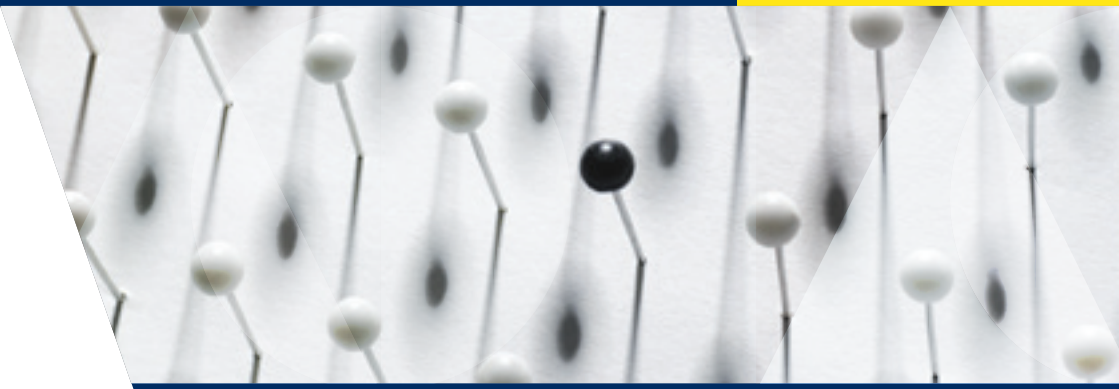
VADOVAS



Europos duomenų apsaugos teisės vadovas

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 baigtas rengti 2014 m. balandžio mėn.
Ateityje su vadovo atnaujinimais bus galima susipažinti FRA svetainėje fra.europa.eu, Europos Tarybos svetainėje coe.int/dataprotection, , ir Europos Žmogaus Teisių Teismo svetainėje echr.coe.int spustelėjus meniu nuorodą „Teismo praktika“.

Europe Direct – tai paslauga, padėsianti Jums rasti atsakymus į klausimus apie Europos Sąjungą

Informacija teikiama nemokamai telefonu (*):

00 800 6 7 8 9 10 11

(*) Informacija teikiama nemokamai, daugelis skambučių taip pat nemokami (nors kai kurie ryšio paslaugų teikėjai gali imti mokestį, taip pat gali reikėti mokėti, jeigu skambinsite taksofonu arba viešbučio telefonu).

Nuotraukų autorius (viršelio ir nugarėlės): © iStockphoto

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

Bibliografiniai duomenys pateikti šio leidinio pabaigoje.

Liuksemburgas: Europos Sąjungos leidinių biuras, 2014

ISBN 978-92-871-9943-0 (Europos Taryba)
ISBN 978-92-9239-336-6 (FRA)
doi:10.2811/54643

Printed in Belgium

Spausdinta popieriuje, balintame nenaudojant elementinio chloro (ECF)

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

Europos duomenų apsaugos teisės vadovas

Pratarmė

Šį Europos duomenų apsaugos teisės vadovą Europos Sąjungos pagrindinių teisių agentūra (FRA) ir Europos Taryba parengė kartu su Europos Žmogaus Teisių Teismo kanceliarija. Tai yra trečias teisės vadovų serijos, kurią kartu rengia FRA ir Europos Taryba, leidinys. 2011 m. kovo mėn. paskelbtas pirmasis – Europos nediskriminavimo teisės, vadovas, o 2013 m. balandžio mėn. – antrasis, Europos prieglobsčio, sienų ir imigracijos teisės, vadovas.

Nusprendėme toliau bendradarbiauti spręsdami ypač svarbų klausimą, su kuriuo kiekvienas iš mūsų susiduriame kiekvieną dieną, būtent – asmens duomenų apsaugos klausimą. Šioje srityje Europa gali pasigirti viena griežčiausių apsaugos sistemų, kurios pagrindą sudaro Europos Tarybos konvencija Nr. 108, Europos Sąjungos (ES) priemonės, taip pat Europos Žmogaus Teisių Teismo (EŽTT) ir Europos Sąjungos Teisingumo Teismo (ESTT) praktika.

Šio vadovo, kuriuo skaitytojai galės naudotis kaip orientyru, tikslas – didinti informuotumą ir gerinti žinias apie Europos Sąjungoje ir Europos Tarybos valstybėse narėse galiojančias duomenų apsaugos taisykles. Vadovas skirtas bendrosios specializacijos teisės specialistams, teisėjams, nacionalinėms duomenų apsaugos institucijoms ir kitiems duomenų apsaugos srityje dirbantiems asmenims.

2009 m. gruodžio mėn. įsigaliojus Lisabonos sutarčiai, ES pagrindinių teisių chartija tapo teisiškai privaloma ir dėl šios priežasties teisei į asmens duomenų apsaugą suteiktas atskiros pagrindinės teisės statusas. Siekiant užtikrinti šios pagrindinės teisės apsaugą labai svarbu geriau suprasti Europos Tarybos konvenciją Nr. 108 ir ES priemones, kuriomis grindžiama duomenų apsauga Europoje, taip pat ESTT ir EŽTT praktiką.

Norėtume padėkoti Liudviko Boltzmano žmogaus teisių instutui už indėlį rengiant šį vadovą. Taip pat norime išreikšti padėką Europos duomenų apsaugos priežiūros pareigūno įstaigai už pastabas rengiant leidinį. Ypatingai dėkojame Europos Komisijos duomenų apsaugos skyriui rengiant šį vadovą. Galiausiai, mes norėtume išreikšti padėką Valstybinės duomenų apsaugos inspekcijai, kuri peržiūrėjo vadovo vertimą į lietuvių kalbą.

Philippe Boillat
Europos Tarybos
žmogaus teisių ir teisės viršenybės
generalinis direktorius

Morten Kjaerum
Europos Sąjungos pagrindinių
teisių agentūros
direktorius

Turinys

Santrumpos ir akronimai

AVSS	apsauginė vaizdo stebėjimo sistema
BCR	įmonei privalomos taisyklės
CETS	Europos Tarybos sutarčių serija
Chartija	Europos Sąjungos pagrindinių teisių chartija
C-SIS	Centrinė Šengeno informacinė sistema
CRM	ryšių su klientais valdymas
EAO	Europos arešto orderis
EB	Europos bendrija
EBPO	Ekonominio bendradarbiavimo ir plėtros organizacija
EDAPP	Europos duomenų apsaugos priežiūros pareigūnas
EEE	Europos ekonominė erdvė
ELPA	Europos laisvosios prekybos asociacija
ENISA	Europos tinklų ir informacijos apsaugos agentūra
ENU	nacionalinis Europolo padalinys
ES	Europos Sąjunga
ESMA	Europos vertybinių popierių ir rinkų institucija
ES sutartis	Europos Sąjungos sutartis
ESTT	Europos Sąjungos Teisingumo Teismas (iki 2009 m. vadintas Europos Bendrijų Teisingumo Teismu (ETT)
eTEN	transeuropiniai telekomunikacijų tinklai
ET	Europos Taryba
eu-LISA	ES 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	globalinė padėties nustatymo sistema
JPI	jungtinė priežiūros institucija
JT	Jungtinės Tautos
Konvencija Nr. 108	Europos Tarybos konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu
MIS	muitinės informacinė sistema
N-SIS	nacionalinė Šengeno informacinė sistema
NVO	nevyriausybinė organizacija
PIN	asmeninis identifikavimo numeris
PNR	keleivio duomenų įrašas
SEPA	bendra mokėjimų eurais erdvė
SESV	Sutartis dėl Europos Sąjungos veikimo
SIS	Šengeno informacinė sistema
SWIFT	Pasaulinė tarpbankinių finansinių telekomunikacijų organizacija
VIS	Vizų informacinė sistema
VŽTD	Visuotinė žmogaus teisių deklaracija

Kaip naudotis šiuo vadovu

Šiame vadove pateikiama Europos Sąjungos (ES) ir Europos Tarybos (ET) duomenų apsaugai taikytinos teisės apžvalga.

Vadovas sukurtas kaip pagalbinė priemonė praktikuojantiems teisininkams, kurie nesispecializuoja duomenų apsaugos srityje; jis skirtas advokatams, teisėjams arba kitiems specialistams, taip pat kitose įstaigose, įskaitant nevyriausybines organizacijas, dirbantiems asmenims, kurie gali susidurti su klausimais, susijusiais su duomenų apsauga.

Vadovas yra pirmasis orientyras nagrinėjant su duomenų apsauga susijusią ES teisę ir Europos žmogaus teisių konvenciją (EŽTK) ir jame paaiškinama šios srities reglamentavimo ES teisėje, EŽTK, ET konvencijoje dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (Konvencija Nr. 108) ir kituose ET priemonėse tvarka. Kiekviename skyriuje visų pirma pateikiama bendra lentelė, kurioje nurodomos taikytinos teisės nuostatos, įskaitant iš dviejų atskirų Europos teisinių sistemų atrinktą svarbią teismų praktiką. Paskui paeiliui, atsižvelgiant į jų ryšį su kiekviena aptariama tema, pateikiami pagal šias dvi Europos teisines tvarkas galiojantys susiję teisės aktai. Todėl skaitytojas gali matyti, kuriose srityse dvi teisinės sistemos sutampa ir kuriose skiriasi.

Kiekvieno skyriaus pradžioje pateikiamose lentelėse išvardijamos tame skyriuje aptariamos temos, nurodomos taikytinos teisės nuostatos ir kita susijusi medžiaga, pvz., jurisprudencija. Temų eiliškumas gali šiek tiek skirtis nuo skyriaus teksto struktūros, jei manoma, kad skyriaus turinį taip galima pateikti glausčiau. Lentelėse pristatoma tiek ET, tiek ES teisė. Tai turėtų padėti naudotojams rasti pagrindinę informaciją, susijusią su jų padėtimi, visų pirma tais atvejais, kai jiems taikoma tik ET teisė.

ES nepriklausančių valstybių, kurios yra ET valstybės narės ir EŽTK ir Konvencijos Nr. 108 susitariančiosios šalys, specialistai su jų šalimi susijusią informaciją gali rasti dalyse, kuriose aptariama ET teisė. ES valstybių narių specialistai turės naudoti abi dalis, nes šiose valstybėse galioja abi teisinės tvarkos. Norintieji konkrečiu klausimu gauti daugiau informacijos gali susipažinti su specializuota medžiaga, į kurią nuorodos pateikiamos vadovo dalyje „Papildoma literatūra“.

ET teisė pristatoma pateikiant trumpas nuorodas į atrinktas Europos žmogaus teisių teismo (EŽTT) bylas. Šios bylos parinktos atsižvelgiant į daugybę EŽTT sprendimų ir nutarimų, kuriuose aptariami duomenų apsaugos klausimai.

ES teisę galima rasti patvirtintose teisėkūros priemonėse, susijusiose Sutarčių nuostatose ir Europos Sąjungos pagrindinių teisių chartijoje, kaip ją savo praktikoje išaiškino Europos Sąjungos Teisingumo Teismas (ESTT, iki 2009 m. vadintas Europos Bendrijų Teisingumo Teismu).

Šiame vadove aprašomoje arba cituojamoje teismų praktikoje pateikiama nemažai svarbių EŽTT ir ESTT praktikos pavyzdžių. Šio vadovo pabaigoje pateiktų gairių tikslas – padėti skaitytojams internete rasti nurodytą teismų praktiką.

Be to, tekstiniuose intarpuose pateikiami hipotetiniai pavyzdžiai, kuriais siekiama papildomai paaiškinti praktinį Europos duomenų apsaugos taisyklių taikymą, visų pirma tais atvejais, kai atitinkama tema nėra konkrečios EŽTT arba ESTT praktikos.

Vadovo pradžioje trumpai aprašomas dviejų teisinių sistemų, kurių pagrindą sudaro EŽTK ir ES teisė (1 skyrius), vaidmuo. 2–8 skyriuose aptariami šie klausimai:

- duomenų apsaugos terminija;
- pagrindiniai Europos duomenų apsaugos teisės principai;
- Europos duomenų apsaugos teisės taisyklės;
- duomenų subjektų teisės ir jų įgyvendinimo užtikrinimas;
- valstybės sienas kertančių duomenų srautai;
- duomenų apsauga policijos ir baudžiamosios teisenos srityje;
- kiti konkretūs Europos duomenų apsaugos teisės aktai.

1

Europos duomenų apsaugos teisės turinys ir pagrindas

ES	Aptariami klausimai	ET
Teisė į 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.		EŽTK 8 straipsnis (teisė į privataus ir šeimos gyvenimo gerbimą, būsto neliečiamybę ir susirašinėjimo slaptumą). Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (Konvencija Nr. 108).
Teisių pusiausvyra		
2010 m. lapkričio 9 d. ESTT sprendimas *Volker und Markus Schecke GbR ir Hartmut Eifert prieš Land Hessen*, sujungtos bylos C-92/09 ir C-93/09.	**Bendro pobūdžio.**	
2008 m. gruodžio 16 d. ESTT sprendimas *Tietosuojavaltuutettu prieš Satakunnan Markkinapörssi Oy ir Satamedia Oy*, C-73/07.	**Saviraiškos laisvė.**	2012 m. vasario 7 d. EŽTT sprendimas *Axel Springer AG prieš Vokietiją*. 2011 m. gegužės 10 d. EŽTT sprendimas *Mosley prieš Jungtinę Karalystę*.
	Menų ir mokslo laisvė.	2007 m. sausio 25 d. EŽTT sprendimas *Vereinigung bildender Künstler prieš Austriją*.
2008 m. sausio 28 d. ESTT sprendimas *Productores de Música de España (Promusicae) prieš Telefónica de España SAU*, C-275/06.	**Nuosavybės apsauga.**	

ES	Aptariami klausimai	ET
2010 m. birželio 29 d. ESTT sprendimas *Europos Komisija prieš The Bavarian Lager Co. Ltd*, C-28/08 P.	Galimybė susipažinti su dokumentais.	2009 m. balandžio 14 d. EŽTT sprendimas *Társaság a Szabadságjogokért prieš Vengriją*.

1.1. Teisė į duomenų apsaugą

Pagrindiniai faktai

- Pagal EŽTK 8 straipsnį teisė į tai, kad asmens duomenys nebūtų renkami ir naudojami, yra sudedamoji teisės į privataus ir šeimos gyvenimo gerbimą, būsto neliečiamybę ir susirašinėjimo slaptumą dalis.
- ET konvencija Nr. 108 yra pirmoji tarptautinė teisiškai privaloma priemonė, kurioje aiškiai reglamentuojama duomenų apsauga.
- ES teisėje duomenų apsauga pirmą kartą pradėta reglamentuoti Duomenų apsaugos direktyvoje.
- ES teisėje pripažįstama, kad duomenų apsauga yra pagrindinė teisė.

Teisė į asmens privačios erdvės apsaugą nuo kitų subjektų, visų pirma valstybės, įsikišimo pirmą kartą tarptautinėje teisinėje priemonėje buvo nustatyta 1948 m. Jungtinių Tautų (JT) visuotinės žmogaus teisių deklaracijos (VŽTD) 12 straipsnyje dėl teisės į privataus ir šeimos gyvenimo gerbimą[1]. VŽTD darė įtaką Europoje kuriant kitas su žmogaus teisėmis susijusias priemones.

1.1.1. Europos žmogaus teisių konvencija

Europos Taryba įsteigta po Antrojo pasaulinio karo siekiant, kad Europos valstybės bendrai puoselėtų teisės viršenybės, demokratijos, žmogaus teisių ir socialinio vystymosi principus. Šiuo tikslu Europos Taryba 1950 m. priėmė Europos žmogaus teisių konvenciją (EŽTK), kuri įsigaliojo 1953 m.

1 Jungtinės Tautos (JT), 1948 m. gruodžio 10 d. Visuotinė žmogaus teisų deklaracija.

Valstybės tarptautiniu lygmeniu yra įpareigotos laikytis EŽTK. Visos ET valstybės narės į savo nacionalinę teisę jau perkėlė arba joje įteisino EŽTK, todėl reikalaujama, kad jos veiktų laikydamosi Konvencijos nuostatų.

Siekiant užtikrinti, kad susitariančiosios šalys laikytųsi savo įsipareigojimų pagal EŽTK, 1959 m. Strasbūre (Prancūzija) buvo įkurtas Europos Žmogaus Teisių Teismas (EŽTT). EŽTT užtikrina, kad valstybės laikytųsi savo įsipareigojimų pagal Konvenciją, ir nagrinėja pavienių asmenų, asmenų grupių, NVO arba juridinių asmenų, teigiančių, kad Konvencija buvo pažeista, skundus. 2013 m. Europos Tarybą sudarė 47 valstybės narės, iš kurių 28 valstybės taip pat priklausė ES. Į EŽTT besikreipiantis pareiškėjas nebūtinai turi būti vienos iš valstybių narių pilietis. EŽTT taip pat gali nagrinėti tarpvalstybines bylas, vienos ar daugiau ET valstybių narių iškeltas kitai valstybei narei.

Teisė į asmens duomenų apsaugą yra viena iš teisių, saugomų pagal EŽTK 8 straipsnį, kuriame garantuojama teisė į privataus ir šeimos gyvenimo gerbimą, būsto neliečiamybę ir susirašinėjimo slaptumą, ir nustatomos sąlygos, kurių laikantis galima nustatyti šios teisės apribojimus[2].

Savo jurisprudencijoje EŽTT išnagrinėjo daugybę situacijų, kuriose iškilo duomenų apsaugos klausimas; šios situacijos visų pirma buvo susijusios su pranešimų perėmimu[3], įvairiomis stebėjimo formomis[4] ir užtikrinimu, kad valdžios institucijos nesaugotų asmens duomenų[5]. EŽTT išaiškino, kad EŽTK 8 straipsniu valstybės ne tik įpareigojamos susilaikyti nuo bet kokių veiksmų, kuriais galėtų būti pažeidžiama ši Konvencijoje įtvirtinta teisė, bet ir tam tikromis aplinkybėmis joms taip pat taikomi pozityvūs įpareigojimai aktyviais veiksmais užtikrinti faktinę pagarbą privačiam ir šeimos gyvenimui[6]. Dauguma šių bylų bus išsamiai aprašytos atitinkamuose skyriuose.

2 ET, 1950 m. Europos žmogaus teisių konvencija, ET SS Nr. 005.

3 Žr., pvz., 1984 m. rugpjūčio 2 d. EŽTT sprendimą *Malone prieš Jungtinę Karalystę*, Nr. 8691/79, 2007 m. balandžio 3 d. EŽTT sprendimą *Copland prieš Jungtinę Karalystę*, Nr. 62617/00.

