens duomenys gali būti atsitiktinai arba neteisėtai sunaikinti, prarasti, pakeisti, su jais gali būti susipažįstama be leidimo arba jie gali būti atskleisti. Pagal Europos duomenų apsaugos teisę

1022 29 straipsnio darbo grupė (2011 m.), *Nuomonė Nr. 15/2011 dėl sąvokos „sutikimas" apibrėžties*, WP 187, 2011 m. liepos 13 d., p. 18.

1023 Žr. Bendrojo duomenų apsaugos reglamento 8 straipsnį. ES valstybės narės gali teisės aktais nustatyti mažesnį amžių, su sąlyga, kad jis bus ne jaunesnis kaip 13 metų.

reikalaujama, kad duomenų valdytojai ir duomenų tvarkytojai įgyvendintų tinkamas technines ir organizacines priemones, kad užkirstų kelią bet kokiam nesankcionuotam kišimuisi į duomenų tvarkymo operacijas. Socialinių tinklų paslaugų teikėjai, kuriems taikomos Europos duomenų apsaugos taisyklės, taip pat privalo laikytis šio įpareigojimo.

Pagal privatumo / pritaikytosios ir standartizuotosios duomenų apsaugos principus reikalaujama, kad duomenų valdytojai išlaikytų savo produktų dizaino saugumą ir automatiškai taikytų tinkamas privatumo ir duomenų apsaugos nuostatas. Tai reiškia, kad asmeniui nusprendus prisijungti prie socialinio tinklo, paslaugų teikėjas negali automatiškai suteikti visos informacijos apie naująjį paslaugų vartotoją visiems jo naudotojams. Prisijungiant prie paslaugos, numatytosios privatumo ir duomenų apsaugos nuostatos turėtų būti tokios, kad informacija būtų prieinama tik pasirinktiems kontaktiniams asmenims. Išplėsti prieigą asmenims, kurie nepatenka į tą sąrašą, turėtų būti įmanoma tik paslaugų gavėjui rankiniu būdu pakeitus numatytąsias privatumo ir duomenų apsaugos nuostatas. Tai taip pat gali turėti poveikį tais atvejais, kai duomenų saugumo pažeidimas įvyksta nepaisant įdiegtų saugumo priemonių. Tokiais atvejais paslaugų teikėjai privalo pranešti susijusiems naudotojams, jei dėl to gali kilti didelis pavojus duomenų subjekto teisėms ir laisvėms[1024].

Privatumas / pritaikytoji ir standartizuotoji duomenų apsauga yra ypač svarbūs kalbant apie socialinių tinklų paslaugas, nes, be leidžiamos prieigos, susijusios su daugumos rūšių duomenų tvarkymu, dalijimasis informacija socialiniuose tinkluose kelia papildomą pavojų saugumui. Dažnai taip yra dėl to, kad asmenys nesupranta, *kas* gali susipažinti su jų informacija ir kaip šie žmonės gali ją panaudoti. Plačiai naudojantis socialiniais tinklais padaugėjo tapatybės vagysčių ir aukų.

Pavyzdys. Tapatybės vagystė yra reiškinys, kai asmuo gauna informaciją, duomenis ar dokumentus, priklausančius kitam asmeniui (nukentėjusiajam), ir vėliau pasinaudoja šia informacija siekdamas apsimesti nukentėjusiuoju, kad jo vardu gautų prekių ir paslaugų. Pavyzdžiui, Paulas turi paskyrą socialinės žiniasklaidos interneto svetainėje. Paulas yra mokytojas ir aktyvus savo bendruomenės narys, mėgstantis bendrauti ir nelabai besirūpinantis privatumo ir duomenų apsaugos nuostatomis savo socialinio tinklo paskyroje. Jo kontaktinių asmenų sąrašas yra ilgas, kartais jame yra žmonių, kurie nebūtinai jį asmeniškai pažįsta. Kadangi jis dirba didelėje mokykloje ir yra

1024 *Ten pat*, 34 straipsnis.

gana populiarus mokyklos futbolo komandos treneris, jis mano, kad labiausiai tikėtina, jog šie žmonės yra mokyklos tėvai arba draugai. Paulo e. pašto adresas ir gimimo diena rodomi jo socialinio tinklo paskyroje. Be to, Paulas reguliariai skelbia savo šuns Tobio nuotraukas, po kuriomis užrašo tokį tekstą kaip „Mano ir Tobio pasivaikščiojimas ryte“. Paulas nesupranta, kad vienas iš populiariausių saugumo klausimų siekiant apsaugoti jo e. pašto arba mobiliojo telefono paskyrą yra „koks jūsų augintinio vardas“. Naudodamasis Paulo socialinės žiniasklaidos profilyje pateikta informacija, Nickas lengvai gali įsilaužti į Paulo paskyras.

Asmenų teisės

SNS paslaugų teikėjai privalo gerbti fizinių asmenų teises (žr. 6.1 skirsnį), įskaitant teisę būti informuotam apie duomenų tvarkymo tikslą ir apie tai, kaip asmens duomenys gali būti naudojami tiesioginės rinkodaros tikslais. Asmenims taip pat turi būti suteikta teisė susipažinti su asmens duomenimis, kuriuos jie sukūrė socialinių tinklų platformoje, ir prašyti juos ištrinti. Net jei asmenys sutiko su asmens duomenų tvarkymu ir internete įkelia informaciją, jie turėtų turėti galimybę prašyti „būti pamiršti“, jei nebenori gauti socialinio tinklo paslaugų. Teisė į duomenų perkeliamumą taip pat suteikia naudotojams galimybę gauti asmens duomenų, kuriuos jie pateikė socialinių tinklų paslaugų teikėjui, kopiją struktūrizuotu, įprastai naudojamu ir kompiuterio skaitomu formatu ir perduoti savo duomenis iš vieno socialinių tinklų paslaugų teikėjo kitam[1025].

Duomenų valdytojai

Sudėtingas klausimas, kuris dažnai kyla socialinių tinklų srityje, yra susijęs su duomenų valdytojo tapatybe, t. y. kuris asmuo turi pareigą ir atsakomybę laikytis duomenų apsaugos taisyklių. Socialinių tinklų paslaugų teikėjai pagal Europos duomenų apsaugos teisę laikomi duomenų valdytojais. Tai yra akivaizdu atsižvelgiant į plačią sąvokos „duomenų valdytojas“ apibrėžtį ir tai, kad šie paslaugų teikėjai nustato asmens duomenų, kuriais asmenys dalijasi, tvarkymo tikslą ir priemones. Pagal ES teisę, jeigu duomenų valdytojai siūlo paslaugas ES duomenų subjektams, reikalaujama, kad jie laikytųsi Bendrojo duomenų apsaugos reglamento nuostatų, net jeigu jie nėra įsisteigę ES.

1025 Bendrojo duomenų apsaugos reglamento 21 straipsnis.

Vis dėlto, ar socialinių tinklų paslaugų teikėjai taip pat gali būti laikomi duomenų valdytojais? Jeigu fizinis asmuo asmens duomenis tvarko „užsiimdamas išimtinai asmenine ar namų ūkio veikla“, duomenų apsaugos taisyklės netaikomos. Europos duomenų apsaugos teisėje tai vadinama „namų ūkio išimtimi“. Tačiau tam tikrais atvejais socialinių tinklų paslaugos naudotojui namų ūkio išimtis gali būti netaikoma.