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

5 Žr., pvz., 1987 m kovo 26 d. EŽTT sprendimą *Leander prieš Švediją*, Nr. 9248/81, 2008 m. gruodžio 4 d. EŽTT sprendimą *S. ir Marper prieš Jungtinę Karalystę*, Nr. 30562/04 ir 30566/04.

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

1.1.2. Europos Tarybos konvencija Nr. 108

XX a. 7-ajame dešimtmetyje pradėjus kurti informacines technologijas, vis didėjo poreikis nustatyti išsamesnes (asmens) duomenų apsaugos taisykles, kurios padėtų užtikrinti asmenų apsaugą. Iki XX a. 8-ojo dešimtmečio vidurio Europos Tarybos Ministrų Komitetas, remdamasis EŽTK 8 straipsniu, priėmė įvairias rezoliucijas dėl asmens duomenų apsaugos[7]. 1981 m. pateikta pasirašyti Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (Konvencija Nr. 108)[8]. Konvencija Nr. 108 buvo ir tebėra vienintelė duomenų apsaugos srityje galiojanti teisiškai privaloma tarptautinė priemonė.

Konvencija Nr. 108 taikoma duomenų tvarkymui tiek privačiame, tiek viešajame sektoriuje, kaip antai, duomenų tvarkymui teisėsaugos institucijų. Ja užtikrinama asmenų apsauga nuo piktnaudžiavimo atvejų, kurie gali pasitaikyti renkant ir tvarkant asmens duomenis, ir kartu siekiama reglamentuoti valstybės sienas kertančių duomenų srautus. Kalbant apie asmens duomenų rinkimą ir tvarkymą pažymėtina, kad konvencijoje nustatyti principai visų pirma yra susiję su sąžiningu ir teisėtu duomenų rinkimu ir automatiniu tvarkymu siekiant konkrečių teisėtų tikslų, o ne jų panaudojimu pažeidžiant šiuos tikslus ar duomenų laikymu ilgesnį laikotarpį, nei tai yra būtina. Šie principai taip pat susiję su duomenų kokybe, visų pirma atsižvelgiant į tai, kad duomenys turi būti adekvatūs, susiję, neperteklinai (proporcingi) ir tikslūs.

Konvencijoje nustatytos ne tik su asmens duomenų rinkimu ir tvarkymu susijusios garantijos, bet ir draudžiama tvarkyti ypatingus duomenis, pvz., susijusius su asmens rase, politiniais įsitikinimais, sveikata, religija, lytiniu gyvenimu arba informacija apie teistumą, jeigu nėra tinkamų teisinių apsaugos priemonių.

Konvencijoje taip pat numatyta asmens teisė žinoti, kad informacija apie jį yra saugoma, ir teisė prireikus reikalauti, kad tokia informacija būtų ištaisyta. Konvencijoje numatytus teisių apribojimus galima taikyti tik tuomet, kai gresia pavojus svarbesniems interesams, pvz., valstybės saugumui arba gynybai.

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

8 ET, 1981 m. Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu, Europos Taryba, ET SS Nr. 108.

Nors konvencijoje numatytas laisvas asmens duomenų srautas tarp valstybių, šios konvencijos šalių, joje taip pat nustatomi tam tikri valstybėms privalomi tokių srautų apribojimai, kai teisiniu reglamentavimu neužtikrinama lygiavertė apsauga.

Siekdamas toliau plėtoti Konvencijoje Nr. 108 nustatytus bendruosius principus ir taisykles, ET Ministrų Komitetas priėmė keletą teisiškai neįpareigojančių rekomendacijų (žr. 7 ir 8 skyrius).

Konvenciją Nr. 108 ratifikavo visos ES valstybės narės. 1999 m. Konvencija Nr. 108 buvo iš dalies pakeista siekiant, kad jos susitariančiąja šalimi galėtų tapti ES[9]. 2001 m. buvo priimtas Konvencijos Nr. 108 papildomas protokolas, kuriame įtvirtintos konvencijos nepasirašiusioms šalims, t. y. trečiosioms valstybėms, taikytinos nuostatos dėl valstybės sienas kertančių duomenų srautų ir dėl privalomo nacionalinių duomenų apsaugos priežiūros institucijų įkūrimo[10].

Apžvalga

Priėmus sprendimą atnaujinti Konvenciją Nr. 108 ir 2011 m. atlikus viešas konsultacijas buvo galima patvirtinti du pagrindinius Konvencijos Nr. 108 atnaujinimo darbo tikslus: sustiprinti privatumo apsaugą skaitmeninėje erdvėje ir sugriežtinti konvencijos įgyvendinimo priežiūros mechanizmą.

Konvenciją Nr. 108 gali pasirašyti ET nepriklausančios valstybės, įskaitant ne Europos valstybes. Konvencijos potencialas tapti visuotiniu standartu ir atvirumas galėtų būti pagrindu skatinančiu užtikrinti duomenų apsaugą visame pasaulyje.

Šiuo metu 45 iš 46 Konvencijos Nr. 108 susitariančiųjų šalių yra ET valstybės narės. Pirmoji ne Europos valstybė – Urugvajus – prie Konvencijos Nr. 108 prisijungė 2013 m. rugpjūčio mėn., o Marokas, kurį prisijungti prie Konvencijos Nr. 108 paragino Ministrų Komitetas, šiuo metu rengia oficialius prisijungimo dokumentus.

9 ET, 1999 m. birželio 15 d. Strasbūre posėdžiavusio Ministrų Komiteto priimti Konvencijos dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108) pakeitimai, kuriais Europos Bendrijoms leidžiama prisijungti prie konvencijos; Konvencijos Nr. 108 23 straipsnio 2 dalis su pakeitimais.

10 ET, 2001 m. Konvencijos dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu Papildomas protokolas dėl priežiūros institucijų ir tarpvalstybinių duomenų srautų, ET SS Nr. 181.

1.1.3. Europos Sąjungos duomenų apsaugos teisė

ES teisę sudaro Sutartys ir ES antrinė teisė. Sutartis, t. y. Europos Sąjungos sutartį (ES sutartis) ir Sutartį dėl Europos Sąjungos veikimo (SESV), patvirtino visos ES valstybės narės ir jos kartu vadinamos ES pirmine teise. ES reglamentus, direktyvas ir sprendimus priima ES institucijos, kurioms tokie įgaliojimai suteikti Sutartimis; dažnai šie teisės aktai vadinami ES antrine teise.

Pagrindinė ES teisinė priemonė, susijusi su duomenų apsauga, yra 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*)[11]. Direktyva buvo priimta 1995 m., t. y. kaip tik tuo metu, kai keletas valstybių narių jau buvo priėmusios nacionalinius įstatymus, susijusius su duomenų apsauga. Laisvas prekių, kapitalo, paslaugų ir asmenų judėjimas vidaus rinkoje taip pat reiškė laisvą duomenų judėjimą, kurio nebūtų galima įgyvendinti valstybėms narėms neužtikrinus vienodo aukšto lygio duomenų apsaugos.

Priimant Duomenų apsaugos direktyvą buvo siekiama suderinti[12] nacionalinius duomenų apsaugos įstatymus, tačiau joje numatytas tam tikras specifinio reglamentavimo lygis, panašus į (tuo metu) galiojusius nacionalinius duomenų apsaugos įstatymus. Pagal ESTT „Direktyva 95/46 yra skirta [...] užtikrinti, kad teisių ir laisvių, susijusių su asmens duomenų tvarkymu lygis būtų lygiavertis visose valstybėse narėse. [...] nacionalinių teisės aktų, taikomų šioje srityje, suderinimas neturi sąlygoti jų teikiamos apsaugos susilpnėjimo, bet priešingai, turi siekti užtikrinti aukštą apsaugos lygį Europos Sąjungoje. Taigi, [...] šių nacionalinių teisės aktų suderinimas neturi būti ribojamas minimaliu suderinimu, bet siekti galutinio harmonizavimo[13]. Todėl valstybės narės, įgyvendindamos direktyvą, turi ribotą laisvę veikti savo nuožiūra.

Duomenų apsaugos direktyva sukurta siekiant konkretizuoti teisės į privatumą, kuri jau numatyta Konvencijoje Nr. 108, principus ir juos praplėsti. Tai, kad 15 ES valstybių narių 1995 m. taip pat buvo Konvencijos Nr. 108 susitariančiosios šalys, panaikina galimybę šiose dviejose teisinėse priemonėse nustatyti prieštaraujančias taisykles. Vis dėlto Duomenų apsaugos direktyvoje įtvirtinta Konvencijos Nr. 108 11 straipsnyje numatyta galimybė nustatyti papildomas apsaugos priemones. Visų pirma paaiškėjo, kad nepriklausomos priežiūros, kaip priemonės, padedančios užtikrinti

11 Duomenų apsaugos direktyva, OL L 281, 1995, p. 31.

12 Žr., pvz., Duomenų apsaugos direktyvos 1, 4, 7 ir 8 konstatuojamąsias dalis.

13 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 lapkričio 24 d., 28-29 p.

geresnę atitiktį duomenų apsaugos taisyklėms, numatymas buvo svarbus indėlis siekiant veiksmingos Europos duomenų apsaugos teisės. (Todėl ši priežiūra 2001 m. buvo perkelta į ET teisę priimant Konvencijos Nr. 108 papildomą protokolą.)

Teritoriniu požiūriu Duomenų apsaugos direktyva taikoma ne tik 28 ES valstybėms narėms, bet ir kitoms ES nepriklausančioms valstybėms narėms, kurios yra prisijungusios prie Europos ekonominės erdvės (EEE)[14], t. y. Islandijai, Lichtenšteinui ir Norvegijai.

Liuksemburge įsikūręs ESTT turi jurisdikciją nustatyti, ar valstybė narė įgyvendino savo įsipareigojimus pagal Duomenų apsaugos direktyvą, ir priimti prejudicinius sprendimus dėl direktyvos galiojimo ir aiškinimo, kad ji būtų veiksmingai ir vienodai taikoma valstybėse narėse. Svarbi Duomenų apsaugos direktyvos taikymo išimtis yra susijusi su šeimai taikoma išimtimi, t. y. atvejai, kai asmens duomenis privatūs asmenys tvarko tik asmeniniais arba šeimos tikslais[15]. Paprastai toks tvarkymas laikomas sudedamąja privataus asmens laisvių dalimi.

Atsižvelgiant į Duomenų apsaugos direktyvos priėmimo metu galiojusią ES pirminę teisę, direktyvos esminės nuostatos taikomos tik su vidaus rinka susijusiems klausimams. Ypač svarbu paminėti, kad direktyva netaikoma klausimams, susijusiems su bendradarbiavimu policijos ir baudžiamosios teisenos srityje. Sprendžiant šiuos klausimus taikomos skirtingos duomenų apsaugą reglamentuojančios teisinės priemonės, kurios išsamiai aprašomos 7 skyriuje.

Duomenų apsaugos direktyva galėjo būti taikoma tik ES valstybėse narėse, todėl siekiant nustatyti duomenų apsaugą ES institucijoms ir įstaigoms tvarkant asmens duomenis, reikėjo patvirtinti papildomą teisinę priemonę. Šiuo tikslu priimtas 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*)[16].

Be to, net ir tose srityse, kuriose taikoma Duomenų apsaugos direktyva, dažnai reikia išsamesnių duomenų apsaugos nuostatų, siekiant didesnio aiškumo nustatant kitų teisėtų interesų pusiausvyrą. Galima paminėti du pavyzdžius – Direktyvą 2002/58/EB

14 Europos ekonominės erdvės susitarimas, OL L 1, 1994, kuris įsigaliojo 1994 m. sausio 1 d.

15 Duomenų apsaugos direktyvos 3 straipsnio 2 dalies antra įtrauka.

16 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.

dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (*Direktyva dėl privatumo ir elektroninių ryšių*)[17] ir Direktyvą 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 (*Duomenų saugojimo direktyva*)[18] (neteko galios 2014 m. balandžio 8d.). Kiti pavyzdžiai bus aptarti 8 skyriuje. Tokios nuostatos turi atitikti Duomenų apsaugos direktyvą.

Europos Sąjungos pagrindinių teisių chartija

Pirmosiose Europos Bendrijų sutartyse nebuvo užsimenama apie žmogaus teises arba jų apsaugą. Tačiau pirmosioms byloms, kuriose buvo nagrinėjami tariami žmogaus teisių pažeidimai ES teisės taikymo srityje, pasiekus tuometinį Europos Bendrijų Teisingumo Teismą, prireikė įtvirtinti naują požiūrį. Siekdamas asmenims suteikti apsaugą, ESTT įtraukė pagrindines teises į bendruosius Europos teisės principus. Pasak ESTT, šie bendrieji principai atspindi žmogaus teisių apsaugos turinį, kurį galima rasti nacionalinėse konstitucijose ir sutartyse dėl žmogaus teisių, visų pirma EŽTK. ESTT nurodė užtikrinsiantis ES teisės atitiktį šiems principams.

ES, pripažindama, kad jos politika galėtų daryti poveikį žmogaus teisėms, ir stengdamasi labiau priartinti piliečius prie ES, 2000 m. paskelbė Europos Sąjungos pagrindinių teisių chartiją (toliau – Chartija). Šioje Chartijoje, sujungiant konstitucines tradicijas ir valstybių narių bendrus tarptautinius įsipareigojimus, įtvirtinamos pačios įvairiausios pilietinės, politinės, ekonominės ir socialinės Europos piliečių teisės. Chartijoje teisės aprašomos šešiuose skirsniuose: orumas, laisvės, lygybė, solidarumas, pilietinės teisės ir teisingumas.

Iš pradžių Chartija buvo tik politinio pobūdžio, tačiau vėliau ji tapo teisiškai privalomu dokumentu[19], o 2009 m. gruodžio 1 d. įsigaliojus Lisabonos sutarčiai[20], buvo įtraukta į ES pirminę teisę (žr. ES sutarties 6 straipsnio 1 dalį).

17 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.

18 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 *(Duomenų saugojimo direktyva)* (neteko galios 2014 m. balandžio 8d.), OL L 105, 2006.

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

20 Žr. Europos Bendrijos (2012 m.), Europos Sąjungos sutarties suvestinę redakciją, OL C 326, 2012; ir Europos Bendrijos (2012 m.), SESV suvestinę redakciją, OL C 326, 2012.

ES pirminėje teisėje taip pat numatyta bendroji ES kompetencija priimti su duomenų apsaugos klausimų reglamentavimu susijusius teisės aktus (SESV 16 straipsnis).

Chartijoje ne tik garantuojama pagarba į privatų ir šeimos gyvenimą (7 straipsnis), bet ir nustatoma teisė į duomenų apsaugą (8 straipsnis), kuri aiškiai prilyginama ES teisėje galiojančiai pagrindinės teisės apsaugai. ES institucijos ir valstybės narės privalo užtikrinti ir garantuoti šią teisę, kuri taip pat taikoma valstybėms narėms įgyvendinant Sąjungos teisę (Chartijos 51 straipsnis). Chartijos 8 straipsnis, suformuluotas praėjus keleriems metams po Duomenų apsaugos direktyvos priėmimo, turi būti suprantamas kaip apimantis iki tol galiojusią ES duomenų apsaugos teisę. Todėl Chartijos 8 straipsnio 1 dalyje aiškiai užsimenama apie teisę į duomenų apsaugą, o 8 straipsnio 2 dalyje pateikiama nuoroda į pagrindinius duomenų apsaugos principus. Galiausiai Chartijos 8 straipsnio 3 dalyje užtikrinama, kad nepriklausoma institucija kontroliuos šių principų įgyvendinimą.

Apžvalga

2012 m. sausio mėn. Europos Komisija pasiūlė duomenų apsaugos reformos dokumentų rinkinį ir nurodė, kad dabartines duomenų apsaugos taisykles reikia atnaujinti atsižvelgiant į sparčią technologinę pažangą ir globalizaciją. Reformos dokumentų rinkinį sudaro Bendrojo duomenų apsaugos reglamento pasiūlymas[21], kuriuo planuojama pakeisti Duomenų apsaugos direktyvą, ir nauja Duomenų apsaugos direktyva[22], kurioje bus numatyta duomenų apsauga srityse, susijusiose su policijos ir teisminiu bendradarbiavimu baudžiamosiose bylose. Rengiant šį vadovą diskusijos dėl reformų dokumentų rinkinio dar nebuvo baigtos.

1.2. Teisių pusiausvyra

Pagrindinis faktas

- Teisė į duomenų apsaugą nėra absoliuti teisė; ji turi būti derinama su kitomis teisėmis.

21 Europos Komisija (2012 m.), 2012 m. sausio 25 d. *Pasiūlymas dėl Europos Parlamento ir Tarybos reglamento dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (Bendrasis duomenų apsaugos reglamentas)*, KOM(2012) 11 galutinis, Briuselis.

22 Europos Komisija (2012 m.), 2012 m. sausio 25 d. *Pasiūlymas dėl Europos Parlamento ir Tarybos direktyvos dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, nustatymo ar traukimo baudžiamojon atsakomybėn už jas arba baudžiamųjų sankcijų vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo (Bendroji duomenų apsaugos direktyva)*, KOM(2012) 10 galutinis, Briuselis.

Chartijos 8 straipsnyje numatyta pagrindinė teisė į asmens duomenų apsaugą „nėra absoliuti ir turi būti vertinama atsižvelgiant į jos socialinį tikslą“[23]. Todėl Chartijos 52 straipsnio 1 dalyje pripažįstama, kad įgyvendinant tokias teises, kurios, pvz., įtvirtintos Chartijos 7 ir 8 straipsniuose, gali būti nustatomi apribojimai, jei jie numatyti įstatymo, nekeičia tokių teisių ir laisvių esmės ir, remiantis proporcingumo principu, yra būtini ir tikrai atitinka bendruosius Europos Sąjungos pripažintus principus arba reikalingi kitų teisėms ir laisvėms apsaugoti[24].

EŽTK sistemoje duomenų apsauga garantuojama 8 straipsnyje (teisė į privataus ir šeimos gyvenimo gerbimą) ir, kaip numatyta Chartijos sistemoje, šią teisę reikia taikyti atsižvelgiant į kitų konkuruojančių teisių taikymo sritį. Pagal EŽTK 8 straipsnio 2 dalį „valstybės institucijos neturi teisės apriboti naudojimosi šiomis teisėmis, išskyrus įstatymų nustatytus atvejus ir kai tai būtina demokratinėje visuomenėje <...> kitų asmenų teisėms ir laisvėms apsaugoti“.

Todėl tiek EŽTT, tiek ESTT ne kartą nurodė, kad taikant ir aiškinant EŽTK 8 straipsnį ir Chartijos 8 straipsnį būtina užtikrinti teisės į duomenų apsaugą ir kitų teisių pusiausvyrą[25]. Keletas svarbių pavyzdžių padės atskleisti, kaip ši pusiausvyra užtikrinama.

1.2.1. Saviraiškos laisvė

Tikėtina, kad praktikoje pirmiausia susidursime su teisės į duomenų apsaugą ir saviraiškos laisvės kolizija.

Saviraiškos laisvės apsauga užtikrinama Chartijos 11 straipsnyje („Saviraiškos ir informacijos laisvė“). Ši teisė apima „laisvę turėti savo įsitikinimus, gauti bei skleisti informaciją ir idėjas valdžios institucijoms nekliudant ir nepaisant valstybių sienų“. 11 straipsnis yra susijęs su EŽTK 10 straipsniu. Pagal Chartijos 52 straipsnio 3 dalį joje nurodytų teisių, atitinkančių EŽTK garantuojamas teises, „esmė ir taikymo sritis

23 Žr., pvz., 2010 m. lapkričio 9 d. ESTT sprendimo *Volker ir Markus Schecke GbR ir Hartmut Eifert prieš Land Hessen*, sujungtos bylos C-92/09 ir C-93/09, 48 punktą.

24 *Ibid.*, 50 punktas.

25 2012 m. vasario 7 d. EŽTT sprendimas *Von Hannover prieš Vokietiją (Nr. 2)* (didžioji kolegija, toliau – DK), Nr. 40660/08 ir 60641/08; 2011 m. lapkričio 24 d. ESTT sprendimo *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) ir Federación de Comercio Electrónico y Marketing Directo (FECEMD) prieš Administración del Estado*, sujungtos bylos C-468/10 ir C-469/10, 48 punktas; 2008 m. sausio 29 d. ESTT sprendimo *Productores de Música de España (Promusicae) prieš Telefónica de España SAU*, C-275/06, 68 punktas. Taip pat žr. Europos Taryba (2013 m.), Europos žmogaus teisių teismo praktika, susijusi su asmens duomenų apsauga, DP (2013 m.). Teismo praktiką galima rasti adresu www.coe.int/t/dghl/standardsESTTing/dataprotection/Judgments/DP%202013%20Case%20Law_Eng%20%28final%2018%2007%202013%29.pdf.

yra tokia, kaip nustatyta toje Konvencijoje“. Todėl apribojimai, kuriuos galima teisėtai nustatyti Chartijos 11 straipsnyje garantuojamai teisei, negali būti didesni už EŽTK 10 straipsnio 2 dalyje numatytus apribojimus, kitaip tariant, jie turi būti nustatomi įstatymu ir būtini demokratinėje visuomenėje „kitų asmenų garbei ir teisėms“ apsaugoti. Ši samprata taikoma ir teisei į duomenų apsaugą.

Asmens duomenų apsaugos ir saviraiškos laisvės santykis reglamentuojamas Duomenų apsaugos direktyvos 9 straipsnyje „Asmens duomenų tvarkymas ir laisvė reikšti savo mintis ir įsitikinimus“[26]. Pagal šį straipsnį valstybės narės numato įvairias išimtis arba apribojimus, susijusius su duomenų apsauga, įskaitant pagrindinės teisės į privatumą, numatytos direktyvos II, IV ir VI skyriuose, apribojimus. Tokios išimtys turi būti numatomos tik žurnalistiniais sumetimais arba meninės ar literatūrinės raiškos tikslais, kurie atitinka pagrindinės teisės į saviraiškos laisvę turinį, ir jeigu tokios išimtys yra būtinos teisę į privatumą suderinti su saviraiškos laisvę reglamentuojančiomis taisyklėmis.

Pavyzdys. Byloje *Tietosuojavaltuutettu prieš Satakunnan Markkinapörssi Oy ir Satamedia Oy*[27] ESTT buvo prašoma išaiškinti Duomenų apsaugos direktyvos 9 straipsnį ir apibūdinti duomenų apsaugos ir spaudos laisvės santykį. Teismas turėjo nagrinėti klausimą dėl *Markkinapörssi* ir *Satamedia* paskelbtų apytiksliai 1,2 mln. fizinių asmenų mokestinių duomenų, kurie buvo teisėtai gauti iš Suomijos mokesčių institucijų. Visų pirma Teismas turėjo patikrinti, ar asmens duomenys, su kuriais leido susipažinti mokesčių institucijos, siekdamos sudaryti sąlygas mobiliųjų telefonų naudotojams gauti mokestinius duomenis, susijusius su kitais fiziniais asmenimis, buvo tvarkomi tik žurnalistiniais sumetimais. Priėjęs prie išvados, kad *Satakunnan* „tvarkė asmens duomenis“ taip, kaip nurodyta Duomenų apsaugos direktyvos 3 straipsnio 1 dalyje, Teismas toliau aiškino direktyvos 9 straipsnį. Teismas pirmiausia atkreipė dėmesį į teisės į saviraiškos laisvę svarbą kiekvienoje demokratinėje visuomenėje ir nurodė, kad su laisve susijusios sąvokos, pvz., žurnalistika, turėtų būti aiškinamos plačiai. Paskui jis atkreipė dėmesį į tai, kad, siekiant nustatyti dviejų pagrindinių teisių pusiausvyrą, teisės į duomenų apsaugą išimtys ir apribojimai turi būti taikomi tik tiek, kiek tai yra būtina. Šiomis aplinkybėmis Teismas manė, kad *Markkinapörssi* ir *Satamedia* vykdyta veikla, susijusi su dokumentų, kurie pagal nacionalinės teisės aktus yra skelbiami viešai, duomenimis, gali būti prilyginama žurnalistinei veiklai, jeigu jos

26 Duomenų apsaugos direktyvos 9 straipsnis.

27 2008 m. gruodžio 16 d. ESTT sprendimo *Tietosuojavaltuutettu prieš Satakunnan Markkinapörssi Oy ir Satamedia Oy*, C-73/07, 56, 61 ir 62 punktai.

tikslas – atskleisti visuomenei informaciją, nuomones arba idėjas, nepaisant šiuo tikslu joms teikti naudojamų priemonių. Teismas taip pat nusprendė, kad ši veikla nėra susijusi tik su žiniasklaidos įmonėmis; ją taip pat galima vykdyti siekiant gauti pelno. Vis dėlto ESTT nurodė, kad nacionalinis teismas turi nuspręsti, ar šioje byloje buvo vykdoma žurnalistinė veikla.

Kalbant apie teisės į duomenų apsaugą ir teisės į saviraiškos laisvę derinimą, pažymėtina, kad šioje srityje EŽTT priėmė keletą žinomų sprendimų.

Pavyzdys. Byloje *Axel Springer AG prieš Vokietiją*[28] EŽTT nusprendė, kad vidaus teismo nustatytas draudimas laikraščio savininkui, kuris norėjo išspausdinti straipsnį apie garsaus aktoriaus areštą ir nuteisimą, prieštaravo EŽTK 10 straipsniui. EŽTT pakartojo teismo praktikoje nusistovėjusius kriterijus, kuriais vadovaujantis nustatoma teisės į saviraiškos laisvę ir teisės į privataus gyvenimo gerbimą pusiausvyra:

- pirma, ar susijusiame straipsnyje paskelbtas įvykis buvo visuotinės svarbos: asmens areštas ir nuteisimas buvo viešas teisminis faktas, todėl jis buvo susijęs su viešuoju interesu;
- antra, ar susijusį asmenį galima priskirti viešų asmenų grupei: susijęs asmuo buvo aktorius, pakankamai gerai žinomas, kad jį būtų galima priskirti viešų asmenų grupei, ir
- trečia, kaip informacija buvo gauta ir ar ji buvo patikima: informaciją pateikė prokuroras, o abiejuose leidiniuose pateiktos informacijos tikslumo šalys neginčijo.

Todėl EŽTT nusprendė, kad įmonei nustatyti leidybos apribojimai nebuvo pagrįstai proporcingi atsižvelgiant į teisėtą tikslą apsaugoti pareiškėjo privatų gyvenimą. Teismas nusprendė, kad EŽTK 10 straipsnis buvo pažeistas.

Pavyzdys. Byloje *Von Hannover prieš Vokietiją (Nr. 2)*[29] EŽTT nustatė, kad, nepatenkinus Monako princesės Karolinos prašymo uždrausti viešai spausdinti jos ir

28 2012 m. vasario 7 d. EŽTT sprendimo *Axel Springer AG prieš Vokietiją* (DK), Nr. 39954/08, 90 ir 91 punktai.

29 2012 m. vasario 7 d. EŽTT sprendimo *Von Hannover prieš Vokietiją (Nr. 2)* (DK), Nr. 40660/08 ir 60641/08, 118 ir 124 punktai.

jos vyro, slidinėjančių per atostogas, nuotrauką, teisė į privataus gyvenimo gerbimą nebuvo pažeista. Nuotrauka buvo pridėta prie straipsnio, kuriame, be kitų klausimų, pranešama ir apie prastą princo Rainiero sveikatos būklę. EŽTT padarė išvadą, kad vidaus teismai nustatė tinkamą leidybos įmonių teisės į saviraiškos laisvę ir pareiškėjų teisės į jų privataus gyvenimo gerbimą pusiausvyrą. Negalima būtų teigti, kad vidaus teismai nepagrįstai kvalifikavo princo Rainiero ligą kaip svarbų šiuolaikinei visuomenei įvykį, todėl EŽTT galėjo sutikti, kad kartu su straipsniu paskelbta nuotrauka tam tikrais aspektais paskatino diskusijas viešojo intereso klausimais. Teismas nusprendė, kad EŽTK 8 straipsnis nebuvo pažeistas.

EŽTT praktikoje vienas esminių kriterijų, susijusių su pusiausvyros tarp šių teisių nustatymu, yra tai, ar saviraiškos laisvė padeda skatinti diskusijas bendrais viešojo intereso klausimais.

Pavyzdys. Byloje *Mosley prieš Jungtinę Karalystę*[30] nacionaliniame savaitraštyje buvo paviešinta intymi pareiškėjo nuotrauka. Tuomet pareiškėjas teigė, kad buvo pažeistas EŽTK 8 straipsnis, nes prieš paviešinant atitinkamas nuotraukas jis neturėjo galimybės uždrausti tokio veiksmo, kadangi laikraščiui tais atvejais, kai viešinama medžiaga galėjo pažeisti asmens teisę į privatumą, nebuvo taikomi jokie išankstinio pranešimo reikalavimai. Nors tokia medžiaga iš esmės buvo skelbiama pramoginiais, o ne šviečiamojo pobūdžio tikslais, neabejotina, kad ją skelbiant buvo taikoma EŽTK 10 straipsnio apsauga, kuri galėtų būti ne tokia svarbi, palyginti su EŽTK 8 straipsnio reikalavimais, kai informacija buvo privataus ir intymaus turinio ir kai jos skleidimas neatitiko viešojo intereso. Vis dėlto reikia ypač atidžiai nagrinėti apribojimus, kurie galėtų būti taikomi kaip tam tikros cenzūros priemonės prieš paskelbiant medžiagą. Atsižvelgdamas į išankstinio pranešimo reikalavimo galimą atgrasomąjį poveikį, abejones dėl jo veiksmingumo ir įvairias interpretacijas toje srityje, EŽTT padarė išvadą, kad pagal 8 straipsnį teisiškai privalomas išankstinio pranešimo reikalavimas nebuvo būtinas. Todėl Teismas nusprendė, kad 8 straipsnis nebuvo pažeistas.

Pavyzdys. Byloje *Biriuk prieš Lietuvą*[31] pareiškėjas prašė, kad dienraštis atlygintų nuostolius, jo patirtus paskelbus straipsnį, kuriame buvo nurodyta, kad pareiškėjas yra užsikrėtęs ŽIV. Šią informaciją tariamai patvirtino vietos ligoninės gydytojai. EŽTT nemanė, kad atitinkamas straipsnis padėjo skatinti

30 2011 m. gegužės 10 d. EŽTT sprendimo *Mosley prieš Jungtinę Karalystę*, Nr. 48009/08, 129 ir 130 punktai.

31 2008 m. lapkričio 25d. EŽTT sprendimas *Biriuk prieš Lietuvą*, Nr. 23373/03.

diskusijas viešojo intereso klausimais, ir pakartojo, kad asmens duomenų, visų pirma medicininių duomenų, apsauga yra labai svarbi asmeniui siekiant tinkamai naudotis teise į privataus ir šeimos gyvenimo gerbimą, kaip nustatyta EŽTK 8 straipsnyje. Teismas ypatingą dėmesį atkreipė į tai, kad, kaip nurodoma dienraščio straipsnyje, ligoninės gydytojai informaciją apie pareiškėjo ŽIV infekciją pateikė akivaizdžiai pažeisdami savo pareigą išsaugoti medicinos paslaptį. Todėl valstybė nesugebėjo užtikrinti pareiškėjo teisės į privataus gyvenimo gerbimą apsaugos. Teismas nusprendė, kad 8 straipsnis buvo pažeistas.

1.2.2. Teisė susipažinti su dokumentais

Chartijos 11 straipsnyje ir EŽTK 10 straipsnyje numatyta informacijos laisve apsaugoma teisė ne tik skleisti, bet ir *gauti* informaciją. Vis geriau suprantama skaidrios vyriausybės veiklos svarba demokratinės visuomenės veikimui. Todėl pastaruosius du dešimtmečius teisė susipažinti su valdžios institucijų turimais dokumentais pripažįstama svarbia kiekvieno ES piliečio ir bet kurio fizinio arba juridinio asmens, gyvenančio arba turinčio registruotą būstinę valstybėje narėje, teise.

ET teisėje galima nurodyti Rekomendacijoje dėl galimybės susipažinti su oficialiais dokumentais įtvirtintus principus, kuriais remdamiesi teisės aktų kūrėjai parengė Konvenciją dėl galimybės susipažinti su oficialiais dokumentais (*Konvencija Nr. 205*)[32]. **ES teisėje** teisė susipažinti su dokumentais garantuojama Reglamente (EB) Nr. 1049/2001 dėl galimybės visuomenei susipažinti su Europos Parlamento, Tarybos ir Komisijos dokumentais (*Galimybės susipažinti su dokumentais reglamentas*)[33]. Chartijos 42 straipsnyje ir SESV 15 straipsnio 3 dalyje ši teisė susipažinti buvo praplėsta ir apima teisę susipažinti su „Sąjungos institucijų, įstaigų ir organų dokumentais bet kokiu pavidalu“. Pagal Chartijos 52 straipsnio 2 dalį teisė susipažinti su dokumentais taip pat įgyvendinama laikantis SESV 15 straipsnio 3 dalyje numatytų sąlygų ir ribų. Ši teisė gali prieštarauti teisei į duomenų apsaugą, jeigu susipažinus su dokumentu būtų atskleisti kitų asmenų asmens duomenys. Todėl gali prireikti nustatyti prašymų leisti susipažinti su valdžios institucijų turimais dokumentais arba informacija ir asmenų, kurių duomenys pateikiami prašomuose dokumentuose, teisės į duomenų apsaugą pusiausvyrą.

32 Europos Tarybos Ministrų Komitetas (2002 m.), 2002 m. vasario 21 d. Europos Tarybos Ministrų Komiteto rekomendacija Nr. R (2002) 2 valstybėms narėms dėl galimybės susipažinti su oficialiais dokumentais; Europos Taryba, 2009 m. birželio 18 d. Konvencija dėl galimybės susipažinti su oficialiais dokumentais, ET SS Nr. 205. Konvencija dar neįsigaliojo.

33 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.

Pavyzdys. Byloje *Komisija prieš Bavarian Lager*[34] ESTT apibrėžė asmens duomenų apsaugos taikymo sritį atsižvelgiant į galimybę susipažinti su ES institucijų dokumentais ir apibūdino reglamentų (EB) Nr. 1049/2001 (*Galimybės susipažinti su dokumentais reglamentas*) ir Nr. 45/2001 (*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* yra palankesni nacionaliniams gamintojams. Reaguodama į *Bavarian Lager* skundą, Europos Komisija nusprendė iškelti Jungtinei Karalystei bylą dėl įsipareigojimų nevykdymo, kurioje Jungtinė Karalystė buvo įpareigota pakeisti ginčijamas teisės aktų nuostatas ir suderinti jas su ES teise. Tuomet *Bavarian Lager* paprašė, kad Komisija, be kitų dokumentų, pateiktų posėdžio, kuriame dalyvavo Komisijos, Britanijos valdžios institucijų ir *Confédération des Brasseurs du Marché Commun* (CBMC) atstovai, protokolo kopiją. Komisija sutiko atskleisti tam tikrus posėdžio dokumentus, tačiau išbraukė penkias protokole nurodytas pavardes (du asmenys aiškiai nesutiko, kad jų tapatybė būtų atskleista, o su kitais trimis asmenimis Komisijai nepavyko susisiekti). 2004 m. kovo 18 d. sprendimu Komisija atmetė naują *Bavarian Lager* prašymą pateikti išsamų posėdžio protokolą ir šiuo atveju ji visų pirma rėmėsi minėtų asmenų privataus gyvenimo apsauga, kurią garantuoja Duomenų apsaugos reglamentas. *Bavarian Lager* nebuvo patenkinta tokiu Komisijos atsakymu ir pareiškė ieškinį Pirmosios instancijos teisme, kuris 2007 m. lapkričio 8 d. sprendimu (byla T-194/04, *Bavarian Lager prieš Komisiją*) panaikino Komisijos sprendimą ir visų pirma nurodė, kad vien atitinkamų asmenų pavardžių įrašymas į atitinkamą asmenų, dalyvaujančių posėdyje ir atstovaujančių savo įstaigai, sąrašą nepažeidė privataus gyvenimo ir nekėlė jokio pavojaus šių asmenų privačiam gyvenimui.

Atsižvelgdamas į Komisijos skundą ESTT panaikino Pirmosios instancijos teismo sprendimą. ESTT nusprendė, kad Reglamente dėl galimybės susipažinti su dokumentais nustatyta „speciali sistema, kuria sustiprinama asmens, kurio duomenys tam tikrais atvejais gali būti atskleisti visuomenei, apsauga“. Pasak ESTT, kai pagal Reglamentą dėl galimybės susipažinti su dokumentais pateiktame prašyme prašoma leisti susipažinti su dokumentais, kuriuose pateikiami asmens duomenys, Duomenų apsaugos reglamento nuostatos taikomos visa apimtimi. Paskui ESTT padarė išvadą, kad Komisija teisingai atmetė prašymą

34 2010 m. birželio 29 d. ESTT sprendimo *Europos Komisija prieš The Bavarian Lager Co. Ltd.*, C-28/08 P, 60, 63, 76, 78 ir 79 punktai.

leisti susipažinti su išsamiu 1996 m. spalio mėn. vykusio posėdžio protokolu. Atsižvelgiant į tai, kad penki minėto posėdžio dalyviai nedavė sutikimo, Komisija, pateikdama prašomo dokumento versiją, kurioje buvo išbrauktos minėtų asmenų pavardės, tinkamai laikėsi jai nustatyto viešumo įsipareigojimo.