Naudotojai savanoriškai dalijasi savo asmenine informacija internete. Tačiau informacija, kuria dalijamasi internete, apima kitų asmenų asmeninę informaciją.

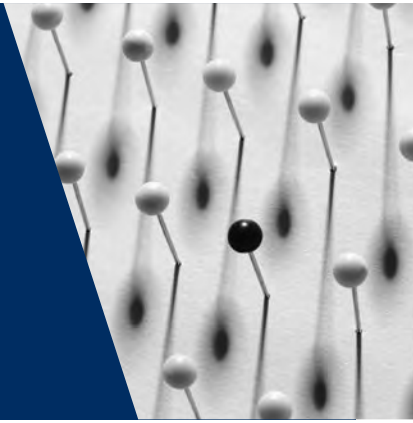
Pavyzdys. Paulas turi paskyrą labai populiarioje socialinių tinklų platformoje. Paulas bando tapti aktoriumi ir savo paskyrą naudoja nuotraukoms, vaizdo įrašams ir skelbimams, kuriuose paaiškinama jo aistra menui, skelbti. Populiarumas yra svarbus jo ateičiai; todėl jis nusprendė, kad jo profilis turėtų būti prieinamas ne tik jo uždaram kontaktinių asmenų sąrašui, bet ir visiems interneto naudotojams, nepaisant to, ar jie yra tinklo nariai. Ar gali Paulas skelbti nuotraukas ir vaizdo įrašus, kuriame yra jis ir jo draugė Sarah, be jos sutikimo? Sarah, kuri yra ikimokyklinio ugdymo įstaigos mokytoja, stengiasi neviešinti savo asmeninio gyvenimo darbdaviui, savo mokiniams ir jų tėvams. Įsivaizduokite atvejį, kai Sarah, kuri nesinaudoja socialiniais tinklais, iš savo bendro draugo Niko sužino, kad internete buvo paskelbta jos nuotrauka iš vakarėlio, kurioje ji yra su Paulu. Tokiu atveju Paulo duomenų tvarkymui ES teisė nebus taikoma, remiantis „namų ūkio išimtimi“.

Tačiau labai svarbu, kad naudotojai žinotų ir suvoktų, kad informacijos apie kitus asmenis įkėlimas be jų sutikimo gali pažeisti šių asmenų teisę į privatumą ir duomenų apsaugą. Net ir tais atvejais, kai taikoma namų ūkio išimtis, pavyzdžiui, kai vartotojas turi profilį, kuris viešai matomas tik jo pasirinktų kontaktinių asmenų sąrašui, dėl kitų asmenų asmeninės informacijos paskelbimo vartotojas vis tiek gali būti atsakingas. Nors duomenų apsaugos taisyklės nebūtų taikomos, jei taikoma namų ūkio išimtis, atsakomybė galėtų kilti dėl kitų nacionalinių taisyklių, pavyzdžiui, šmeižto ar asmens teisių pažeidimo, taikymo. Galiausiai tik socialinių tinklų paslaugų naudotojams suteikiama apsauga pagal namų ūkio išimtis: duomenų valdytojams ir duomenų tvarkytojams, kurie suteikia priemones tokiam privačiam duomenų tvarkymui, taikoma ES duomenų apsaugos teisė[1026].

1026 *Ten pat*, 18 konstatuojamoji dalis.

Reformuojant Direktyvą dėl privatumo ir elektroninių ryšių, pagal dabartinę teisinę sistemą telekomunikacijų paslaugų teikėjams taikomos duomenų apsaugos, privatumo ir saugumo taisyklės taip pat galiotų mašinų sąveikos ir elektroninių ryšių paslaugoms, įskaitant, pavyzdžiui, virštinklines paslaugas.

Papildoma literatūra



1 skyrius

M. Araceli Mangas (red.) „Carta de los derechos fundamentales de la Unión Europea“, Bilbao, *Fundación BBVA*, 2008.

W. Berka „Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit“, Viena, *Manzsche Verlags- und Universitätsbuchhandlung*, 2012.

C. Docksey „Four fundamental rights: finding the balance“, *International Data Privacy Law*, 6 t., Nr. 3, p. 195–209.

EDRi, *An introduction to data protection*, Briuselis.

J. Frowein ir W. Peukert „Europäische Menschenrechtskonvention“, Berlynas, *N. P. Engel Verlag*, 2009.

G. González Fuster ir G. Gellert „The fundamental right of data protection in the European Union: in search of an uncharted right“, *International Review of Law, Computers and Technology*, 26 (1) t., 2012, p. 73–82.

C. Grabenwarter ir K. Pabel „Europäische Menschenrechtskonvention“, Miunchenas, *C. H. Beck*, 2012.

S. Gutwirth, Y. Poullet, P. de Hert, C. de Terwange ir S. Nouwt (red.) „Reinventing Data Protection“, *Springer*, 2009.

D. Harris, M. O'Boyle, C. Warbrick ir E. Bates „Law of the European Convention on Human Rights", Oksfordas, *Oxford University Press*, 2009.

H. Hijmans „The European Union as Guardian of Internet Privacy – the Story of Art 16 TFEU", *Springer*, 2016.

P. Hustinx „EU Data Protection Law: the review of Directive 95/46/EC and the Proposed General Data Protection Regulation", 2016 m.

H. Jarass „Charta der Grundrechte der Europäischen Union", Miunchenas, *C. H. Beck*, 2010.

J. Kokott ir C. Sobotta „The distinction between privacy and data protection in the case law of the CJEU and the ECtHR", *International Data Privacy Law*, 3 t., Nr. 4, 2013, p. 222–228.

H. Kranenborg „Google and the Right to be Forgotten", *European Data Protection Law Review*, 1 t., Nr. 1, 2015, p. 70–79.

O. Lynskey „Deconstructing data protection: the 'added-value' of a right to data protection in the EU legal order", *International and Comparative Law Quarterly*, 63 t., Nr. 3, 2014, p. 569–597.

O. Lynskey „The Foundations of EU Data Protection Law", Oksfordas, *Oxford University Press*, 2015.

J. Mayer „Charta der Grundrechte der Europäischen Union", *Baden-Baden*, *Nomos*, 2011.

A. Mowbray „Cases, materials, and commentary on the European Convention on Human Rights", Oksfordas, *Oxford University Press*, 2012.

M. Nowak, K. Januszewski ir T. Hofstätter „All human rights for all – Vienna manual on human rights", *Antwerp, intersentia N. V., Neuer Wissenschaftlicher Verlag*, 2012.

C. Picharel ir L. Coutron „Charte des droits fondamentaux de l'Union européenne et convention européenne des droits de l'homme", Briuselis, *Emile Bruylant*, 2010.

S. Simitis „Die EU-Datenschutz-Richtlinie – Stillstand oder Anreiz?", *Neue Juristische Wochenschrift*, Nr. 5, 1997, p. 281–288.