Be to, pasak ESTT, „kadangi *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 pagal Duomenų apsaugos reglamentą.

Pagal šį sprendimą teisės į duomenų apsaugą ribojimas, atsižvelgiant į galimybę susipažinti su dokumentais, turi būti pagrįstas konkrečia priežastimi. Teisė susipažinti su dokumentais negali automatiškai būti viršesnė už teisę į duomenų apsaugą[35].

Konkretus prašymo susipažinti su dokumentais aspektas buvo nagrinėjamas toliau nurodytoje EŽTT byloje.

Pavyzdys. Byloje *Társaság a Szabadságjogokért prieš Vengriją*[36] pareiškėjas (žmogaus teisių NVO) prašė, kad Konstitucinis Teismas leistų susipažinti su nagrinėjama byla. Nepasikonsultavęs su bylą iškėlusiu parlamento nariu, Konstitucinis Teismas atsisakė patenkinti prašymą ir motyvavo tuo, kad jis gali leisti susipažinti su jam pateiktais skundais tik pritarus skundo pateikėjui. Vidaus teismai palaikė šį atsisakymą motyvuodami tuo, kad tokių asmens duomenų apsauga negali būti ribojama vadovaujantis kitais teisėtais interesais, įskaitant galimybę visuomenei susipažinti su informacija. Pareiškėjas vykdė socialinio stebėtojo funkciją ir jo veikla buvo pagrįsta panašia apsauga, kuri suteikiama spaudai. Dėl spaudos laisvės EŽTT ne kartą nurodė, kad visuomenė turi teisę gauti su bendruoju interesu susijusią informaciją. Pareiškėjo prašoma informacija buvo „parengta ir baigta“ ir norint ją pateikti nereikėjo rinkti jokių duomenų. Tokiomis aplinkybėmis valstybė turėjo pareigą nesudaryti kliūčių informacijos

35 Tačiau žr. Europos duomenų apsaugos priežiūros pareigūno (EDAPP) išsamius argumentus (2011 m.), *Visuomenės galimybė susipažinti su dokumentais, kuriuose pateikiami asmens duomenys, priėmus sprendimą Bavarian Lager byloje*, Briuselis, 2011 m. kovo 24 d., galima rasti adresu www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/BackgroundP/11-03-24_Bavarian_Lager_EN.pdf.

36 2009 m. balandžio 14 d. EŽTT sprendimas *Társaság a Szabadságjogokért prieš Vengriją*, Nr. 37374/05; žr. 27, 36–38 punktus.

srautui, kuriuo norėjo pasinaudoti pareiškėjas. Apibendrindamas EŽTT nurodė, kad kliūtys, kurios trukdo gauti su viešuoju interesu susijusią informaciją, galėtų atgrasyti žiniasklaidoje arba panašiose srityse veikiančius subjektus nuo svarbios viešo stebėtojo funkcijos vykdymo. Teismas nusprendė, kad 10 straipsnis buvo pažeistas.

ES teisėje skaidrumui teikiama ypatinga svarba. Skaidrumo principas numatytas ES sutarties 1 ir 10 straipsniuose ir SESV 15 straipsnio 1 dalyje[37]. Reglamento (EB) Nr. 1049/2001 2 konstatuojamojoje dalyje nustatyta, kad skaidrumas leidžia piliečiams artimiau dalyvauti sprendimų priėmimo procese bei garantuoja didesnį valdymo teisėtumą ir veiksmingumą, aukštesnį atskaitomybės piliečiui mastą demokratinėje sistemoje[38].

Vadovaujantis šiais argumentais, Tarybos reglamente (EB) Nr. 1290/2005 dėl bendrosios žemės ūkio politikos finansavimo ir Komisijos reglamente (EB) Nr. 259/2008, kuriuo nustatomos išsamios minėto reglamento taikymo taisyklės, reikalaujama skelbti informaciją apie tam tikrų ES žemės ūkio sektoriaus fondų paramos gavėjus ir kiekvieno paramos gavėjo gaunamas lėšas[39]. Toks informacijos skelbimas turėtų padėti visuomenei kontroliuoti, kad administravimo institucijos tinkamai naudotų viešąsias lėšas. Kai kurie paramos gavėjai ginčijo tokio informacijos skelbimo proporcingumą.

Pavyzdys. Byloje *Volker ir Markus Schecke ir Hartmut Eifert prieš Land Hessen*[40] ESTT turėjo išspręsti ES teisės aktuose reikalaujamo informacijos, susijusios su ES žemės ūkio subsidijų gavėjų pavardėmis ir gautų subsidijų dydžiu, skelbimo proporcingumą.

Teismas, atkreipdamas dėmesį į tai, kad teisė į duomenų apsaugą nėra absoliuti, teigė, kad svetainėje viešai skelbiant duomenis, kuriais nurodomi dviejų ES

37 ES (2012 m.), Europos Sąjungos sutarties ir SESV suvestinės redakcijos, OL C 326, 2012.

38 2003 m. kovo 6 d. ESTT sprendimo *Interporc Im- und Export GmbH prieš Europos Bendrijų Komisiją*, C-41/00 P, 39 punktas ir 2010 m. birželio 29 d. ESTT sprendimo *Europos Komisija prieš The Bavarian Lager Co. Ltd.*, C-28/08 P, 54 punktas.

39 2005 m. birželio 21 d. Tarybos reglamentas (EB) Nr. 1290/2005 dėl bendrosios žemės ūkio politikos finansavimo, OL L 209, 2005; ir 2008 m. kovo 18 d. Komisijos reglamentas (EB) Nr. 259/2008, kuriuo nustatomos išsamios Tarybos reglamento (EB) Nr. 1290/2008 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.

40 2010 m. lapkričio 9 d. ESTT sprendimo *Volker ir Markus Schecke GbR (C-92/09) ir Hartmut Eifert (C-93/09) prieš Land Hessen*, sujungtos bylos C-92/09 ir C-93/09, 47–52, 58, 66–67, 75, 86 ir 92 punktai.

žemės ūkio pagalbos fondų paramos gavėjai ir tikslus jų gautos paramos dydis, iš esmės buvo ribojamos jų teisės į privatų gyvenimą, ypač jų asmens duomenų apsauga.

Teismas manė, kad toks Chartijos 7 ir 8 straipsnių ribojimas buvo numatytas įstatymu ir atitiko ES pripažįstamą viešąjį interesą, t. y. didinti Bendrijos lėšų naudojimo skaidrumą. Vis dėlto ESTT nusprendė, kad fizinių asmenų, kuriems iš šių dviejų fondų teikiama ES žemės ūkio pagalba, pavardžių ir tikslaus gautos paramos dydžio skelbimas buvo neproporcinga priemonė ir jos nebuvo galima pagrįsti Chartijos 52 straipsnio 1 dalimi. Todėl Teismas paskelbė, kad ES teisės aktas dėl informacijos, susijusios su Europos žemės ūkio fondo paramos gavėjais, skelbimo iš dalies negaliojo.

1.2.3. Menų ir mokslo laisvė

Kita teisė, kurios pusiausvyrą reikia nustatyti atsižvelgiant į teisę į privataus gyvenimo gerbimą ir duomenų apsaugą, yra menų ir mokslo laisvė, kurios apsauga aiškiai numatyta Chartijos 13 straipsnyje. Ši teisė visų pirma kildinama iš teisės į minties ir saviraiškos laisvę ir ji turi būti įgyvendinama atsižvelgiant į Chartijos 1 straipsnį (Žmogaus orumas). EŽTT nuomone, menų ir mokslo laisvės apsauga užtikrinama EŽTK 10 straipsnyje[41]. Chartijos 13 straipsnyje garantuojama teisė taip pat gali būti ribojama vadovaujantis EŽTK 10 straipsniu[42].

Pavyzdys. Byloje *Vereinigung bildender Künstler prieš Austriją*[43] Austrijos teismai uždraudė pareiškėjo asociacijai toliau eksponuoti piešinius, kuriuose įvairių viešų asmenų veidų nuotraukos buvo naudojamos intymias gyvenimo scenas vaizduojančiuose piešiniuose. Austrijos parlamento narys, kurio nuotrauka buvo panaudota piešinyje, iškėlė bylą pareiškėjo asociacijai ir siekė, kad piešinį būtų uždrausta eksponuoti. Vidaus teismas patenkino jo prašymą ir nustatė draudimą. EŽTT pakartojo, kad EŽTK 10 straipsnis buvo taikomas skleidžiant idėjas, kurios įžeidė, šokiravo arba sutrikdė valstybę arba bet kurią gyventojų grupę. Meno kūrinius sukūrę, atlikę, platinę arba eksponavę asmenys padėjo keistis idėjomis ir nuomonėmis ir valstybė turėjo pareigą nepagrįstai netrukdyti tokiems asmenims įgyvendinti savo saviraiškos laisvę. Atsižvelgdamas į tai,

41 1988 m. gegužės 24 d. EŽTT sprendimas *Müller ir kiti prieš Šveicariją*, Nr. 10737/84.

42 Pagrindinių teisių chartijos išaiškinimai, OL C 303, 2007 m.

43 2007 m. sausio 25 d. EŽTT sprendimas *Vereinigung bildender Künstler prieš Austriją*, Nr. 68345/01; visų pirma žr. 26 ir 34 punktus.

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. Teismas padarė išvadą, kad EŽTK 10 straipsnis buvo pažeistas.

Kalbant apie mokslą pažymėtina, kad Europos duomenų apsaugos teisėje suprantama ypatinga mokslo nauda visuomenei. Todėl bendri asmens duomenų naudojimo apribojimai yra švelnesni. Duomenų apsaugos direktyvoje ir Konvencijoje Nr. 108 leidžiama duomenis saugoti mokslinio tyrimo tikslais, kai jie nebetenkina pradinio tikslo, dėl kurio jie buvo surinkti. Be to, vėlesnis asmens duomenų naudojimas mokslinio tyrimo tikslais negali būti laikomas nesuderinamu naudojimu. Nacionalinės teisės aktų leidėjams pavesta parengti išsamesnes nuostatas, įskaitant būtinas apsaugos priemones, kad mokslinių tyrimų interesai būtų suderinti su teise į duomenų apsaugą (taip pat žr. 3.3.3 ir 8.4 dalis).

1.2.4. Nuosavybės apsauga

Teisė į nuosavybės apsaugą numatyta EŽTK Protokolo Nr. 1 1 straipsnyje ir Chartijos 17 straipsnio 1 dalyje. Svarbus teisės į nuosavybę aspektas yra intelektinės nuosavybės apsauga, apie kurią aiškiai užsimenama Chartijos 17 straipsnio 2 dalyje. ES teisinėje tvarkoje galima rasti keletą direktyvų, kuriomis siekiama užtikrinti veiksmingą intelektinės nuosavybės, ypač autorių teisių, apsaugą. Intelektinė nuosavybė apima ne tik literatūros ir meno kūrinius, bet ir patentą, prekių ženklą ir gretutines teises.

Iš ESTT praktikos aiškiai matyti, kad turi būti nustatoma pagrindinės teisės į nuosavybę apsaugos ir kitų pagrindinių teisių, visų pirma teisės į duomenų apsaugą, apsaugos pusiausvyra[44]. Išnagrinėtos kelios bylos, kuriose autorių teisių apsaugos institucijos reikalavo, kad interneto paslaugų teikėjai atskleistų internetinių dalijimosi failais platformų naudotojų tapatybę. Tokiose platformose interneto naudotojai gali

44 2013 m. sausio 10 d. EŽTT sprendimas *Ashby Donald ir kiti prieš Prancūziją*, Nr. 36769/08.

nemokamai atsisiųsti muzikos kūrinius, nepaisant to, kad jiems taikoma autorių teisių apsauga.

Pavyzdys. Byla *Promusicae prieš Telefónica de España*[45] buvo susijusi su Ispanijos interneto prieigos paslaugų teikėjo *Telefónica* atsisakymu atskleisti muzikos prodiuserių ir muzikos ir audiovizualinių įrašų leidėjų ne pelno organizacijai *Promusicae* tam tikrų asmenų, kuriems ji teikė interneto prieigos paslaugas, asmens duomenis. *Promusicae* siekė gauti informaciją, kad galėtų iškelti civilinę bylą prieš minėtus asmenis, kurie, kaip ji teigė, naudojo keitimosi failais programą ir galėjo gauti prieigą prie fonogramų, teisė kurias naudoti priklausė *Promusicae* nariams.

Ispanijos teismas kreipėsi į ESTT prašydamas priimti prejudicinį sprendimą ir klausė, ar tokie asmens duomenys pagal Bendrijos teisę turi būti suteikti siekiant iškelti civilinę bylą ir užtikrinti veiksmingą autorių teisių apsaugą. Ispanijos teismas rėmėsi direktyvomis 2000/31, 2001/29 ir 2004/48, kurios buvo aiškinamos atsižvelgiant į Chartijos 17 ir 47 straipsnius. Teismas padarė išvadą, kad šiose trijose direktyvose, taip pat E. privatumo direktyvoje (Direktyva 2002/58) nedraudžiama valstybei narei nustatyti pareigą atskleisti asmens duomenis siekiant iškelti civilinę bylą ir taip užtikrinti veiksmingą autorių teisių apsaugą.

Todėl ESTT nurodė, kad byloje keliamas klausimas dėl poreikio suderinti skirtingų pagrindinių teisių apsaugos reikalavimus, t. y. teisės į privataus gyvenimo gerbimą ir teisių į nuosavybės apsaugą ir veiksmingą teisių gynimą.

ESTT padarė išvadą, jog, „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“[46].

45 2008 m. sausio 29 d. ESTT sprendimo *Productores de Música de España (Promusicae) prieš Telefónica de España SAU*, C-275/06, 54 ir 60 punktai.

46 *Ibid.*, 65 ir 68 punktai; taip pat žr. 2012 m. vasario 16 d. ESTT sprendimą *SABAM prieš Netlog N.V.*, C-360/10.

2

Duomenų apsaugos terminija

ES	Aptariami klausimai	ET
Asmens duomenys		
Duomenų apsaugos direktyvos 2 straipsnio a punktas. 2008 m. lapkričio 9 d. ESTT sprendimas *Volker ir Markus Schecke GbR (C-92/09) ir Hartmut Eifert (C-93/09) prieš Land Hessen*, sujungtos bylos C-92/09 ir C-93/09. 2008 m. sausio 29 d. ESTT sprendimas *Productores de Música de España (Promusicae) prieš Telefónica de España SAU*, C-275/06.	**Teisinė apibrėžtis.**	Konvencijos Nr. 108 2 straipsnio a punktas. 2013 m. kovo 14 d. EŽTT sprendimas *Bernh Larsen Holding AS ir kiti prieš Norvegiją*, Nr. 24117/08.
Duomenų apsaugos direktyvos 8 straipsnio 1 dalis. 2003 m. lapkričio 6 d. ESTT sprendimas *Bodil Lindqvist*, C-101/01.	**Specialios asmens duomenų kategorijos (ypatingi duomenys).**	Konvencijos Nr. 108 6 straipsnis.
Duomenų apsaugos direktyvos 6 straipsnio 1 dalies e punktas.	**Anoniminiai ir pseudoniminiai duomenys.**	Konvencijos Nr. 108 5 straipsnio e punktas. Konvencijos Nr. 108 aiškinamojo rašto 42 dalis.
Duomenų tvarkymas		
Duomenų apsaugos direktyvos 2 straipsnio b punktas. 2003 m. lapkričio 6 d. ESTT sprendimas *Bodil Lindqvist*, C-101/01.	**Apibrėžtys.**	Konvencijos Nr. 108 2 straipsnio c punktas.

ES	Aptariami klausimai	ET
Duomenų naudotojai		
Duomenų apsaugos direktyvos 2 straipsnio d punktas.	**Duomenų valdytojas.**	Konvencijos Nr. 108 2 straipsnio d punktas. Rekomendacijos dėl profiliavimo 1 straipsnio g punktas*.
Duomenų apsaugos direktyvos 2 straipsnio e punktas. 2003 m. lapkričio 6 d. ESTT sprendimas *Bodil Lindqvist*, C-101/01.	**Duomenų tvarkytojas.**	Rekomendacijos dėl profiliavimo 1 straipsnio h punktas.
Duomenų apsaugos direktyvos 2 straipsnio g punktas.	**Duomenų gavėjas.**	Konvencijos Nr. 108 Papildomo protokolo 2 straipsnio 1 punktas.
Duomenų apsaugos direktyvos 2 straipsnio f punktas.	**Trečioji šalis.**	
Sutikimas		
Duomenų apsaugos direktyvos 2 straipsnio h punktas. 2011 m. gegužės 5 d. ESTT sprendimas *Deutsche Telekom AG prieš Bundesrepublik Deutschland*, C-543/09.	**Galiojančio sutikimo apibrėžtis ir reikalavimai.**	Rekomendacijos dėl medicininių duomenų 6 straipsnis ir įvairios vėlesnės rekomendacijos.

Pastaba. * *2010 m. lapkričio 23 d. Europos Tarybos Ministrų Komiteto (2010 m.) rekomendacija R(2010) 13 valstybėms narėms dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu, atsižvelgiant į profiliavimą (Rekomendacija dėl profiliavimo).*

2.1. Asmens duomenys

Pagrindiniai faktai

- Duomenys laikomi asmens duomenimis, jeigu jie susiję su asmeniu, kurio tapatybė nustatyta arba ją bent jau galima nustatyti (toks asmuo vadinamas duomenų subjektu).
- Asmens tapatybę galima nustatyti, jeigu pernelyg nesistengiant galima gauti papildomą informaciją, kuri leidžia nustatyti 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, vadinamų ypatingais duomenimis, kurių sąrašas pateikiamas Konvencijoje Nr. 108 ir Duomenų apsaugos direktyvoje ir kuriems reikalinga didesnė apsauga, todėl šiems duomenims taikomas specialus teisinis režimas.
- Duomenys yra anoniminiai, jeigu juose nėra jokių žymenų tapatybei nustatyti; duomenys pseudoniminiai, jeigu žymenys tapatybei nustatyti yra užšifruojami.
- Skirtingai nei anoniminiai duomenys, pseudoniminiai duomenys laikomi asmens duomenimis.

2.1.1. Pagrindiniai asmens duomenų sąvokos aspektai

ES teisėje ir **ET teisėje** „asmens duomenys“ apibrėžiami kaip informacija, susijusi su fiziniu asmeniu, kurio tapatybė yra nustatyta arba kurio tapatybę galima nustatyti[47], t. y. informacija apie asmenį, kurio tapatybė yra neabejotinai aiški arba ją bent jau galima nustatyti gavus papildomos informacijos.

Asmuo, kurio duomenys tvarkomi, yra vadinamas duomenų subjektu.

Asmuo

Teisė į duomenų apsaugą atsirado iš teisės į privataus gyvenimo gerbimą. Privataus gyvenimo sąvoka yra susijusi su žmonėmis. Todėl duomenų apsauga visų pirma naudojasi fiziniai asmenys. Be to, remiantis 29 straipsnio duomenų apsaugos darbo grupės nuomone, Europos duomenų apsaugos teisės suteikiama apsauga gali naudotis tik *gyvi asmenys*[48].

EŽTT jurisprudencija, susijusi su EŽTK 8 straipsniu, rodo, kad kartais gali būti sudėtinga visiškai atskirti privataus ir profesinio gyvenimo sritis[49].

Pavyzdys. Byloje *Amann prieš Šveicariją*[50] valdžios institucijos slapta klausėsi pareiškėjo pokalbio telefonu verslo klausimais. Remdamosi šio pokalbio

47 Duomenų apsaugos direktyvos 2 straipsnio a punktas; Konvencijos Nr. 108 2 straipsnio a punktas.

48 29 straipsnio duomenų apsaugos darbo grupė (2007 m.), 2007 m. birželio 20 d. *Nuomonės dėl asmens duomenų apsaugos sąvokos*, WP 136, p. 22.

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

50 2000 m. vasario 16 d. EŽTT sprendimo *Amann prieš Šveicariją* (DK), Nr. 27798/95, 65 punktas.

duomenimis, valdžios institucijos atliko tyrimą dėl pareiškėjo ir į nacionalinio saugumo kartoteką įtraukė su pareiškėju susijusią bylos medžiagą. Nors slaptas klausymasis buvo susijęs su pokalbiu telefonu verslo klausimais, EŽTT laikėsi nuomonės, kad saugomi šio pokalbio duomenys buvo susiję su pareiškėjo privačiu gyvenimu. EŽTT nurodė, kad sąvoka „privatus gyvenimas" neturi būti aiškinama siauriai, visų pirma atsižvelgiant į tai, kad privataus gyvenimo gerbimas apima teisę užmegzti ir plėtoti santykius su kitais žmonėmis. Be to, nebuvo jokios pagrįstos priežasties į sąvoką „privatus gyvenimas" neįtraukti su profesiniu gyvenimu arba verslu susijusios veiklos. Toks platus aiškinimas buvo susijęs su Konvencija Nr. 108. EŽTT taip pat nustatė, kad slaptas pokalbio klausymasis pareiškėjo byloje neatitiko įstatymų, kadangi vidaus teisėje nebuvo numatyta konkrečių ir išsamių nuostatų dėl informacijos rinkimo, įrašymo ir saugojimo. Todėl EŽTT padarė išvadą, kad EŽTK 8 straipsnis buvo pažeistas.

Be to, jeigu duomenų apsauga taip pat gali būti taikoma profesinio gyvenimo klausimams, atrodo, būtų galima abejoti tuo, kad apsauga turėtų būti suteikiama tik fiziniams asmenims. EŽTK numatytos teisės garantuojamos ne tik fiziniams, bet ir visiems asmenims.

EŽTT jurisprudencijoje priimtas sprendimas dėl juridinių asmenų, kurie teigia, kad buvo pažeista jų teisė į jų duomenų naudojimo apsaugą pagal EŽTK 8 straipsnį, prašymų. Vis dėlto EŽTT bylą nagrinėjo atsižvelgdamas į teisę į būsto neliečiamybę ir susirašinėjimo slaptumą, o ne į teisę į privatų gyvenimą.

Pavyzdys. Byloje *Bernh Larsen Holding AS ir kiti prieš Norvegiją*[51] buvo nagrinėjamas trijų Norvegijos įmonių skundas dėl mokesčių institucijos sprendimo, kuriuo jos buvo įpareigotos pateikti mokesčių auditoriams visų trijų įmonių bendrai naudojamame kompiuterio serveryje esančių duomenų kopiją.

EŽTT nustatė, kad toks įpareigojimas pareiškėjoms įmonėms reiškė jų teisių į būsto neliečiamybę ir susirašinėjimo slaptumą pagal EŽTK 8 straipsnį ribojimą. Vis dėlto Teismas nustatė, kad mokesčių institucijose buvo taikomos veiksmingos ir tinkamos apsaugos nuo piktnaudžiavimo priemonės: įmonės pareiškėjos buvo iš anksto tinkamai informuotos; jų atstovai dalyvavo mokesčių institucijoms atliekant patikrą vietoje ir galėjo teikti paaiškinimus, o medžiaga turėjo

51 2013 m. kovo 14 d. EŽTT sprendimas *Bernh Larsen Holding AS ir kiti prieš Norvegiją*, Nr. 24117/08. Tačiau taip pat žr. 2008 m. liepos 1 d. EŽTT sprendimą *Liberty ir kiti prieš Jungtinę Karalystę*, Nr. 58243/00.

būti sunaikinta iš karto, vos tik baigus mokestinį patikrinimą. Tokiomis aplinkybėmis reikėjo nustatyti tinkamą, viena vertus, įmonių pareiškėjų teisės į būsto neliečiamybės ir susirašinėjimo slaptumą gerbimo ir jų intereso užtikrinti jose dirbančių asmenų privatumą, ir, kita vertus, viešojo intereso užtikrinti veiksmingą mokestinį patikrinimą pusiausvyrą. Todėl Teismas nustatė, kad 8 straipsnis nebuvo pažeistas.

Pagal Konvenciją Nr. 108 duomenų apsauga visų pirma taikoma fiziniams asmenims; tačiau susitariančiosios šalys savo vidaus teisėje į duomenų apsaugos taikymo sritį gali įtraukti ir juridinius asmenis, pvz., įmones ir asociacijas. **ES duomenų apsaugos teisė** iš esmės nėra taikoma juridiniams asmenims atsižvelgiant į su jais susijusių duomenų tvarkymą. Nacionalinės reguliavimo institucijos, reglamentuodamos šį klausimą, yra visiškai laisvos[52].

Pavyzdys. Byloje *Volker ir Markus Schecke ir Hartmut Eifert prieš Land Hessen*[53] ESTT, atsižvelgdamas į su žemės ūkio pagalbos paramos gavėjais susijusių asmens duomenų skelbimą, nurodė, 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. <...> Teisė į privataus gyvenimo gerbimą tvarkant asmens duomenis siejama su visa informacija apie fizinį asmenį, kurio tapatybė nustatyta arba gali būti nustatyta <...>“[54].

Asmens tapatybės nustatymas

Pagal ES teisę ir **ET teisę** informacijoje pateikiami duomenys apie asmenį, jeigu:

- remiantis šia informacija nustatoma asmens tapatybė arba
- jeigu asmuo, kol jo tapatybė dar nenustatyta, aprašomas šioje informacijoje taip, kad atlikus papildomą paiešką galima išsiaiškinti duomenų subjekto tapatybę.

Europos duomenų apsaugos teisėje užtikrinama abiejų rūšių informacijos apsauga. EŽTT ne kartą nurodė, kad EŽTK vartojama asmens duomenų sąvoka yra tokia pati

52 Duomenų apsaugos direktyvos 24 konstatuojamoji dalis.

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

54 *Ibid.*, 52 punktas.

kaip ir Konvencijoje Nr. 108, visų pirma atsižvelgiant į asmens duomenų susiejimo su asmenimis, kurių tapatybė yra nustatyta arba gali būti nustatyta, sąlygą[55].

Teisinėse apibrėžtyse, susijusiose su asmens duomenimis, išsamiau nepaaiškinama, kada asmens tapatybė laikoma nustatyta[56]. Akivaizdu, kad tapatybei nustatyti reikalingi elementai, kuriuose asmuo aprašomas taip, kad jį galima atskirti nuo visų kitų asmenų ir atpažinti kaip konkretų asmenį. Asmens vardas ir pavardė yra pagrindinis tokio aprašymo elemento pavyzdys. Pavyzdžiui, kartais pakanka nurodyti viešų asmenų asmens pareigas, pvz., Europos Komisijos pirmininkas.

Pavyzdys. Byloje *Promusicae*[57] ESTT nurodė, jog „nebuvo ginčyta, kad *Promusicae* prašomas tam tikrų (internetinių dalijimosi failais platformų) 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 2 straipsnio a punkte pateikiamame apibrėžime, prieinamus <...>. Toks duomenų, kuriuos, *Promusicae* teigimu, saugo *Telefónica*, o to ši neginčija, pateikimas yra asmens duomenų tvarkymas Direktyvos 2002/58 2 straipsnio pirmosios pastraipos, skaitomos kartu su Direktyvos 95/46 2straipsnio b punktu, prasme“.

Kadangi dauguma vardų ir pavardžių nėra unikalūs, nustatant asmens tapatybę gali prireikti papildomų žymenų, kurie padėtų nesupainioti asmens su kuriuo nors kitu asmeniu. Dažnai naudojama gimimo data ir vieta. Be to, kai kuriose šalyse, siekiant patikimiau identifikuoti piliečius, jiems priskiriami individualūs numeriai. Biometriniai duomenys, pvz., pirštų atspaudai, skaitmeninės nuotraukos arba duomenys apie akies rainelės atvaizdą, šiame technologijų amžiuje vis dažniau naudojami asmenų tapatybei nustatyti.

Tačiau tam, kad būtų taikoma Europos duomenų apsaugos teisė, aukštos kokybės duomenų subjekto tapatybės nustatymas nėra būtinas; pakanka to, kad atitinkamo asmens tapatybę galima nustatyti. Tariama, kad asmens tapatybę galima nustatyti, jeigu informacijoje yra su tapatybe susijusių duomenų, kuriais remiantis tiesiogiai

55 Žr. 2000 m. vasario 16 d. EŽTT sprendimo *Amann prieš Šveicariją* (DK), Nr. 27798/95, 65 ir kt. punktus.

56 Taip pat žr. 2003 m. vasario 13 d. EŽTT sprendimą *Odièvre prieš Prancūziją* (DK), Nr. 42326/98, ir 2012 m. rugsėjo 25 d. EŽTT sprendimą *Godelli prieš Italiją*, Nr. 33783/09.

57 2008 m. sausio 29 d. ESTT sprendimo *Productores de Música de España (Promusicae) prieš Telefónica de España SAU*, C-275/06, 45 punktas.

arba netiesiogiai galima nustatyti asmens tapatybę[58]. Duomenų apsaugos direktyvos 26 konstatuojamojoje dalyje nustatyta, kad orientuojamasi atsižvelgiant į tai, ar bus galima pasinaudoti pagrįstomis tapatybės nustatymo priemonėmis ir ar tokias priemones naudos numatomi duomenų naudotojai; tai apima trečiąsias šalis duomenų gavėjas (žr. 2.3.2 dalį).

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

Šie argumentai neatitinka Duomenų apsaugos direktyvos 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 valdžios institucijos negali tiesiogiai pasinaudoti tapatybės nustatymo priemonėmis, jos pateiks duomenis kitai kompetentingai institucijai (policijai), kuri tokiomis priemonėmis gali pasinaudoti. 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 valdžios institucijos veiksmai prilygsta duomenų apie asmenis, kurių tapatybę galima nustatyti, rinkimui, todėl pagal duomenų apsaugos teisę tokiam rinkimui būtinas teisinis pagrindas.

ET teisėje galimybė nustatyti tapatybę suprantama panašiai. Pavyzdžiui, Rekomendacijos dėl asmens duomenų, naudojamų apmokėjimui, 1 straipsnio 2 dalyje[59] nustatyta, kad asmuo negali būti traktuojamas kaip „nustatomos tapatybės“, jeigu tapatybės nustatymui reikia nepagrįstai daug laiko, išlaidų ir pastangų.

58 Duomenų apsaugos direktyvos 2 straipsnio a punktas.

59 ET Ministrų Komitetas (1990 m.), 1990 m. rugsėjo 13 d. Rekomendacija Nr. R (90) 19 dėl asmens duomenų, naudojamų apmokėjimui arba kitoms su tuo susijusioms operacijoms, apsaugos.

Tapatumo nustatymas

Tai yra procedūra, per kurią asmuo gali įrodyti, kad turi tam tikrą tapatybę ir (arba) yra įgaliotas atlikti tam tikrus veiksmus, pvz., įeiti į saugomą zoną arba pasiimti pinigų iš banko sąskaitos. Tapatumą galima nustatyti palyginant biometrinius duomenis, pvz., pase esančią nuotrauką arba pirštų atspaudus, su atitinkamo asmens, pvz., esančio imigracijos kontrolės institucijoje, duomenimis; arba paprašius pateikti informaciją, kurią turėtų žinoti tik tam tikros tapatybės arba atitinkamus įgaliojimus turintis asmuo, pvz., 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, pvz., specialią lustinę kortelę arba banko seifo raktą. Be slaptažodžių ir lustinių kortelių, kartais PIN ir elektroniniai parašai yra ypač patikimos priemonės elektroniniais ryšiais besinaudojančių asmenų tapatybei arba tapatumui nustatyti.

Duomenų pobūdis

Asmens duomenimis gali būti laikoma bet kokios rūšies informacija, jeigu ji yra susijusi su asmeniu.

> Pavyzdys. Darbuotojo asmeninėje byloje saugomas darbuotojo darbo rezultatų vertinimas, kurį atliko priežiūros darbuotojas, yra darbuotojo asmens duomenys, net jeigu šiame vertinime iš dalies arba visiškai atsispindi priežiūros darbuotojo nuomonė, pvz., teiginys, kad „darbuotojas nėra atsidavęs savo darbui“, o ne konkretūs faktai, pvz., „per pastaruosius šešis mėnesius darbuotojas nedirbo penkias savaites“.

Asmens duomenys apima informaciją, susijusią su asmens privačiu gyvenimu, taip pat informaciją apie jo profesinį arba viešą gyvenimą.

Amann byloje[60] EŽTT išaiškino, kad sąvoka „asmens duomenys“ nėra susijusi tik su asmens privataus gyvenimo sritimi (žr. 2.1.1 dalį). Ši sąvokos „asmens duomenys“ reikšmė atsižvelgiant į Duomenų apsaugos direktyvą taip pat yra svarbi.

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

Pavyzdys. Byloje *Volker ir Markus Schecke ir Hartmut Eifert prieš Land Hessen*[61] ESTT nurodė, jog „šiam vertinimui nėra svarbu tai, kad skelbiami duomenys susiję su profesine veikla <...>. Šiuo klausimu Europos Žmogaus Teisių Teismas, aiškindamas EŽTK 8 straipsnį, yra nusprendęs, kad terminas „privatus gyvenimas“ neturi būti aiškinamas siaurai ir kad jokia svarbi priežastis neleidžia pašalinti profesinės veiklos <...> iš „privataus gyvenimo“ sąvokos apimties“.

Duomenys taip pat yra susiję su asmenimis, jeigu informacijos turinyje netiesiogiai atsispindi asmens duomenys. Tam tikrais atvejais, kai tarp objekto arba įvykio, – pvz., mobiliojo telefono, automobilio, nelaimingo atsitikimo, – ir asmens, – pvz., mobiliojo telefono savininko, automobilio vairuotojo, nelaimingo atsitikimo aukos, – yra glaudus ryšys, informacija apie objektą arba įvykį taip pat turi būti laikoma asmens duomenimis.

Pavyzdys. Byloje *Uzun prieš Vokietiją*[62] pareiškėjas ir kitas vyras buvo stebimi naudojant globalinės padėties nustatymo sistemos (GPS) prietaisą, kuris buvo pritvirtintas kito vyro automobilyje, dėl to, kad jie buvo įtariami dalyvavę atliekant sprogdinimus. Šioje byloje EŽTT nusprendė, kad pareiškėjo stebėjimas naudojant GPS reiškė kišimąsi į jo privatų gyvenimą, kurio apsauga užtikrinama EŽTK 8 straipsnyje. Vis dėlto stebėjimas naudojant GPS atitiko įstatymą ir buvo proporcingas siekiant ištirti keletą kaltinimų pasikėsinimu nužudyti. Todėl toks stebėjimas demokratinėje visuomenėje buvo būtinas. Teismas nusprendė, kad EŽTK 8 straipsnis nebuvo pažeistas.

Duomenų pateikimo forma

Asmens duomenų saugojimo arba naudojimo forma nėra svarbus aspektas taikant asmens duomenų apsaugos teisę. Asmens duomenys gali būti pateikiami rašytiniuose arba žodiniuose pranešimuose, taip pat atvaizduose[63], įskaitant apsauginės

61 2010 m. lapkričio 9 d. ESTT sprendimo *Volker ir Markus Schecke GbR ir Hartmut Eifert prieš Land Hessen*, sujungtos bylos C-92/09 ir C-93/09, 59 punktas.

62 2010 m. rugsėjo 2 d. EŽTT sprendimas *Uzun prieš Vokietiją*, Nr. 35623/05.

63 2004 m. birželio 24 d. EŽTT sprendimas *Von Hannover prieš Vokietiją*, Nr. 59320/00; 2005 m. sausio 11 d. EŽTT sprendimas *Sciacca prieš Italiją*, Nr. 50774/99.

vaizdo stebėjimo sistemos (AVSS) įrašus[64], arba garso medžiagoje[65]. Asmens duomenys taip pat gali būti pateikiami elektroninėje arba popierinėje informacijoje; net žmogaus audinio ląstelių mėginiuose gali būti asmens duomenų, nes juose yra informacija apie asmens DNR.

2.1.2. Specialios asmens duomenų kategorijos

ES teisėje ir **ET teisėje** yra specialių kategorijų asmens duomenų, kuriuos, atsižvelgiant į jų pobūdį, tvarkant gali kilti pavojus duomenų subjektams, tad tokiems duomenims reikalinga didesnė apsauga. Todėl tokių specialių kategorijų duomenis (ypatingus duomenis) turi būti leidžiama tvarkyti tik taikant konkrečias apsaugos priemones.