S. Warren ir L. Brandeis „The right to privacy“, *Harvard Law Review,* 4 t., Nr. 5, 1890, p. 193–220.

R. White ir C. Ovey „The European Convention on Human Rights“, Oksfordas, *Oxford University Press*, 2010.

2 skyrius

A. Acquisty ir R. Gross „Predicting Social Security numbers from public data“, *Proceedings of the National Academy of Science*, 2009, 2009 m. liepos 7 d.

P. Carey „Data protection: A practical guide to UK and EU law“, Oksfordas, *Oxford University Press*.

Y.-A. de Montjoye, C. A. Hidalgo, M. Verleysen irV. D. Blondel „Unique in the Crowd: the Privacy Bounds of Human Mobility“, *Nature Scientific Reports*, 3 t., 2013.

L. Delgado „Vida privada y protección de datos en la Unión Europea“, Madridas, *Dykinson S. L.*, 2008.

G. Desgens-Pasanau „La protection des données à caractère personnel“, Paryžius, *LexisNexis*, 2012.

A. Di Martino „Datenschutz im europäischen Recht“, Baden Badenas, *Nomos*, 2005 m.

G. González Fuster „The Emergence of Personal Data Protection as a Fundamental Right in the EU“, *Springer*, 2014.

R. Morgan ir R. Boardman „Data protection strategy: Implementing data protection compliance“, Londonas, *Sweet & Maxwell*.

P. Ohm „Broken promises of privacy: Responding to the surprising failure of anonymization“, *UCLA Law Review*, 57 t., Nr. 6, 2010, p. 1701–1777.

P. Samarati ir L. Sweeney „Protecting Privacy when Disclosing Information: k-Anonymity and Its Enforcement through Generalization and Suppression“, *Technical Report SRI-CSL-98-04*, 1998.

L. Sweeney „K-Anonymity: A Model for Protecting Privacy“, *International Journal of Uncertainty, Fuzziness and Knowledge-based Systems*, 10 t., Nr. 5, 2002, p. 557–570.

M. Tinnefeld, B. Buchner irT. Petri „Einführung in das Datenschutzrecht: Datenschutz und Informationsfreiheit in europäischer Sicht“, Miunchenas, *Oldenbourg Wissenschaftsverlag*, 2012.

Jungtinės Karalystės informacijos komisaro biuras „Anonymisation: managing data protection risk. Code of practice“, 2012.

3–6 skyriai

U. Brühann „Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr“, 2012, skelbiama E. Grabitz, M. Hilf ir M. Nettesheim (red.) „Das Recht der Europäischen Union“, IV t., A. 30, Miunchenas, *C. H. Beck*.

C. Conde Ortiz „La protección de datos personales“, *Cadiz, Dykinson*, 2008.

L. Coudray „La protection des données personnelles dans l'Union européenne“, Sarbriukenas, *Éditions universitaires européennes*, 2010.

L. Curren ir J. Kaye „Revoking consent: a 'blind spot' in data protection law?“, *Computer Law & Security Review*, 26 t., Nr. 3, p. 273–283.

U. Dammann ir S. Simitis „EG-Datenschutzrichtlinie“, Baden Badenas, *Nomos*, 1997.

P. De Hert ir V. Papakonstantinou „The Police and Criminal Justice Data Protection Directive: Comment and Analysis“, *Computers & Law Magazine of SCL*, 22 t., Nr. 6, p. 1–5, 2012.

P. De Hert ir V. Papakonstantinou „The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals“, *Computer Law & Security Review*, 28 t., Nr. 2, p. 130–142, 2012.

Federico Feretti „A European perspective on data processing consent through the re-conceptualization of European data protection's looking glass after the Lisbon Treaty: Taking rights seriously“, *European Review of Private Law*, 20 t., Nr. 2, p. 473–506, 2012.

FRA (Europos Sąjungos pagrindinių teisių agentūra), *Data Protection in the European Union: the role of National Supervisory authorities (Strengthening the fundamental rights architecture in the EU II)*, Liuksemburgas, Europos Sąjungos leidinių biuras (Leidinių biuras), 2010.

FRA, „Developing indicators for the protection, respect and promotion of the rights of the child in the European Union" (konferencijos redakcija), Viena, FRA, 2010.

FRA, „Access to justice in Europe: an overview of challenges and opportunities", Liuksemburgas, Leidinių biuras.

Irish Health Information and Quality Authority, „Guidance on Privacy Impact Assessment in Health and Social Care", 2010.

S. Kierkegaard, N. Waters, G. Greenleaf, L. A. Bygrave, I. Lloyd ir S. Saxby „30 years on – The review of the Council of Europe Data Protection Convention 108", *Computer Law & Security Review*, 27 t., Nr. 3, p. 223-231, 2011.

S. Simitis „Bundesdatenschutzgesetz", Baden Badenas, *Nomos*, 2011.

United Kingdom Information Commissioner's Office „Privacy Impact Assessment".

7 skyrius

29 straipsnio darbo grupė (2005 m.), „Darbo dokumentas dėl 1995 m. spalio 24 d. Direktyvos 95/46/EB 26 straipsnio 1 dalies vienodo aiškinimo", WP 114, Briuselis, 2005 m. lapkričio 25 d.

Europos duomenų apsaugos priežiūros pareigūnas, „Asmens duomenų perdavimas trečiosioms šalims ir tarptautinėms organizacijoms, kurį vykdo ES institucijos ir įstaigos, poziciją nusakantis dokumentas", 2014.

S. Gutwirth, Y. Poullet, P. De Hert, C. De Terwangne ir S. Nouwt „Reinventing data protection?", Berlynas, *Springer*, 2009.

C. Kuner „Transborder data flow regulation and data privacy law", Oksfordas, *Oxford University Press*, 2013.

C. Kuner „European data protection law", Oksfordas, *Oxford University Press*, 2007.

8 skyrius

C. Blasi Casagran „Global Data Protection in the Field of Law Enforcement, an EU Perspective“, Londonas, *Routledge*, 2016.

F. Boehm „Information Sharing and Data Protection in the Area of Freedom, Security and Justice. Towards Harmonised Data Protection Principles for Information Exchange at EU-level“, Berlynas, *Springer*, 2012.

P. De Hert ir V. Papakonstantinou „The Police and Criminal Justice Data Protection Directive: Comment and Analysis“, *Computers & Law Magazine of SCL*, 22 t., Nr. 6, p. 1–5, 2012.

D. Drewer ir J. Ellermann „Europol's data protection framework as an asset in the fight against cybercrime“, *ERA Forum*, 13 t., Nr. 3, p. 381–395, 2012.

Eurojustas „Data protection at Eurojust: A robust, effective and tailor-made regime“, Haga, Eurojustas, 2014.

Europolas „*Data Protection at Europol*“, Liuksemburgas, Leidinių biuras, 2012.

A. Gutiérrez Zarza „Exchange of Information and Data Protection in Cross-border Criminal Proceedings in Europe“, Berlynas, *Springer*, 2015.

S. Gutwirth,Y. Poullet ir P. De Hert „Data protection in a profiled world“, Dordrechtas, *Springer*, 2010.

S. Gutwirth, Y. Poullet, P. De Hert ir R. Leenes „Computers, privacy and data protection: An element of choice“, Dordrechtas, *Springer*, 2011.