Kalbant apie ypatingų duomenų sąvoką pažymėtina, kad Konvencijoje Nr. 108 (6 straipsnis) ir Duomenų apsaugos direktyvoje (8 straipsnis) nurodomos tokios duomenų kategorijos:

- asmens duomenys, kurie atskleidžia rasinę arba etninę kilmę;
- asmens duomenys, kurie atskleidžia politines, religines arba kitokias pažiūras, ir
- asmens duomenys apie sveikatą arba intymų gyvenimą.

> Pavyzdys. Byloje *Bodil Lindqvist*[66] ESTT nurodė, jog „aplinkybės, kad asmuo susižeidė koją ir yra dalinėse laikinojo nedarbingumo atostogose, paminėjimas yra asmens duomenys apie sveikatą Direktyvos 95/46 8 straipsnio 1 dalies prasme“.

Duomenų apsaugos direktyvoje prie ypatingų duomenų taip pat priskiriamas „priklausymas profesinėms sąjungoms“, nes remiantis šia informacija gali būti vienareikšmiškai atskleidžiamos politinės pažiūros arba priklausymas politinei partijai.

64 2003 m. sausio 28 d. EŽTT sprendimas *Peck prieš Jungtinę Karalystę*, Nr. 44647/98; 2010 m. spalio 5 d. EŽTT sprendimas *Köpke prieš Vokietiją*, Nr. 420/07.

65 Duomenų apsaugos direktyvos 16 ir 17 konstatuojamosios dalys; 2001 m. rugsėjo 25 d. EŽTT sprendimo *P. G. ir J. H. prieš Jungtinę Karalystę*, Nr. 44787/98, 59 ir 60 punktai; 2005 m. gruodžio 20 d. EŽTT sprendimas *Wisse prieš Prancūziją*, Nr. 71611/01.

66 2003 m. lapkričio 6 d. ESTT sprendimo *Bodil Lindqvist*, C-101/01, 51 punktas.

Konvencijoje Nr. 108 prie ypatingų duomenų taip pat priskiriami su teistumu susiję asmens duomenys.

Duomenų apsaugos direktyvos 8 straipsnio 7 dalyje ES valstybėms narėms pavedama „apibrėžti sąlygas, kuriomis gali būti tvarkomas nacionalinis asmens identifikavimo kodas ar bet kuris kitas bendrojo taikymo žymuo tapatybei nustatyti“.

2.1.3. Anoniminiai ir pseudoniminiai duomenys

Vadovaujantis Duomenų apsaugos direktyvoje ir Konvencijoje Nr. 108 numatytu riboto duomenų saugojimo principu (kuris išsamiau aptariamas 3 skyriuje), duomenys turi būti laikomi „tokio pavidalo, kad duomenų subjektų tapatybes būtų galima nustatyti ne ilgiau, nei tai yra reikalinga tais tikslais, dėl kurių duomenys buvo surinkti arba po to tvarkomi“[67]. Todėl duomenys turi būti anonimizuojami, jeigu duomenų valdytojas nori juos saugoti pasibaigus jų saugojimo terminui arba kai tokie duomenys nebeatitinka pradinio tikslo, dėl kurio jie buvo surinkti.

Anoniminiai duomenys

Duomenys yra anoniminiai, jeigu visi padedantys nustatyti tapatybę elementai yra pašalinami iš asmens duomenų rinkinio. Informacijoje negali likti jokių elementų, kuriais remiantis ir imantis pagrįstų priemonių būtų galima iš naujo nustatyti susijusio (-ių) asmens (-ų) tapatybę (-es)[68]. Sėkmingai anonimizuoti duomenys nebelaikomi asmens duomenimis.

Jeigu asmens duomenys nebeatitinka pradinio tikslo, dėl kurio buvo surinkti, tačiau yra laikomi personalizuota forma istorinio, statistinio arba mokslinio naudojimo tikslais, Duomenų apsaugos direktyvoje ir Konvencijoje Nr. 108 toks laikymas yra leidžiamas, jeigu taikomos tinkamos apsaugos priemonės, padedančios apsisaugoti nuo netinkamo tokių duomenų naudojimo[69].

67 Duomenų apsaugos direktyvos 6 straipsnio 1 dalies e punktas; Konvencijos Nr. 108 5 straipsnio e punktas.

68 *Ibid.*, 26 konstatuojamoji dalis.

69 *Ibid.*, 6 straipsnio 1 dalies e punktas; Konvencijos Nr. 108 5 straipsnio e punktas.

Pseudoniminiai duomenys

Asmeninę informaciją sudaro žymenys tapatybei nustatyti, pvz., vardas, pavardė, gimimo data, lytis ir adresas. Pseudonimizavus asmeninę informaciją, žymenys tapatybei nustatyti pakeičiami vienu pseudonimu. Duomenų pseudonimizavimas atliekamas, pvz., užšifruojant su asmens duomenimis susijusius žymenis tapatybei nustatyti.

Konvencijoje Nr. 108 ar Duomenų apsaugos direktyvoje nėra aiškiai užsimenama apie pseudoniminius duomenis. Tačiau Konvencijos Nr. 108 aiškinamojo rašto 42 punkte nurodyta, kad „reikalavimas <...>, susijęs su duomenų, kurie yra susieti su vardu ir pavarde, saugojimo terminais, nereiškia, kad duomenys po kurio laiko turi būti negrįžtamai atskirti nuo asmens, su kuriuo jie yra susiję, vardo ir pavardės, tačiau turėtų būti neįmanoma susieti esamų duomenų su žymenimis tapatybei nustatyti“. Šį tikslą galima pasiekti duomenis pseudonimizuojant. Iššifravimo rakto neturintiems asmenims pseudoniminiai duomenys būtų sunkiai identifikuojami. Ryšys su tapatybe vis dar yra ir jį galima atkurti pseudonimus atkoduojant iššifravimo raktu. Iššifravimo raktą turintys asmenys gali lengvai atkurti tapatybės duomenis. Ypač reikėtų saugotis, kad iššifravimo raktų nenaudotų neįgalioti asmenys.

Duomenų pseudonimizavimas yra viena svarbiausių priemonių, naudojamų dideliam kiekiui duomenų apsaugoti, kai neįmanoma visiškai atsisakyti duomenų naudojimo. Tokios priemonės logiką ir poveikį reikia paaiškinti išsamiau.

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

„Č. S. 1967 m. yra keturių vaikų (dviejų berniukų ir dviejų mergaičių) tėvas“ arba

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

„YESz320l yra keturių vaikų (dviejų berniukų ir dviejų mergaičių) tėvas“.

Šių pseudoniminių duomenų naudotojai paprastai negalės nustatyti fakto „Čarlzas Spenseris, gimęs 1967 m. balandžio 3 d.“, jei jie matys tik kodus „324“ arba „YESz320l“. Todėl pseudoniminiai duomenys yra geriau apsaugoti nuo netinkamo jų panaudojimo.

Vis dėlto pirmasis pavyzdys nėra itin saugus. Jeigu sakinys „Č. S. 1967 m. yra keturių vaikų (dviejų berniukų ir dviejų mergaičių) tėvas“ bus naudojamas mažame kaimelyje, kuriame gyvena Čarlzas Spenseris, jį būtų galima lengvai atpažinti. Nuo duomenų pseudonimizavimo būdo priklauso duomenų apsaugos veiksmingumas.

Asmens duomenys, kurių žymenys tapatybei nustatyti yra užšifruoti, naudojami įvairiomis aplinkybėmis, siekiant užtikrinti asmenų tapatybės slaptumą. Tai ypač naudinga tuomet, 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, pvz., tuo atveju, kai tyrėjas tiria pacientų, kurių tapatybė žinoma tik ligoninės personalui, o ligoninė tyrėjui pateikė pseudonimines ligų istorijas, ligos eigą. Todėl duomenų pseudonimizavimas yra svarbi priemonė, susijusi su didesnę privatumo apsaugą padedančia užtikrinti technologija. Ji gali būti naudojama kaip svarbus elementas įgyvendinant pritaikytąją privatumo apsaugą. Tai reiškia duomenų apsaugos integravimą kuriant pažangias duomenų tvarkymo sistemas.

2.2. Duomenų tvarkymas

Pagrindiniai faktai

- Sąvoka „tvarkymas“ visų pirma reiškia automatinį tvarkymą.
- ES teisėje „tvarkymas“ taip pat reiškia rankinį tvarkymą susistemintose rinkmenose.
- Pagal ET teisę vidaus įstatymuose gali būti numatyta, kad „tvarkymas“ apima ir rankinį tvarkymą.

Konvencijoje Nr. 108 ir Duomenų apsaugos direktyvoje reglamentuojant duomenų apsaugą daugiausia dėmesio skiriama automatiniam duomenų tvarkymui.

Tačiau **ET teisėje** pateikiamoje automatinio tvarkymo sąvokos apibrėžtyje pripažįstama, kad atliekant automatizuoto tvarkymo operacijas gali prireikti asmens duomenis tvarkyti rankiniu būdu. Panašiai **ES teisėje** automatizuotas duomenų tvarkymas apibrėžiamas kaip „operacijos, kurias naudojant asmens duomenys visiškai arba iš dalies tvarkomi automatiniais būdais“[70].

70 Konvencijos Nr. 108 2 straipsnio c punktas ir Duomenų apsaugos direktyvos 2 straipsnio b punktas ir 3 straipsnio 1 dalis.

Pavyzdys. Byloje *Bodil Lindqvist*[71] ESTT nusprendė, kad

„operacijos, kai interneto puslapyje minimi įvairūs asmenys, kurių tapatybė atskleidžiama nurodant pavardę arba kitus duomenis, pavyzdžiui, telefono numerį ar su darbo sąlygomis ar pomėgiais susijusią informaciją, yra atliktos „visiškai ar iš dalies automatiniais būdais tvarkant asmens duomenis“ Direktyvos 95/46/EB 3 straipsnio 1 dalies prasme“.

Rankiniam duomenų tvarkymui taip pat turi būti taikomi duomenų apsaugos reikalavimai.

ES teisėje nustatyta duomenų apsauga jokiais būdais nėra taikoma tik automatiniam duomenų tvarkymui. Todėl pagal ES teisę duomenų apsauga taikoma tvarkant asmens duomenis rankinėje susistemintoje rinkmenoje, t. y. specialią struktūrą turinčioje popierinėje rinkmenoje[72]. Ši platesnė duomenų apsaugos taikymo sritis yra nustatyta dėl to, kad:

- popierines rinkmenas galima sugrupuoti taip, kad būtų galima greitai ir lengvai rasti informaciją, ir

- tam tikrą struktūrą turinčiose popierinėse rinkmenose saugant asmens duomenis galima lengvai apeiti automatiniam duomenų tvarkymui taikomus įstatymų nustatytus apribojimus[73].

Pagal ET teisę Konvencijoje Nr. 108 visų pirma reglamentuojamas duomenų tvarkymas naudojant automatizuotas duomenų rinkmenas[74]. Tačiau joje taip pat numatyta, kad vidaus teisėje apsaugą galima taikyti ir rankiniam duomenų tvarkymui. Nemažai Konvencijos Nr. 108 susitariančiųjų šalių pasinaudojo šia galimybe ir apie tai pranešė ET generaliniam sekretoriui[75]. Platesnė duomenų apsauga, kuri nustatoma pateikiant tokį pareiškimą, turi būti susijusi su visais rankinio duomenų tvarkymo būdais, o ne apsiriboti tik duomenų tvarkymu rankinėse susistemintose rinkmenose[76].

71 2003 m lapkričio 6 d. ESTT sprendimo *Bodil Lindqvist*, C-101/01, 27 punktas.

72 Duomenų apsaugos direktyvos 3 straipsnio 1 dalis.

73 *Ibid.*, 27 konstatuojamoji dalis.

74 Konvencijos Nr. 108 2 straipsnio b punktas.

75 Žr. pareiškimus, pateiktus pagal Konvencijos Nr. 108 3 straipsnio 2 dalies c punktą.

76 Žr. Konvencijos Nr. 108 3 straipsnio 2 dalies formuluotę.

Kalbant apie numatytų duomenų tvarkymo operacijų pobūdį pažymėtina, kad duomenų tvarkymo sąvoka yra išsamiai nustatyta **tiek ES, tiek ET teisėje**: „asmens duomenų tvarkymas <...> reiškia bet kurią tvarkymo operaciją <...> su asmens duomenimis, kaip antai: rinkimas, užrašymas, rūšiavimas, saugojimas, adaptavimas ar keitimas, atgaminimas, paieška, naudojimas, atskleidimas teikiant, platinant ar kitu būdu padarant juos prieinamus, išdėstymas reikiama tvarka ar sujungimas derinant, blokavimas, trynimas ar naikinimas“[77]. Sąvoka „duomenų tvarkymas“ taip pat apima veiksmus, kuriais vienas duomenų valdytojas atsakomybę už duomenis perduoda kitam duomenų valdytojui.

Pavyzdys. Darbdaviai renka ir tvarko duomenis apie savo darbuotojus, įskaitant informaciją, susijusią su jų darbo užmokesčiu. Teisinis pagrindas teisėtai rinkti ir tvarkyti tokius duomenis yra numatytas darbo sutartyje.

Darbdaviai duomenis apie savo darbuotojų darbo užmokestį turės pateikti mokesčių institucijoms. Toks duomenų perdavimas taip pat reikš „duomenų tvarkymą“ atsižvelgiant į šios sąvokos reikšmę pagal Konvenciją Nr. 108 ir Duomenų apsaugos direktyvą. Vis dėlto tokio duomenų atskleidimo teisinis pagrindas nėra darbo sutartis. Duomenų tvarkymo operacijos, kurias atlikdamas darbdavys teikia mokesčių institucijoms duomenis apie darbo užmokestį, turi būti pagrįstos papildomu teisiniu pagrindu. Šis teisinis pagrindas paprastai būna numatytas nacionalinių mokesčių įstatymų nuostatose. Duomenų teikimas reikštų neteisėtą jų tvarkymą, jeigu įstatymuose nebūtų numatytos tokios nuostatos.

2.3. Asmens duomenų naudotojai

Pagrindiniai faktai

- Pagal duomenų apsaugos teisę bet kuris asmuo, nusprendęs tvarkyti kitų asmenų asmens duomenis, laikomas duomenų valdytoju; jei sprendimą tvarkyti duomenis keli asmenys priima kartu, jie gali būti vadinami bendrais duomenų valdytojais.
- Duomenų tvarkytojas yra atskiras subjektas, kuris asmens duomenis tvarko duomenų valdytojo vardu.

77 Duomenų apsaugos direktyvos 2 straipsnio b punktas. Taip pat žr. Konvencijos Nr. 108 2 straipsnio c punktą.

- Duomenų tvarkytojas tampa duomenų valdytoju, kai jis pradeda duomenis naudoti savais tikslais ir nesivadovauja duomenų valdytojo nurodymais.
- Bet kuris asmuo, kuris gauna duomenis iš duomenų valdytojo, yra duomenų gavėjas.
- Trečioji šalis – tai fizinis arba juridinis asmuo, kuris nesivadovauja duomenų valdytojo nurodymais (todėl nėra duomenų subjektas).
- Trečioji šalis duomenų gavėja – tai fizinis arba juridinis asmuo, kuris yra teisiškai nepriklausomas nuo duomenų valdytojo, tačiau iš jo gauna asmens duomenis.

2.3.1. Duomenų valdytojai ir duomenų tvarkytojai

Pagrindinė duomenų valdytojo arba duomenų tvarkytojo statuso pasekmė yra susijusi su teisine atsakomybe laikytis atitinkamų duomenų apsaugos teisėje nustatytų pareigų. Todėl šį statusą gali įgyti tik tie subjektai, kuriuos pagal taikytiną teisę galima laikyti atsakingais. Privačiajame sektoriuje paprastai tai yra fizinis arba juridinis asmuo; viešajame sektoriuje paprastai tai yra valdžios institucija. Kiti subjektai, pvz., juridinio asmens teisių neturinčios įstaigos arba institucijos, duomenų valdytojais arba duomenų tvarkytojais gali būti tik jeigu tokia galimybė numatyta konkrečiose teisės nuostatose.

Pavyzdys. Kai įmonės „Sunshine“ rinkodaros skyrius, ketindamas atlikti rinkos tyrimą, planuoja tvarkyti duomenis, tokios duomenų tvarkymo operacijos duomenų valdytoju bus laikoma įmonė „Sunshine“, o ne rinkodaros skyrius. Rinkodaros skyrius negali būti duomenų valdytoju, nes jis nėra atskiras juridinis asmuo.

Kalbant apie įmonių grupes, patronuojančioji bendrovė ir kiekviena susijusi įmonė, kuri veikia kaip savarankiškas juridinis asmuo, yra laikoma atskira duomenų valdytoja arba duomenų tvarkytoja. Dėl šio atskiro teisinio statuso duomenų perdavimas tarp atskirų įmonių grupės narių turės būti pagrįstas konkrečiu teisiniu pagrindu. Nėra išskirtinės teisės, suteikiančios galimybę atskiriems įmonių grupės teisės subjektams keistis asmens duomenimis.

Šiomis aplinkybėmis reikia atkreipti dėmesį į privačių asmenų vaidmenį. **Pagal ES teisę** privatiems asmenims, kurie kitų asmenų duomenis tvarko tik asmeninėms arba šeimos reikmėms, Duomenų apsaugos direktyvos taisyklės netaikomos; tokie asmenys nėra laikomi duomenų valdytojais[78].

78 Duomenų apsaugos direktyvos 12 konstatuojamoji dalis ir 3 straipsnio 2 dalies paskutinė įtrauka.

Tačiau, nepaisant to, jurisprudencijoje nustatyta, kad duomenų apsaugos teisė bus taikoma tais atvejais, kai privatus asmuo, naudodamasis internetu, skelbia kitų asmenų duomenis.

Pavyzdys. Byloje *Bodil Lindqvist*[79] ESTT nusprendė, kad

„operacijos, kai interneto puslapyje minimi įvairūs asmenys, kurių tapatybė atskleidžiama nurodant pavardę arba kitus duomenis <...>, yra atliktos „visiškai ar iš dalies automatiniais būdais tvarkant asmens duomenis“ Direktyvos 95/46/EB 3 straipsnio 1 dalies prasme“[80].

Toks asmens duomenų tvarkymas nepatenka tik į asmeninės arba šeimos veiklos taikymo sritį, kuriai netaikoma Duomenų apsaugos direktyva, 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“[81].