T. Konstadinides „Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem“, *European Law Review*, 36 t., Nr. 5, p. 722–776, 2011.

J. Santos Vara „The role of the European Parliament in the conclusion of the Transatlantic Agreements on the transfer of personal data after Lisbon“, *Centre for the Law of External Relations*, *CLEER Working Papers 2013/2*, 2013.

9 skyrius

A. Büllesbach, S. Gijrath, Y. Poullet ir R. Hacon „Concise European IT law“, Amsterdamas, *Kluwer Law International*, 2010.

S. Gutwirth,Y. Poullet ir P. De Hert „Data protection in a profiled world“, Dordrechtas, *Springer*, 2010.

S. Gutwirth, Y. Poullet, P. De Hert ir R. Leenes „Computers, privacy and data protection: An element of choice“, Dordrechtas, *Springer*, 2011.

S. Gutwirth, R. Leenes, P. De Hert ir Y. Poullet „European data protection: In good health?“, Dordrechtas, *Springer*, 2012.

T. Konstadinides „Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem“, *European Law Review*, 36 t., Nr. 5, p. 722–776, 2011.

J. Rosemary ir A. Hamilton „Data protection law and practice“, Londonas, *Sweet & Maxwell*, 2012.

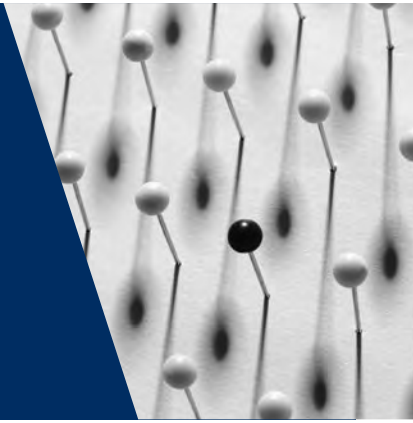
10 skyrius

K. El Emam ir C. Álvarez „A critical appraisal of the Article 29 Working Party Opinion 05/2014 on data anonymization techniques“, *International Data Privacy Law*, 5 t., Nr. 1, p. 73–87, 2015 m.

V. Mayer-Schönberger ir F. Cate „Notice and consent in a world of Big Data“, *International Data Privacy Law*, 3 t., Nr. 2, p. 67–73, 2013 m.

I. Rubistein „Big Data: The End of Privacy or a New Beginning?“, *International Data Privacy Law*, 3 t., Nr. 2, p. 74–87.

Teismų praktika



Atrinkta Europos Žmogaus Teisių Teismo praktika

Galimybė susipažinti su asmens duomenimis
Gaskin prieš Jungtinę Karalystę, Nr. 10454/83, 1989 m. liepos 7 d.
Godelli prieš Italiją, Nr. 33783/09, 2012 m. rugsėjo 25 d.
K. H. ir kiti prieš Slovakiją, Nr. 32881/04, 2009 m. balandžio 28 d.
Leander prieš Švediją, Nr. 9248/81, 1987 m. kovo 26 d.
M. K. prieš Prancūziją, Nr. 19522/09, 2013 m. balandžio 18 d.
Odièvre prieš Prancūziją (DK), Nr. 42326/98, 2003 m. vasario 13 d.

Duomenų apsaugos ir saviraiškos laisvės bei teisės gauti informaciją pusiausvyros nustatymas
Axel Springer AG prieš Vokietiją (DK), Nr. 39954/08, 2012 m. vasario 7 d.
Bohlen prieš Vokietiją, Nr. 53495/09, 2015 m. vasario 19 d.
Coudec ir Hachette Filipacchi Associés prieš Prancūziją (DK), Nr. 40454/07, 2015 m. lapkričio 10 d.
Magyar Helsinki Bizottság prieš Vengriją (DK), Nr. 18030/11, 2016 m. lapkričio 8 d.
Müller ir kiti prieš Šveicariją, Nr. 10737/84, 1988 m. gegužės 24 d.
Satakunnan Markkinapörssi Oy ir Satamedia Oy prieš Suomiją, Nr. 931/13, 2017 m. birželio 27 d.
Vereinigung bildender Künstler prieš Austriją, Nr. 68354/01, 2007 m. sausio 25 d.
Von Hannover prieš Vokietiją (Nr. 2) (DK), Nr. 40660/08 ir 60641/08, 2012 m. vasario 7 d.

Duomenų apsaugos ir religijos laisvės pusiausvyros nustatymas
Sinan Işık prieš Turkiją, Nr. 21924/05, 2010 m. vasario 2 d.

Iššūkiai, su kuriais susiduriama apsaugant duomenis internete
K. U. prieš Suomiją, Nr. 2872/02, 2008 m. gruodžio 2 d.

Duomenų subjekto sutikimas
Elberte prieš Latviją, Nr. 61243/08, 2015 m. sausio 13 d.
Sinan Işık prieš Turkiją, Nr. 21924/05, 2010 m. vasario 2 d.
Y prieš Turkiją, Nr. 648/10, 2015 m. vasario 17 d.

Susirašinėjimas
Amann prieš Šveicariją (DK), Nr. 27798/95, 2000 m. vasario 16 d.
Association for European Integration and Human Rights ir Ekimdzhiev prieš Bulgariją, Nr. 62540/00, 2007 m. birželio 28 d.
Bernh Larsen Holding AS ir kiti prieš Norvegiją, Nr. 24117/08, 2013 m. kovo 14 d.
Cemalettin Canli prieš Turkiją, Nr. 22427/04, 2008 m. lapkričio 18 d.
D. L. prieš Bulgariją, Nr. 7472/14, 2016 m. gegužės 19 d.
Dalea prieš Prancūziją, Nr. 964/07, 2010 m. vasario 2 d.
Gaskin prieš Jungtinę Karalystę, Nr. 10454/83, 1989 m. liepos 7 d.
Haralambie prieš Rumuniją, Nr. 21737/03, 2009 m. spalio 27 d.
Khelili prieš Šveicariją, Nr. 16188/07, 2011 m. spalio 18 d.
Leander prieš Švediją, Nr. 9248/81, 1987 m. kovo 26 d.
Malone prieš Jungtinę Karalystę, Nr. 8691/79, 1984 m. rugpjūčio 2 d.
Rotaru prieš Rumuniją (DK), Nr. 28341/95, 2000 m. gegužės 4 d.
S. ir Marper prieš Jungtinę Karalystę (DK), Nr. 30562/04 ir 30566/04, 2008 m. gruodžio 4 d.
Shimovolos prieš Rusiją, Nr. 30194/09, 2011 m. birželio 21 d.
Silver ir kiti prieš Jungtinę Karalystę, Nr. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 1983 m. kovo 25 d.
The Sunday Times prieš Jungtinę Karalystę, Nr. 6538/74, 1979 m. balandžio 26 d.

Nuosprendžių registro duomenų bazės
Aycaguer prieš Prancūziją, Nr. 8806/12, 2017 m. birželio 22 d.
B. B. prieš Prancūziją, Nr. 5335/06, 2009 m. gruodžio 17 d.
Brunet prieš Prancūziją, Nr. 21010/10, 2014 m. rugsėjo 18 d.
M. K. prieš Prancūziją, Nr. 19522/09, 2013 m. balandžio 18 d.
M. M. prieš Jungtinę Karalystę, Nr. 24029/07, 2012 m. lapkričio 13 d.

Duomenų saugumas
Haralambie prieš Rumuniją, Nr. 21737/03, 2009 m. spalio 27 d.
K. H. ir kiti prieš Slovakiją, Nr. 32881/04, 2009 m. balandžio 28 d.

DNR duomenų bazės
S. ir Marper prieš Jungtinę Karalystę (DK), Nr. 30562/04 ir 30566/04, 2008 m. gruodžio 4 d.

GPS duomenys
Uzun prieš Vokietiją, Nr. 35623/05, 2010 m. rugsėjo 2 d.

Asmens sveikatos duomenys
Avilkina ir kiti prieš Rusiją, Nr. 1585/09, 2013 m. birželio 6 d.
Biriuk prieš Lietuvą, Nr. 23373/03, 2008 m. lapkričio 25 d.
I prieš Suomiją, Nr. 20511/03, 2008 m. liepos 17 d.
L. H. prieš Latviją, Nr. 52019/07, 2014 m. balandžio 29 d.
L. L. prieš Prancūziją, Nr. 7508/02, 2006 m. spalio 10 d.
M. S. prieš Švediją, Nr. 20837/92, 1997 m. rugpjūčio 27 d.
Szuluk prieš Jungtinę Karalystę, Nr. 36936/05, 2009 m. birželio 2 d.
Y prieš Turkiją, Nr. 648/10, 2015 m. vasario 17 d.
Z prieš Suomiją, Nr. 22009/93, 1997 m. vasario 25 d.

Tapatybė
Ciubotaru prieš Moldovą, Nr. 27138/04, 2010 m. balandžio 27 d.
Godelli prieš Italiją, Nr. 33783/09, 2012 m. rugsėjo 25 d.
Odièvre prieš Prancūziją (DK), Nr. 42326/98, 2003 m. vasario 13 d.

Su profesine veikla susijusi informacija
G. S. B. prieš Šveicariją, Nr. 28601/11, 2015 m. gruodžio 22 d.
M. N. ir kiti prieš San Mariną, Nr. 28005/12, 2015 m. liepos 7 d.
Michaud prieš Prancūziją, Nr. 12323/11, 2012 m. gruodžio 6 d.
Niemietz prieš Vokietiją, Nr. 13710/88, 1992 m. gruodžio 16 d.

Ryšių perėmimas
Amann prieš Šveicariją (DK), Nr. 27798/95, 2000 m. vasario 16 d.
Brito Ferrinho Bexiga Villa-Nova prieš Portugaliją, Nr. 69436/10, 2015 m. gruodžio 1 d.
Copland prieš Jungtinę Karalystę, Nr. 62617/00, 2007 m. balandžio 3 d.
Halford prieš Jungtinę Karalystę, Nr. 20605/92, 1997 m. birželio 25 d.
Iordachi ir kiti prieš Moldovą, Nr. 25198/02, 2009 m. vasario 10 d.

Kopp prieš Šveicariją, Nr. 23224/94, 1998 m. kovo 5 d.
Liberty ir kiti prieš Jungtinę Karalystę, Nr. 58243/00, 2008 m. liepos 1 d.
Malone prieš Jungtinę Karalystę, Nr. 8691/79, 1984 m. rugpjūčio 2 d.
Mustafa Sezgin Tanrıkulu prieš Turkiją, Nr. 27473/06, 2017 m. liepos 18 d.
Pruteanu prieš Rumuniją, Nr. 30181/05, 2015 m. vasario 3 d.
Szuluk prieš Jungtinę Karalystę, Nr. 36936/05, 2009 m. birželio 2 d.

Subjektų, kuriems nustatytos pareigos, įsipareigojimai
B. B. prieš Prancūziją, Nr. 5335/06, 2009 m. gruodžio 17 d.
I prieš Suomiją, Nr. 20511/03, 2008 m. liepos 17 d.
Mosley prieš Jungtinę Karalystę, Nr. 48009/08, 2011 m. gegužės 10 d.

Asmens duomenys
Amann prieš Šveicariją (DK), Nr. 27798/95, 2000 m. vasario 16 d.
Bernh Larsen Holding AS ir kiti prieš Norvegiją, Nr. 24117/08, 2013 m. kovo 14 d.
Uzun prieš Vokeitiją, Nr. 35623/05, 2010 m.

Nuotraukos
Sciacca prieš Italiją, Nr. 50774/99, 2005 m. sausio 11 d.
Von Hannover prieš Vokietiją, Nr. 59320/00, 2004 m. birželio 24 d.

Teisė būti pamirštam
Satakunnan Markkinapörssi Oy ir Satamedia Oy prieš Suomiją, Nr. 931/13, 2017 m. birželio 27 d.
Segerstedt-Wiberg ir kiti prieš Švediją, Nr. 62332/00, 2006 m. birželio 6 d.

Teisė nesutikti
Leander prieš Švediją, Nr. 9248/81, 1987 m. kovo 26 d.
M. S. prieš Švediją, Nr. 20837/92, 1997 m. rugpjūčio 27 d.
Mosley prieš Jungtinę Karalystę, Nr. 48009/08, 2011 m. gegužės 10 d.
Rotaru prieš Rumuniją (DK), Nr. 28341/95, 2000 m. gegužės 4 d.
Sinan Işık prieš Turkiją, Nr. 21924/05, 2010 m. vasario 2 d.

Neskelbtinų kategorijų duomenys
Brunet prieš Prancūziją, Nr. 21010/10, 2014 m. rugsėjo 18 d.
I prieš Suomiją, Nr. 20511/03, 2008 m. liepos 17 d.
Michaud prieš Prancūziją, Nr. 12323/11, 2012 m. gruodžio 6 d.
S. ir Marper prieš Jungtinę Karalystę (DK), Nr. 30562/04 ir 30566/04, 2008 m. gruodžio 4 d.

Priežiūra ir vykdymas (įvairių subjektų, įskaitant priežiūros institucijas, vaidmuo)
I prieš Suomiją, Nr. 20511/03, 2008 m. liepos 17 d.
K. U. prieš Suomiją, Nr. 2872/02, 2008 m. gruodžio 2 d.
Von Hannover prieš Vokietiją, Nr. 59320/00, 2004 m. birželio 24 d.
Von Hannover prieš Vokietiją (Nr. 2) (DK), Nr. 40660/08 ir 60641/08, 2012 m. vasario 7 d.