Duomenų valdytojas

Pagal ES teisę duomenų valdytojas apibrėžiamas kaip asmuo, kuris „vienas ar drauge su kitais nustato asmens duomenų tvarkymo tikslus ir būdus“[82]. Duomenų valdytojo sprendime nustatomos duomenų tvarkymo priežastys ir būdai. **Pagal ET teisę** duomenų valdytojo apibrėžtyje papildomai užsimenama, kad duomenų valdytojas priima sprendimą dėl asmens duomenų, kuriuos reikėtų saugoti, kategorijų[83].

Konvencijos Nr. 108 duomenų valdytojo apibrėžtyje nurodomas papildomas duomenų valdymo aspektas, į kurį reikia atkreipti dėmesį. Šioje apibrėžtyje aptariamas klausimas, kurie subjektai, siekdami tam tikro tikslo, gali tvarkyti tam tikrus duomenis. Tačiau kai atliekamos tariamai neteisėtos tvarkymo operacijos, ir reikia nustatyti už tai atsakingą duomenų valdytoją, duomenų valdytoju bus laikomas asmuo arba subjektas, pvz., įmonė arba institucija, kuris nusprendė, kad duomenis reikėtų

79 2003 m lapkričio 6 d. ESTT sprendimas *Bodil Lindqvist*, C-101/01.

80 *Ibid.*, 27 punktas.

81 *Ibid.*, 47 punktas.

82 Duomenų apsaugos direktyvos 2 straipsnio d punktas.

83 Konvencijos Nr. 108 2 straipsnio d punktas.

tvarkyti, nepaisant to, ar jis turėjo teisę tai daryti[84]. Todėl prašymas ištrinti duomenis visada turi būti teikiamas faktiniam duomenų valdytojui.

Bendras duomenų valdymas

Duomenų apsaugos direktyvoje pateikiamoje duomenų valdytojo apibrėžtyje nurodyta, kad tam tikrais atvejais gali būti keletas teisiškai atskirų subjektų, kurie drauge arba kartu su kitais subjektais veikia kaip duomenų valdytojai. Tai reiškia, kad jie drauge priima sprendimą tvarkyti duomenis bendru tikslu[85]. Tačiau tai teisiškai įmanoma tik tais atvejais, kai konkrečioje teisinėje nuostatoje numatyta galimybė kartu tvarkyti duomenis bendru tikslu.

Pavyzdys. Kelių kredito įstaigų tvarkoma duomenų bazė, kurioje pateikiama informacija 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.

Taisyklėse aiškiai nenurodoma, ar bendro duomenų valdymo atveju būtina, kad bendras tikslas atitiktų kiekvieno duomenų valdytojo tikslą, ar tiesiog užtenka, kad jų tikslai sutaptų tik iš dalies. Vis dėlto Europos lygmeniu dar nėra susijusios jurisprudencijos ir nėra aiškus su atsakomybe susijusių pasekmių klausimas. 29 straipsnio duomenų apsaugos darbo grupė yra už platesnį sąvokos „bendras duomenų valdymas“ aiškinimą, kuriuo siekiama užtikrinti tam tikrą lankstumą, kuris padėtų spręsti su vis sudėtingesnėmis duomenų tvarkymo realijomis susijusius klausimus[86]. 29 straipsnio duomenų apsaugos darbo grupės pozicija patvirtinama byloje, kurioje dalyvavo Pasaulinė tarpbankinių finansinių telekomunikacijų organizacija (SWIFT).

Pavyzdys. Vadinamojoje SWIFT byloje Europos bankai naudojosi SWIFT (kuri iš pradžių buvo duomenų tvarkytoja), kad ji, bankams vykdant sandorius, perduotų duomenis. SWIFT atskleidė tokius bankų sandorių duomenis, kurie buvo saugomi Jungtinėse Valstijose esančiame kompiuteriniame serveryje, JAV iždo

84 Taip pat žr. 29 straipsnio duomenų apsaugos darbo grupė (2010 m.), 2010 m. vasario 16 d. *Nuomonės Nr. 1/2010 dėl sąvokų „duomenų valdytojas“ ir „duomenų tvarkytojas“*, WP 169, Briuselis, p. 15.

85 Duomenų apsaugos direktyvos 2 straipsnio d punktas.

86 29 straipsnio duomenų apsaugos darbo grupė (2010 m.), 2010 m. vasario 16 d. *Nuomonės Nr. 1/2010 dėl sąvokų „duomenų valdytojas“ ir „duomenų tvarkytojas“*, WP 169, Briuselis, p. 19.

departamentui, nors SWIFT besinaudojantys Europos bankai nedavė aiškaus nurodymo organizacijai atskleisti tokius duomenis. 29 straipsnio duomenų apsaugos darbo grupė, vertindama tokios padėties teisėtumą, priėjo prie išvados, kad SWIFT besinaudojantys Europos bankai ir pati SWIFT turi būti laikomi bendrais duomenų valdytojais, atsakingais už Europos klientų duomenų atskleidimą JAV valdžios institucijoms[87]. Nuspręsdama atskleisti duomenis, SWIFT neteisėtai prisiėmė duomenų valdytojo vaidmenį; akivaizdu, kad bankai nesugebėjo įvykdyti savo pareigos prižiūrėti savo duomenų tvarkytojo veiklą, todėl kaip duomenų valdytojai negali būti visiškai atleidžiami nuo atsakomybės. Ši situacija yra susijusi bendru duomenų valdymu.

Duomenų tvarkytojas

Duomenų tvarkytojas **ES teisėje** apibrėžiamas kaip asmuo, kuris asmens duomenis tvarko duomenų valdytojo vardu[88]. Duomenų tvarkytojui patikėta veikla gali būti susijusi su konkrečia užduotimi arba aplinkybėmis, arba gali būti gana bendro ir plataus pobūdžio.

ET teisėje duomenų tvarkytojo reikšmė atitinka nustatytąją ES teisėje.

Kitų asmenų duomenis tvarkantys duomenų tvarkytojai taip pat bus savarankiški duomenų valdytojai, kai jie duomenis tvarkys savais tikslais, pvz., administruodami savo darbuotojų, pardavimų ir sąskaitų duomenis.

Pavyzdžiai. Įmonė „Everready“ kitoms įmonėms teikia specializuotas paslaugas, susijusias su žmogiškųjų išteklių duomenų administravimu. Šiuo atveju įmonė „Everready“ yra duomenų tvarkytoja.

Tačiau įmonei „Everready“ tvarkant savo darbuotojų duomenis, ji bus laikoma duomenų valdytoja, vykdančia duomenų tvarkymo operacijas, susijusias su jos, kaip darbdavės, pareigomis.

87 29 straipsnio duomenų apsaugos darbo grupė (2006 m.), 2006 m. lapkričio 22 d. *Nuomonė Nr. 10/2006 dėl Pasaulinės tarpbankinių finansinių telekomunikacijų organizacijos (SWIFT) atliekamo asmens duomenų tvarkymo,* WP 128, Briuselis.

88 Duomenų apsaugos direktyvos 2 straipsnio e punktas.

Duomenų valdytojo ir duomenų tvarkytojo ryšys

Kaip matėme, duomenų valdytojas apibrėžiamas kaip asmuo, kuris nustato duomenų tvarkymo tikslus ir būdus.

> Pavyzdys. Įmonės „Sunshine“ direktorius nusprendžia, kad įmonė „Moonlight“, kuri specializuojasi rinkos analizės srityje, turėtų atlikti įmonės „Sunshine“ klientų duomenų rinkos analizę. Nors užduotis nustatyti tvarkymo būdus perduodama įmonei „Moonlight“, įmonė „Sunshine“ išliks duomenų valdytoja, o įmonė „Moonlight“ bus tik duomenų tvarkytoja, nes pagal sutartį „Moonlight“ gali naudoti „Sunshine“ klientų duomenis tik įmonės „Sunshine“ nustatytais tikslais.

Jeigu įgaliojimai nustatyti duomenų tvarkymo būdus suteikiami duomenų tvarkytojui, duomenų valdytojas vis tiek turi turėti galimybę daryti įtaką duomenų tvarkytojo sprendimams dėl tvarkymo būdų. Visa atsakomybė vis tiek tenka duomenų valdytojui, kuris turi prižiūrėti duomenų tvarkytojų veiklą ir užtikrinti, kad jų sprendimai atitiktų duomenų apsaugos teisę. Todėl sutartis, kurioje duomenų valdytojui būtų draudžiama daryti įtaką duomenų tvarkytojo sprendimams, tikriausiai būtų aiškinama kaip bendro duomenų valdymo sutartis, ir duomenų valdytojo teisinė atsakomybė būtų padalijama abiem šalims.

Be to, jeigu duomenų tvarkytojas nesilaiko duomenų valdytojo nustatytų duomenų naudojimo apribojimų, jis tampa duomenų valdytoju bent tų veiksmų atžvilgiu, kurie pažeidžia duomenų valdytojo nurodymus. Labai tikėtina, kad tokiu atveju duomenų tvarkytojas taps duomenų valdytoju, kuris veikia neteisėtai. Todėl pradinis duomenų valdytojas turės paaiškinti, kaip duomenų tvarkytojas galėjo pažeisti jam suteiktus įgaliojimus. Tiesą sakant, 29 straipsnio duomenų apsaugos darbo grupė tokiais atvejais yra linkusi laikytis bendro duomenų valdymo prielaidos, nes tai padeda užtikrinti geriausią duomenų subjektų interesų apsaugą[89]. Svarbi bendro duomenų valdymo pasekmė turėtų būti solidari atsakomybė už žalą, leidžianti duomenų subjektams pasinaudoti įvairesnėmis teisių gynimo priemonėmis.

Klausimų dėl atsakomybės padalijimo gali kilti ir tais atvejais, kai duomenų valdytojas yra maža įmonė, o duomenų tvarkytojas yra didelė kolektyvinė bendrovė,

89 29 straipsnio duomenų apsaugos darbo grupė (2010 m.), 2010 m. vasario 16 d. *Nuomonės Nr. 1/2010 dėl sąvokų „duomenų valdytojas“ ir „duomenų tvarkytojas“*, WP 169, Briuselis, p. 25, ir 29 straipsnio duomenų apsaugos darbo grupė (2006 m.), 2006 m. lapkričio 22 d. *Nuomonė Nr. 10/2006 dėl Pasaulinės tarpbankinių finansinių telekomunikacijų organizacijos (SWIFT) atliekamo asmens duomenų tvarkymo,* WP 128, Briuselis.

kuri gali nurodyti savo paslaugų teikimo sąlygas. Vis dėlto tokiomis aplinkybėmis 29 straipsnio duomenų apsaugos darbo grupė laikosi nuomonės, kad įprastas atsakomybės lygis neturėtų būti mažinamas atsižvelgiant į ekonominės pusiausvyros nebuvimą, ir duomenų valdytojo sąvoka turėtų būti suprantama taip pat[90].

Siekiant aiškumo ir skaidrumo, duomenų valdytojo ir duomenų tvarkytojo ryšys turėtų būti išsamiai nustatytas rašytinėje sutartyje[91]. Nesant tokios sutarties, laikoma, kad duomenų valdytojas pažeidė pareigą užtikrinti tarpusavio atsakomybės rašytinę dokumentaciją ir dėl šios priežasties jam gali būti taikomos sankcijos[92].

Duomenų tvarkytojai gali norėti perduoti tam tikras užduotis kitiems duomenų tvarkytojams. Teisiškai tai įmanoma. Toks užduočių perdavimas priklausys nuo duomenų valdytojo ir duomenų tvarkytojo sutarties nuostatų, įskaitant tai, ar duomenų valdytojo leidimą būtina gauti kiekvienu konkrečiu atveju, ar užtenka, kad duomenų tvarkytojas apie tai tik informuotų duomenų valdytoją.

ET teisėje pirmiau išaiškintos duomenų valdytojo ir duomenų tvarkytojo sąvokos taikomos be jokių išimčių, kaip nurodyta pagal Konvenciją Nr. 108 parengtose rekomendacijose[93].

2.3.2. Duomenų gavėjai ir trečiosios šalys

Šių dviejų kategorijų asmenų arba subjektų, kurie numatyti Duomenų apsaugos direktyvoje, skirtumas iš esmės pagrįstas jų santykiais su duomenų valdytoju ir jiems suteiktu leidimu susipažinti su duomenų valdytojo turimais asmens duomenimis.

Trečioji šalis teisiškai yra kitas subjektas nei duomenų valdytojas. Todėl atskleidžiant duomenis trečiajai šaliai visada reikia remtis konkrečiu teisiniu pagrindu. Pagal Duomenų apsaugos direktyvos 2 straipsnio f punktą trečioji šalis reiškia „bet kurį fizinį ar juridinį asmenį, valstybės valdžios instituciją, agentūrą ar bet kurį kitą organą, nesantį duomenų subjektu, duomenų valdytoju ar duomenų tvarkytoju, arba tokiu asmeniu, kuriam leidžiama tvarkyti duomenis, tiesiogiai įgaliotam duomenų

90 29 straipsnio duomenų apsaugos darbo grupė (2010 m.), 2010 m. vasario 16 d. *Nuomonės Nr. 1/2010 dėl sąvokų „duomenų valdytojas“ ir „duomenų tvarkytojas“*, WP 169, Briuselis, p. 26.

91 Duomenų apsaugos direktyvos 17 straipsnio 3 ir 4 dalys.

92 29 straipsnio duomenų apsaugos darbo grupė (2010 m.), 2010 m. vasario 16 d. *Nuomonės Nr. 1/2010 dėl sąvokų „duomenų valdytojas“ ir „duomenų tvarkytojas“*, WP 169, Briuselis, p. 27.

93 Žr., pvz., Rekomendacijos dėl profiliavimo 1 straipsnį.

valdytojo ar duomenų tvarkytojo“. Tai reiškia, kad asmenys, dirbantys organizacijoje, kuri teisiškai yra kitas subjektas nei duomenų valdytojas (net jei ji priklauso tai pačiai grupei arba patronuojančiajai bendrovei), bus (arba yra) trečiosios šalys. Kita vertus, banko padaliniai, tvarkantys kliento duomenis pagrindinės buveinės tiesioginiu pavedimu, neturėtų būti laikomi trečiosiomis šalimis[94].

Duomenų gavėjo sąvokos turinys yra platesnis nei trečiosios šalies sąvokos. Vadovaujantis Duomenų apsaugos direktyvos 2 straipsnio g punktu, duomenų gavėjas reiškia „fizinį ar juridinį asmenį, valstybės valdžios instituciją, agentūrą ar bet kurį kitą organą, kuriam atskleidžiami duomenys, net jei jis yra trečioji šalis“. Šiuo duomenų gavėju gali būti duomenų valdytojui arba duomenų tvarkytojui nepriklausantis asmuo (šiuo atveju toks duomenų gavėjas būtų trečioji šalis) arba duomenų valdytojui arba duomenų tvarkytojui dirbantis asmuo, pvz., darbuotojas arba kitas tos pačios įmonės arba institucijos padalinys.

Duomenų gavėjus atskirti nuo trečiųjų šalių yra svarbu tik atsižvelgiant į teisėto duomenų atskleidimo sąlygas. Duomenų valdytojo arba duomenų tvarkytojo darbuotojai be papildomo teisinio reikalavimo gali būti asmens duomenų gavėjais, jeigu jie dalyvauja duomenų valdytojo arba duomenų tvarkytojo vykdomose tvarkymo operacijose. Kita vertus, duomenų valdytojo arba duomenų tvarkytojo atžvilgiu teisiškai nepriklausoma trečioji šalis negali naudoti duomenų valdytojo tvarkomų asmens duomenų, išskyrus atvejus, kai konkrečiu atveju galioja tai leidžiantis daryti teisinis pagrindas. Todėl tam, kad trečiosios šalys duomenų gavėjos galėtų teisėtai gauti asmens duomenis, visada reikalingas teisinis pagrindas.

Pavyzdys. Duomenų tvarkytojo darbuotojas, kuris asmens duomenis naudoja vykdydamas darbdavio nustatytas užduotis, yra duomenų gavėjas, o ne trečioji šalis, ir toks darbuotojas naudoja duomenis duomenų tvarkytojo vardu ir vadovaudamasis jo nurodymais.

Tačiau jeigu tas pats darbuotojas nusprendžia duomenis, su kuriais jis gali susipažinti kaip duomenų tvarkytojo darbuotojas, naudoti savais tikslais ir parduoda juos kitai įmonei, tuomet darbuotojas laikomas veikusiu kaip trečioji šalis. Jis nesivadovauja duomenų tvarkytojo (darbdavio) pateiktais nurodymais. Darbuotojas, kaip trečioji šalis, turėtų pagrįsti duomenų įgijimą ir pardavimą teisiniu

94 29 straipsnio duomenų apsaugos darbo grupė (2010 m.), 2010 m. vasario 16 d. *Nuomonės Nr. 1/2010 dėl sąvokų „duomenų valdytojas“ ir „duomenų tvarkytojas“*, WP 169, Briuselis, p. 31.

pagrindu. Šiame pavyzdyje akivaizdu, kad darbuotojas negali remtis tokiu teisiniu pagrindu, todėl jo veiksmai yra neteisėti.

2.4. Sutikimas

Pagrindiniai faktai

- Sutikimas, kaip asmens duomenų tvarkymo teisinis pagrindas, turi būti savanoriškas, konkretus ir tai turi būti informuoto asmens sutikimas.
- Sutikimas turi būti duodamas nedviprasmiškai. Sutikimas gali būti duodamas aiškiai arba numanomas atsižvelgiant į tokį elgesį, dėl kurio nekyla abejonių, jog duomenų subjektas sutinka, kad jo duomenys būtų tvarkomi.
- Ypatingi duomenys gali būti tvarkomi remiantis tik aiškiu sutikimu.
- Sutikimą galima bet kuriuo metu atšaukti.

Sutikimas reiškia „bet kurį savanoriškai ir žinomai duotą konkretų duomenų subjekto pareiškimą“[95]. Dažniausiai tai ir būna teisėto duomenų tvarkymo teisinis pagrindas (žr. 4.1 dalį).

2.4.1. Galiojančio sutikimo elementai

ES teisėje nustatyti trys galiojančio sutikimo elementai, kuriais siekiama užtikrinti, kad duomenų subjektas iš tikrųjų sutiktų, kad jo duomenys būtų naudojami:

- duomenų subjektas, duodamas sutikimą, neturėjo patirti jokio spaudimo;
- duomenų subjektas turėjo būti tinkamai informuotas apie sutikimo tikslą ir pasekmes ir
- sutikimo turinys turi būti pakankamai konkretus.