Stebėjimo metodai
Allan prieš Jungtinę Karalystę, Nr. 48539/99, 2002 m. lapkričio 5 d.
Association for European Integration and Human Rights ir Ekimdzhiev prieš Bulgariją, Nr. 62540/00, 2007 m. birželio 28 d.
Bărbulescu prieš Rumuniją (DK), Nr. 61496/08, 2017 m. rugsėjo 5 d.
D. L. prieš Bulgariją, Nr. 7472/14, 2016 m. gegužės 19 d.
Dragojević prieš Kroatiją, Nr. 68955/11, 2015 m. sausio 15 d.
Karabeyoğlu prieš Turkiją, Nr. 30083/10, 2016 m. birželio 7 d.
Klass ir kiti prieš Vokietiją, Nr. 5029/71, 1978 m. rugsėjo 6 d.
Roman Zakharov prieš Rusiją (DK), Nr. 47143/06, 2015 m. gruodžio 4 d.
Rotaru prieš Rumuniją (DK), Nr. 28341/95, 2000 m. gegužės 4 d.
Szabó ir Vissy prieš Vengriją, Nr. 37138/14, 2016 m. sausio 12 d.
Taylor-Sabori prieš Jungtinę Karalystę, Nr. 47114/99, 2002 m. spalio 22 d.
Uzun prieš Vokietiją, Nr. 35623/05, 2010 m. rugsėjo 2 d.
Versini-Campinchi ir Crasnianski prieš Prancūziją, Nr. 49176/11, 2016 m. birželio 16 d.
Vetter prieš Prancūziją, Nr. 59842/00, 2005 m. gegužės 31 d.
Vukota-Bojić prieš Šveicariją, Nr. 61838/10, 2016 m. spalio 18 d.

Vaizdo stebėjimas
Köpke prieš Vokietiją, Nr. 420/07, 2010 m. spalio 5 d.
Peck prieš Jungtinę Karalystę, Nr. 44647/98, 2003 m. sausio 28 d.

Balso pavyzdžiai
P. G. ir J. H. prieš Jungtinę Karalystę, Nr. 44787/98, 2001 m. rugsėjo 25 d.
Wisse prieš Prancūziją, Nr. 71611/01, 2005 m. gruodžio 20 d.

Atrinkta Europos Sąjungos Teisingumo Teismo praktika

Su Duomenų apsaugos direktyva susijusi teismo praktika

Sujungtos bylos C-468/10 ir C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) ir Federación de Comercio Electrónico y Marketing Directo (FECEMD) prieš Administración del Estado*, 2011 m. lapkričio 24 d.

(Teisingas Duomenų apsaugos direktyvos 7 straipsnio f punkto – „teisėti kitų asmenų interesai“ – įgyvendinimas nacionalinėje teisėje)

C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) prieš Netlog NV*, 2012 m. vasario 16 d.

(Socialinio tinklo paslaugų teikėjų pareiga užkirsti kelią tinklo naudotojams neteisėtai naudoti muzikos ir audiovizualinius kūrinius)

C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce prieš Salvatore Manni*, 2017 m. kovo 9 d.

(Teisė ištrinti asmens duomenis; teisė nesutikti, kad duomenys būtų tvarkomi)

C-553/07, *College van burgemeester en wethouders van Rotterdam prieš M. E. E. Rijkeboer*, 2009 m. gegužės 7 d.

(Duomenų subjekto teisė susipažinti su duomenimis)

C-101/01, *Baudžiamoji byla prieš Bodil Lindqvist*, 2003 m. lapkričio 6 d.

(Specialios asmens duomenų kategorijos)

C-543/09, *Deutsche Telekom AG prieš Bundesrepublik Deutschland*, 2011 m. gegužės 5 d.

(Būtinybė gauti naują sutikimą)

Sujungtos bylos C-293/12 ir C-594/12, *Digital Rights Ireland Ltd prieš Minister for Communications, Marine and Natural Resources ir kt.* ir Kärntner Landesregierung ir kt. (DK), 2014 m. balandžio 8 d.

(ES pirminės teisės pažeidimas Duomenų saugojimo direktyva; teisėtas duomenų tvarkymas; tikslo ir saugojimo apribojimas)

C-518/07, *Europos Komisija prieš Vokietijos Federacinę Respubliką* (DK), 2010 m. kovo 9 d.
(Nacionalinės priežiūros institucijos nepriklausomumas)

C-288/12, *Europos Komisija prieš Vokietijos Federacinę Respubliką* (DK), 2014 m. balandžio 8 d.
(Nacionalinio duomenų apsaugos pareigūno pašalinimo iš pareigų teisėtumas)

C-614/10, *Europos Komisija prieš Austriją* (DK), 2012 m. spalio 16 d.
(Nacionalinės priežiūros institucijos nepriklausomumas)

C-212/13, *František Ryneš prieš Úřad pro ochranu osobních údajů*, 2014 m. gruodžio 11 d.
(„Duomenų tvarkymo“ ir „duomenų valdytojo“ sąvoka)

C-131/12, *Google Spain SL, Google Inc. prieš Agencia Española de Protección de Datos (AEPD), Mario Costeja González* (DK), 2014 m. gegužės 13 d.
(Paieškos sistemos paslaugų teikėjų pareigos duomenų subjekto prašymu nerodyti asmens duomenų paieškos rezultatuose; Duomenų apsaugos direktyvos taikymas; „duomenų tvarkymo“ sąvoka; sąvokos „duomenų valdytojai“ reikšmė; duomenų apsaugos ir saviraiškos laisvės pusiausvyros nustatymas; teisė būti pamirštam)

C-524/06, *Heinz Huber prieš Bundesrepublik Deutschland* (DK), 2008 m. gruodžio 16 d.
(Duomenų apie užsieniečius statistinių duomenų registruose laikymo teisėtumas)

C-473/12, *Institut professionnel des agents immobiliers (IPI) prieš Geoffrey Englebert ir kt.*, 2013 m. lapkričio 7 d.
(Teisė būti informuotam apie asmens duomenų tvarkymą)

C-362/14, *Maximilian Schrems prieš Data Protection Commissioner* (DK), 2015 m. spalio 6 d.
(Teisėto duomenų tvarkymo principas; pagrindinės teisės; „saugaus uosto“ sprendimo negaliojimas; nepriklausomų priežiūros institucijų įgaliojimai)

C-291/12, *Michael Schwarz prieš Stadt Bochum*, 2013 m. spalio 17 d.
(Prašymas priimti prejudicinį sprendimą; laisvės, saugumo ir teisingumo erdvė; biometrinis pasas; piršto atspaudai; teisinis pagrindas; proporcingumas)

C-582/14, *Patrick Breyer prieš Bundesrepublik Deutschland*, 2016 m. spalio 19 d.
(Sąvokos „asmens duomenys“ apibrėžtis; interneto protokolo adresai; internetinio žiniasklaidos paslaugų teikėjo saugomi duomenys; nacionalinės teisės aktai, pagal kuriuos neleidžiama atsižvelgti į duomenų valdytojo siekiamą teisėtą interesą)

C-434/16, *Peter Nowak prieš Data Protection Commissioner*, generalinės advokatės J. Kokott išvada, 2017 m. liepos 20 d.
(Asmens duomenų sąvoka; galimybė susipažinti su savo egzamino darbu; egzaminuotojo taisymai)

T-462/12 R, *Pilkington Group Ltd prieš Europos Komisiją*, Bendrojo Teismo pirmininko nutartis, 2013 m. kovo 11 d.

C-275/06, *Productores de Música de España (Promusicae) prieš Telefónica de España SAU* (DK), 2008 m. sausio 29 d.
(Asmens duomenų sąvoka; interneto paslaugų teikėjų pareiga atskleisti dalijimosi rinkmenomis programos „KaZaA“ naudotojų tapatybes intelektinės nuosavybės apsaugos asociacijai)

Sujungtos bylos C-465/00, C-138/01 ir C-139/01, *Rechnungshof prieš Österreichischer Rundfunk ir kt.* ir *Christa Neukomm and Jospeh Lauermann prieš Österreichischer Rundfunk*, 2003 m. gegužės 20 d.
(Teisinės pareigos skelbti asmens duomenis apie tam tikrų su viešuoju sektoriumi susijusių institucijų darbuotojų kategorijų darbo užmokestį proporcingumas)

C-70/10, *Scarlet Extended SA prieš Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 2011 m. lapkričio 24 d.
(Informacinė visuomenė; autorių teisės; internetas; tarpusavio keitimosi (angl. *peer-to-peer*) programinė įranga; interneto paslaugų teikėjai; sistemos, kuri elektroniniams pranešimams taiko filtrą, kad būtų užkirstas kelias keitimuisi rinkmenomis pažeidžiant autorių teises, diegimas; bendros pareigos stebėti perduodamą informaciją nebuvimas)

C-201/14, *Smaranda Bara ir kt. prieš Casa Națională de Asigurări de Sănătate ir kt.*, 2015 m. spalio 1 d.
(Teisė būti informuotam apie asmens duomenų tvarkymą)

Sujungtos bylos C-203/15 ir C-698/15, *Tele2 Sverige AB prieš Post- och telestryrelsen* ir *Secretary of State for the Home Department prieš Tom Watson ir kt.* (DK), 2016 m. gruodžio 21 d.

(Elektroninių ryšių konfidencialumas; elektroninių ryšių paslaugų teikėjai; įpareigojimas, susijęs su bendru ir nediferencijuotu srauto ir vietos nustatymo duomenų saugojimu; išankstinės kontrolės, kurią atliktų teismas arba nepriklausoma administracinė institucija, nebuvimas; Europos Sąjungos pagrindinių teisių chartija; suderinamumas su ES teise)

C-73/07, *Tietosuojavaltuutettu prieš Satakunnan Markkinapörssi Oy ir Satamedia Oy* (DK), 2008 m. gruodžio 16 d.

(Žurnalistinės veiklos koncepcija pagal Duomenų apsaugos direktyvos 9 straipsnį)

C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde prieš Rīgas pašvaldības SIA 'Rīgas satiksme'*, 2017 m. gegužės 4 d.

(Teisėto duomenų tvarkymo principas: teisėti interesai, kuriuos siekia įgyvendinti trečioji šalis)

Sujungtos bylos C-92/09 ir C-93/09, *Volker und Markus Schecke GbR ir Hartmut Eifert prieš Land Hessen* (DK), 2010 m.

(Asmens duomenų sąvoka; teisinės pareigos skelbti asmens duomenis apie tam tikrų ES žemės ūkio fondų gavėjus proporcingumas)

C-230/14, *Weltimmo s. r. o. prieš Nemzeti Adatvédelmi és Információszabadság Hatóság*, 2015 m. spalio 1 d.

(Nacionalinių priežiūros institucijų įgaliojimai)

C-342/12, *Worten – Equipamentos para o Lar SA prieš Autoridade para as Condições de Trabalho (ACT)*, 2013 m. gegužės 30 d.

(Asmens duomenų sąvoka; darbo laiko apskaita; su duomenų kokybe susiję principai ir duomenų tvarkymo teisėtumo kriterijai; nacionalinės institucijos, atsakingos už darbo sąlygų stebėseną, galimybė susipažinti su duomenimis; darbdavio pareiga pateikti darbo laiko sąrašus, kad su jais būtų galima nedelsiant susipažinti)

Sujungtos bylos C-141/12 ir C-372/12, *YS prieš Minister voor Immigratie, Integratie en Asiel* ir *Minister voor Immigratie, Integratie en Asiel prieš M ir S*, 2014 m. liepos 17 d.
(Duomenų subjekto teisės susipažinti su duomenimis apimtis; fizinių asmenų apsauga tvarkant asmens duomenis; asmens duomenų sąvoka; duomenys apie prašymo išduoti leidimą gyventi šalyje teikėją ir administraciniame parengiamajame dokumente pateikta teisinė analizė; Europos Sąjungos pagrindinių teisių chartija)

Su Direktyva (ES) 2016/681 susijusi teismo praktika
2017 m. liepos 26 d. *Teisingumo Teismo nuomonė 1/15 (didžioji kolegija)*.
(Teisinis pagrindas; Kanados ir Europos Sąjungos susitarimo dėl keleivio duomenų įrašo duomenų perdavimo ir tvarkymo projektas; susitarimo projekto suderinamumas su SESV 16 straipsniu ir Europos Sąjungos pagrindinių teisių chartijos 7, 8 straipsniais ir 52 straipsnio 1 dalimi)

Su ES institucijų duomenų apsaugos reglamentu susijusi teismo praktika
C-615/13 P, *ClientEarth, Pesticide Action Network Europe (PAN Europe) prieš Europos maisto saugos tarnybą (EFSA), Europos Komisiją*, 2015 m. liepos 16 d.
(Galimybė susipažinti su dokumentais)

C-28/08 P, *Europos Komisija prieš The Bavarian Lager Co. Ltd.* (DK), 2010 m. birželio 29 d.
(Galimybė susipažinti su dokumentais)

Su Direktyva 2002/58/EB susijusi teismo praktika
C-461/10, *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB prieš Perfect Communication Sweden AB*, 2012 m. balandžio 19 d.
(Autorių teisės ir gretutinės teisės; asmens duomenų tvarkymas internetu; išimtinės teisės pažeidimas; įgarsintos knygos, prieinamos per FTP serverį internetu, pasinaudojant interneto paslaugų teikėjo suteiktu IP adresu; interneto paslaugų teikėjui nustatytas įpareigojimas atskleisti IP adreso naudotojo asmenvardį (pavadinimą) ir adresą)

C-70/10, *Scarlet Extended SA prieš Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 2011 m. lapkričio 24 d.

(Informacinė visuomenė; autorių teisės; internetas; tarpusavio keitimosi (angl. *peer-to-peer*) programinė įranga; interneto paslaugų teikėjai; sistemos, kuri elektroniniams pranešimams taiko filtrą, kad būtų užkirstas kelias keitimuisi rinkmenomis pažeidžiant autorių teises, diegimas; bendros pareigos stebėti perduodamą informaciją nebuvimas)

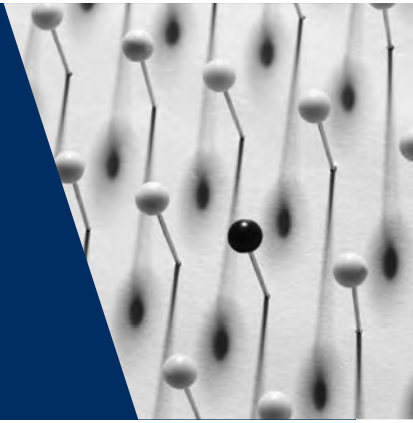
C-536/15, *Tele2 (Netherlands) BV ir kt. prieš Autoriteit Consument en Markt (AMC)*, 2017 m kovo 15 d.

(Nediskriminavimo principas; abonentų asmens duomenų teikimas siekiant teikti informacijos apie viešųjų telefono ryšių abonentus ir abonentų sąrašų paslaugas; abonento sutikimas; skirtumas priklausomai nuo valstybės narės, kurioje teikiamos informacijos apie viešųjų telefono ryšių abonentus ir abonentų sąrašų paslaugos)

Sujungtos bylos C-203/15 ir C-698/15, *Tele2 Sverige AB prieš Post- och telestyrelsen* ir *Secretary of State for the Home Department prieš Tom Watson ir kt.* (DK), 2016 m. gruodžio 21 d.

(Elektroninių ryšių konfidencialumas; elektroninių ryšių paslaugų teikėjai; pareiga bendrai nediferencijuojant saugoti srauto ir vietos nustatymo duomenis; išankstinės kontrolės, kurią atliktų teismas arba nepriklausoma administracinė institucija, nebuvimas; Europos Sąjungos pagrindinių teisių chartija; suderinamumas su ES teise)

Rodyklė



Europos Sąjungos Teisingumo Teismo praktika

Europos Žmogaus Teisių Teismo praktika

Nacionalinių teismų praktika

Daug informacijos apie Europos Sąjungos pagrindinių teisių agentūrą (FRA) paskelbta internete. Su ja galima susipažinti FRA svetainėje adresu fra.europa.eu.

Daugiau informacijos apie Europos Žmogaus Teisių Teismo praktiką yra prieinama Teismo svetainėje echr.coe.int. HUDOC paieškos portale skelbiami Teismo sprendimai ir nutartys anglų ir (arba) prancūzų kalbomis, vertimai į papildomas kalbas, teisinės santraukos, pranešimai spaudai ir kita informacija apie Teismo darbą.

Kaip įsigyti Europos Tarybos leidinių

Europos Tarybos leidinių biuras leidžia leidinius visomis šios organizacijos darbo sričių temomis, įskaitant žmogaus teises, teisės mokslą, sveikatą, etiką, socialinius reikalus, aplinką, švietimą, kultūrą, sportą, jaunimą ir architektūros paveldą. Knygų ir elektroninių leidinių iš didelio jos darbų katalogo galima užsisakyti internete (https://book.coe.int/).

Virtualios skaityklos naudotojai gali nemokamai susipažinti su ką tik išleistų svarbiausių leidinių ištraukomis arba visu tam tikrų oficialių dokumentų tekstu.

Informacija apie Europos Tarybos konvencijas, taip pat nesutrumpinti jų tekstai skelbiami Sutarčių biuro svetainėje: https://conventions.coe.int/

KAIP SUSISIEKTI SU ES

Asmeniškai

Visoje Europos Sąjungoje yra šimtai *Europe Direct* informacijos centrų. Artimiausio centro adresą rasite svetainėje https://europa.eu/european-union/contact_lt

Telefonu arba el. paštu

Europe Direct tarnyba atsakys į jūsų klausimus apie Europos Sąjungą. Su šia tarnyba galite susisiekti:
— nemokamu numeriu: 00 800 6 7 8 9 10 11 (kai kurie operatoriai už šiuos skambučius gali imti mokestį),
— šiuo standartiniu numeriu: +32 22999696 arba
— elektroniniu paštu svetainėje https://europa.eu/european-union/contact_lt.

KAIP RASTI INFORMACIJOS APIE ES

Internetas

Informacijos apie Europos Sąjungą visomis oficialiosiomis ES kalbomis galima rasti svetainėje *Europa* (https://europa.eu/european-union/index_lt).

ES leidiniai

Nemokamų ir mokamų ES leidinių galite atsisiųsti arba užsisakyti https://op.europa.eu/lt/publications. Jeigu jums reikia daugiau nemokamų leidinių egzempliorių, kreipkitės į *Europe Direct* arba į vietos informacijos centrą (žr. https://europa.eu/european-union/contact_lt).

ES teisė ir susiję dokumentai

Norėdami susipažinti su ES teisine informacija, įskaitant visus ES teisės aktus nuo 1951 m. visomis oficialiosiomis kalbomis, apsilankykite svetainėje *EUR-Lex* (http://eur-lex.europa.eu).

ES atvirieji duomenys

ES atvirųjų duomenų portale (http://data.europa.eu/euodp/lt) galima susipažinti su ES duomenų rinkiniais. Duomenis galima nemokamai parsisiųsti ir pakartotinai naudoti tiek komerciniais, tiek nekomerciniais tikslais.

doi:10.2811/022710 TK-05-17-225-LT-N

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

EDPS

Dėl sparčios informacinių technologijų plėtros padidėjo poreikis užtikrinti patikimą asmens duomenų apsaugą taikant tiek Europos Sąjungos, tiek Europos Tarybos priemones. Siekiant užtikrinti šią svarbią teisę, kyla naujų ir svarbių uždavinių, nes dėl technologinės pažangos plečiamos tokių sričių, kaip stebėjimas, ryšių perėmimas ir duomenų saugojimas, ribos. Šis vadovas parengtas siekiant supažindinti teisės specialistus, kurie neturi itin daug žinių apie duomenų apsaugą, su šia naujai besiformuojančia teisės sritimi. Jame pateikiama taikomų Europos Sąjungos ir Europos Tarybos teisės sistemų apžvalga. Jame taip pat paaiškinama svarbiausia teismų praktika ir trumpai aptariami pagrindiniai Europos Sąjungos Teisingumo Teismo ir Europos Žmogaus Teisių Teismo sprendimai. Be to, vadove pateikiami hipotetiniai scenarijai, kurie yra praktiniai įvairių problemų, su kuriomis susiduriama šioje nuolat kintančioje srityje, pavyzdžiai.

FRA – EUROPOS SĄJUNGOS PAGRINDINIŲ TEISIŲ AGENTŪRA
Schwarzenbergplatz 11 – 1040 Viena – Austrija
Tel. +43 (1) 580 30-0 – Faks. +43 (1) 580 30-699
fra.europa.eu
facebook.com/fundamentalrights
linkedin.com/company/eu-fundamental-rights-agency
twitter.com/EURightsAgency

EUROPOS ŽMOGAUS TEISIŲ TEISMAS
EUROPOS TARYBA
67075 Strasbourg Cedex – Prancūzija
Tel. +33 (0) 3 88 41 20 18 – Faks. +33 (0) 3 88 41 27 30
echr.coe.int - publishing@echr.coe.int - twitter.com/ECHR_CEDH

EUROPOS DUOMENŲ APSAUGOS PRIEŽIŪROS PAREIGŪNAS
Rue Wiertz 60 – 1047 Briuselis – Belgija
Tel. +32 2 283 19 00
edps.europa.eu – edps@edps.europa.eu – twitter.com/EU_EDPS

Europos Sąjungos leidinių biuras

ISBN 978-92-871-9828-0 (Europos Taryba)
ISBN 978-92-9474-784-6 (FRA)