Tik patenkinus visus šiuos reikalavimus pagal duomenų apsaugos teisę sutikimas bus laikomas galiojančiu.

95 Duomenų apsaugos direktyvos 2 straipsnio h punktas.

Konvencijoje Nr. 108 nepateikiama sutikimo apibrėžtis; ji turi būti nustatoma vidaus teisėje. Vis dėlto **pagal ET teisę** galiojančio sutikimo sąlygos susijusios su išvardytomis sąlygomis ir tai numatyta pagal Konvenciją Nr. 108 parengtose rekomendacijose[96]. Sutikimo reikalavimai atitinka galiojančio ketinimų pareiškimo pagal Europos civilinę teisę reikalavimus.

Papildomi civilinėje teisėje nustatyti galiojančio sutikimo reikalavimai, pvz., veiksnumas, savaime suprantama, taikomi ir duomenų apsaugos srityje, nes tokie reikalavimai yra pagrindinės būtinosios teisinės sąlygos. Veiksnumo neturinčių asmenų negaliojantis sutikimas reikš, kad nėra teisinio pagrindo tvarkyti tokių asmenų duomenis.

Sutikimas gali būti duodamas aiškiai[97] arba neaiškiai. Žodžiu arba raštu davus aiškų sutikimą, nekyla jokių abejonių dėl duomenų subjekto ketinimų; neaiškus sutikimas nustatomas atsižvelgiant į konkrečias aplinkybes. Kiekvienas sutikimas turi būti duodamas nedviprasmiškai[98]. Tai reiškia, kad neturėtų kilti jokių pagrįstų abejonių dėl to, kad duomenų subjektas norėjo informuoti apie savo sutikimą tvarkyti jo duomenis. Pavyzdžiui, negalima teigti, kad asmuo davė aiškų sutikimą, jeigu toks sutikimas nustatomas atsižvelgiant į žmogaus neveikimą. Tvarkant ypatingus duomenis, būtina gauti aiškų ir nedviprasmišką sutikimą.

Laisvas sutikimas

Laisvas sutikimas galioja tik tuomet, „jeigu duomenų subjektas gali laisvai pasirinkti, o nedavus sutikimo jam nekyla apgaulės, bauginimo, prievartos arba rimtų neigiamų pasekmių atsiradimo rizika“[99].

Pavyzdys. Daugelyje oro uostų keleiviai į įsodinimo vietas įleidžiami tik juos patikrinus kūno skeneriais[100]. Atsižvelgiant į tai, kad skenuojant tvarkomi keleivių duomenys, tvarkymas turi atitikti vieną iš Duomenų apsaugos direktyvos 7 straipsnyje nustatytų tikslų (žr. 4.1.1 dalį). Galimybė pereiti kūno skenerius keleiviams kartais pateikiama kaip alternatyva, reiškianti, kad jų sutikimu gali

96 Žr., pvz., Konvencijos Nr. 108 Rekomendacijos dėl statistinių duomenų 6 punktą.

97 Duomenų apsaugos direktyvos 8 straipsnio 2 dalis.

98 *Ibid.*, 7 straipsnio a punktas ir 26 straipsnio 1 dalis.

99 Taip pat žr. 29 straipsnio duomenų apsaugos darbo grupė (2011 m.), 2011 m. liepos 13 d. *Nuomonės Nr. 15/2011 dėl „sutikimo“ sąvokos*, WP 187, Briuselis, p. 12.

100 Šis pavyzdys pateikiamas *ibid.*, p. 15.

būti grindžiamas duomenų tvarkymas. Tačiau keleiviai galėtų baimintis, kad, atsisakę pereiti kūno skenerį, gali sukelti įtarimų arba jiems gali būti taikomos papildomos kontrolės priemonės, pvz., asmens apžiūra. Dauguma keleivių sutinka būti skenuojami, nes taip išvengia galimų problemų arba vėlavimo. Galima teigti, kad toks sutikimas nėra visiškai laisvas.

Todėl patikimą teisinį pagrindą galima rasti teisės aktų leidėjo įstatyme, pagrįstame Duomenų apsaugos direktyvos 7 straipsnio e punktu, t. y. pareiga keleiviams bendradarbiauti atsižvelgiant į svarbesnį viešąjį interesą. Tokiame teisės akte vis tiek galėtų būti numatyta galimybė rinktis skenavimą arba jo atsisakyti, tačiau tik tuo atveju, jei taikomos papildomos, konkrečiomis aplinkybėmis būtinos pasienio kontrolės priemonės. Būtent tokias nuostatas Europos Komisija 2011 m. įtvirtino dviejuose kūno skeneriams taikomuose reglamentuose[101].

Laisvam sutikimui pavojus taip pat gali kilti pavaldumo atvejais, kai tarp duomenų valdytojo, prašančio duoti sutikimą, ir sutikimą duodančio duomenų subjekto yra didelių ekonominių arba kitokios rūšies skirtumų[102].

Pavyzdys. Didelė įmonė, tiesiog siekdama užtikrinti geresnę vidaus komunikaciją, planuoja sukurti katalogą, kuriame būtų nurodomi visų darbuotojų vardai ir pavardės, jų einamos pareigos ir veiklos adresai. Personalo vadovas pasiūlo kataloge naudoti kiekvieno darbuotojo nuotrauką, kad, pvz., bendradarbiai galėtų vieni kitus lengviau atpažinti per posėdžius. Darbuotojų atstovai teigia, kad tai turėtų būti daroma tik gavus kiekvieno darbuotojo sutikimą.

Šiuo atveju darbuotojo sutikimas turėtų būti laikomas teisiniu pagrindu tvarkyti katalogo nuotraukas, nes akivaizdu, kad nuotraukos paskelbimas kataloge pats savaime nesukelia neigiamų pasekmių ir, be to, tikėtina, kad darbuotojas nesusidurs su neigiamais darbdavio inicijuotų veiksmų padariniais, jei jis nesutiktų, kad jo nuotrauka būtų skelbiama kataloge.

101 2011 m. lapkričio 10 d. Komisijos reglamentas (ES) Nr. 1141/2011, kuriuo dėl kūno skenerių naudojimo ES oro uostuose iš dalies keičiamas Reglamentas (EB) Nr. 272/2009, kuriuo papildomi bendrieji pagrindiniai civilinės aviacijos saugumo standartai, OL L 293, 2011, ir 2011 m. lapkričio 11 d. Komisijos įgyvendinimo reglamentas (ES) Nr. 1147/2011, kuriuo dėl kūno skenerių naudojimo ES oro uostuose iš dalies keičiamas Reglamentas (ES) Nr. 185/2010, kuriuo įgyvendinami bendrieji pagrindiniai aviacijos saugumo standartai, OL L 294, 2011.

102 Taip pat žr. 29 straipsnio duomenų apsaugos darbo grupė (2001 m.), 2001 m. rugsėjo 13 d. *Nuomonė Nr. 8/2001 dėl asmens duomenų tvarkymo atsižvelgiant į darbo santykius*, WP 48, Briuselis, ir 29 straipsnio duomenų apsaugos darbo grupė (2005 m.), 2005 m. lapkričio 25 d. *Darbo dokumentas dėl 1995 m. spalio 24 d. Direktyvos 95/46/EB 26 straipsnio 1 dalies vienodo aiškinimo*, WP 114, Briuselis.

Tačiau tai nereiškia, kad sutikimas niekada negali galioti tokiomis aplinkybėmis, kuriomis sutikimo nedavimas sukeltų neigiamas pasekmes. Jeigu, pvz., nesutikimas gauti prekybos centro kortelę reikštų, kad asmuo negautų nuolaidų tam tikroms prekėms, sutikimas vis tiek būtų galiojantis teisinis pagrindas tvarkyti tų klientų asmens duomenis, kurie sutiko gauti tokią kortelę. Tarp įmonės ir kliento nėra subordinacija pagrįstų santykių ir nesutikimo pasekmės nėra pakankamai rimtos, kad duomenų subjektas negalėtų laisvai duoti sutikimo.

Kita vertus, tais atvejais, kai pakankamai svarbias prekes arba paslaugas galima gauti tik trečiosioms šalims atskleidus asmens duomenis, paprastai duomenų subjekto sutikimas atskleisti duomenis negali būti laikomas laisvu sprendimu ir todėl pagal duomenų apsaugos teisę jis negaliotų.

Pavyzdys. Keleivių sutikimas, kad oro bendrovė teiktų keleivio duomenų įrašus (PNR), t. y. jų tapatybės duomenis, valgymo įpročius arba sveikatos problemas, konkrečios užsienio valstybės imigracijos institucijoms pagal duomenų apsaugos teisę negali būti laikomas galiojančiu sutikimu, nes keliaujantys keleiviai, jei nori apsilankyti šioje valstybėje, neturi kito pasirinkimo. Norint tokius duomenis teikti teisėtai, reikėtų kitokio nei sutikimas teisinio pagrindo: labiausiai tikėtina, kad tokiu atveju turėtų būti remiamasi specialiu įstatymu.

Informuoto asmens sutikimas

Duomenų subjektas, prieš priimdamas sprendimą, turi turėti galimybę susipažinti su pakankamai išsamia informacija. Tai, ar informacija yra pakankamai išsami, nustatoma kiekvienu konkrečiu atveju. Paprastai informuoto asmens sutikimas bus pagrįstas tiksliu ir lengvai suprantamu dalyko, dėl kurio prašoma duoti sutikimą, aprašymu ir, be kita ko, informavimu apie sutikimo arba nesutikimo pasekmes. Informacija turėtų būti aprašoma atsižvelgiant į numatomus tokios informacijos gavėjus.

Duomenų subjektas turi turėti galimybę lengvai susipažinti su informacija. Galimybė susipažinti su informacija ir jos matomumas yra svarbūs elementai. Internetinėje aplinkoje keliais lygmenimis pateikiami informaciniai pranešimai gali būti tinkama priemonė, nes duomenų subjektas, susipažinęs su glausta informacija, be kita ko, gali gauti ir išsamią informaciją.

Konkretus sutikimas

Galiojantis sutikimas taip pat reiškia konkretų sutikimą. Toks sutikimas glaudžiai susijęs su informacijos apie sutikimo objektą kokybe. Šiomis aplinkybėmis svarbu atkreipti dėmesį į vidutinio duomenų subjekto pagrįstus lūkesčius. Duomenų subjekto turi būti prašoma dar kartą duoti sutikimą, jeigu taikomos papildomos arba pakeistos duomenų tvarkymo operacijos, kurių pagrįstai nebuvo galima numatyti duodant pradinį sutikimą.

Pavyzdys. Byloje *Deutsche Telekom AG*[103] ESTT nagrinėjo klausimą, ar telekomunikacijų paslaugų teikėjai turėjo pareigą, pagal *Direktyvos dėl privatumo ir elektroninių ryšių* 12 straipsnį[104] teikdami abonentų asmens duomenis, gauti atnaujintą duomenų subjektų sutikimą, atsižvelgiant į tai, kad duodant sutikimą duomenų gavėjai nebuvo aiškiai nurodyti.

ESTT nusprendė, kad pagal minėtą straipsnį atnaujintas sutikimas prieš teikiant duomenis nebuvo reikalingas, nes duomenų subjektai pagal šią nuostatą turėjo galimybę duoti sutikimą tik dėl duomenų tvarkymo tikslo ir negalėjo pasirinkti skirtingų abonentų knygų, kuriose šie duomenys galėtų būti skelbiami.

ESTT pabrėžė, jog „pagal 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“[105]. Be to, abonentui, o ne abonentų knygos autoriui „gali būti žalingas būtent asmens duomenų paskelbimas specifinės paskirties abonentų knygoje“[106].

103 2011 m. gegužės 5 d. ESTT sprendimas *Deutsche Telekom AG prieš Vokietiją*, C-543/09; visų pirma žr. 53 ir 54 punktus.

104 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 m.

105 2011 m. gegužės 5 d. ESTT sprendimas *Deutsche Telekom AG prieš Vokietiją*, C-543/09; visų pirma žr. 61 punktą.

106 *Ibid.*, visų pirma žr. 62 punktą.

2.4.2. Teisė bet kuriuo metu reikalauti, kad sutikimas būtų atšauktas

Duomenų apsaugos direktyvoje neužsimenama apie bendrą teisę bet kuriuo metu reikalauti, kad sutikimas būtų atšauktas. Tačiau visuotinai pripažįstama, kad tokia teisė yra ir kad duomenų subjektai turi turėti galimybę savo nuožiūra ja pasinaudoti. Atšaukiant sutikimą neturėtų būti reikalaujama nurodyti priežastis ir dėl tokio atšaukimo neturėtų kilti neigiamų pasekmių naudai, duomenų subjekto gautai dėl anksčiau duoto sutikimo naudoti duomenis.

Pavyzdys. Klientas sutinka gauti reklaminius laiškus duomenų valdytojui pateiktu adresu. Klientui atšaukus sutikimą, duomenų valdytojas turi nedelsiant liautis siuntęs reklaminius laiškus. Šiuo atveju neturėtų būti taikomos piniginės sankcijos, pvz., mokesčiai.

Jeigu klientas nuolat galėjo pasinaudoti 5 proc. nuolaida užsisakydamas viešbučio kambarį dėl to, kad sutiko, kad naudojant jo duomenis būtų siunčiami reklaminiai laiškai, sutikimo gauti reklaminius laiškus atšaukimas vėlesniame etape neturėtų reikšti, jog toks klientas turi grąžinti gautų nuolaidų sumą.

3

Pagrindiniai Europos duomenų apsaugos teisės principai

ES	Aptariami klausimai	ET
Duomenų apsaugos direktyvos 6 straipsnio 1 dalies a ir b punktai. 2008 m. gruodžio 16 d. ESTT sprendimas *Huber prieš Vokietiją*, C-524/06. 2010 m. lapkričio 9 d. sprendimas *Volker ir Markus Schecke GbR (C-92/09) ir Hartmut Eifert (C-93/09) prieš Land Hessen*, sujungtos bylos C-92/09 ir C-93/09.	**Teisėto duomenų tvarkymo principas.**	Konvencijos Nr. 108 5 straipsnio a ir b punktai. 2000 m. gegužės 4 d. EŽTT sprendimas *Rotaru prieš Rumuniją* (DK), Nr. 28341/95. 2002 m. spalio 22 d. EŽTT sprendimas *Taylor-Sabori prieš Jungtinę Karalystę*, Nr. 47114/99. 2003 m. sausio 28 d. EŽTT sprendimas *Peck prieš Jungtinę Karalystę*, Nr. 44647/98. 2011 m. spalio 18 d. EŽTT sprendimas *Khelili prieš Šveicariją*, Nr. 16188/07. 1987 m. kovo 26 d. EŽTT sprendimas *Leander prieš Švediją*, Nr. 9248/81.
Duomenų apsaugos direktyvos 6 straipsnio 1 dalies b punktas.	**Tikslo nustatymo ir apribojimo principas.**	Konvencijos Nr. 108 5 straipsnio b punktas.
	Duomenų kokybės principai:	

ES	Aptariami klausimai	ET
Duomenų apsaugos direktyvos 6 straipsnio 1 dalies c punktas.	**duomenų aktualumo principas;**	Konvencijos Nr. 108 5 straipsnio c punktas.
Duomenų apsaugos direktyvos 6 straipsnio 1 dalies d punktas.	**duomenų tikslumo principas;**	Konvencijos Nr. 108 5 straipsnio d punktas.
Duomenų apsaugos direktyvos 6 straipsnio 1 dalies e punktas.	**riboto duomenų saugojimo principas.**	Konvencijos Nr. 108 5 straipsnio e punktas.
Duomenų apsaugos direktyvos 6 straipsnio 1 dalies e punktas.	**Su moksliniais tyrimais ir statistika susijusi išimtis.**	Konvencijos Nr. 108 9 straipsnio 3 dalis.
Duomenų apsaugos direktyvos 6 straipsnio 1 dalies a punktas.	**Sąžiningo duomenų tvarkymo principas.**	Konvencijos Nr. 108 5 straipsnio a punktas. 2009 m. spalio 27 d. EŽTT sprendimas *Haralambie prieš Rumuniją*, Nr. 21737/03. 2009 m. lapkričio 6 d. EŽTT sprendimas *K. H. ir kiti prieš Slovakiją*, Nr. 32881/04.
Duomenų apsaugos direktyvos 6 straipsnio 2 dalis.	**Atskaitomybės principas.**	

Konvencijos Nr. 108 5 straipsnyje nustatytuose principuose įtvirtintos esminės Europos duomenų apsaugos teisės nuostatos. Principai taip pat įtvirtinti Duomenų apsaugos direktyvos 6 straipsnyje ir jais remiamasi nustatant išsamesnes nuostatas kituose direktyvos straipsniuose. Visi vėliau ET arba ES lygmeniu priimti duomenų apsaugos teisės aktai turi atitikti šiuos principus ir į juos būtina atsižvelgti aiškinant tokius teisės aktus. Nacionaliniu lygmeniu galima numatyti įvairias šių principų išimtis ir apribojimus[107]; jie turi būti numatyti įstatymuose, jais turi būti siekiama teisėto tikslo ir jie turi būti būtini demokratinėje visuomenėje. Visos šios sąlygos turi būti tenkinamos.

107 Konvencijos Nr. 108 9 straipsnio 2 dalis; Duomenų apsaugos direktyvos 13 straipsnio 2 dalis.

3.1. Teisėto duomenų tvarkymo principas

Pagrindiniai faktai

- Siekiant suprasti teisėto duomenų tvarkymo principą, reikia atsižvelgti į teisės į duomenų apsaugą teisėto ribojimo sąlygas pagal Chartijos 52 straipsnio 1 dalį ir pateisinamo ribojimo reikalavimus, numatytus EŽTK 8 straipsnio 2 dalyje.
- Todėl asmens duomenų tvarkymas yra teisėtas tik jeigu toks tvarkymas:
  - atitinka įstatymą,
  - juo siekiama teisėto tikslo ir
  - jis yra būtinas demokratinėje visuomenėje siekiant teisėto tikslo.

ES ir ET duomenų apsaugos teisėje kaip pirmasis principas nurodomas teisėto duomenų tvarkymo principas; jis beveik vienodai aprašytas Konvencijos Nr. 108 5 straipsnyje ir Duomenų apsaugos direktyvos 6 straipsnyje.

Nė vienoje iš šių nuostatų nepateikiama „teisėto duomenų tvarkymo“ apibrėžtis. Siekiant suprasti šią teisinę sąvoką, būtina atsižvelgti į EŽTK nustatytus pateisinamus ribojimus, kuriuos savo jurisprudencijoje išaiškino EŽTT, ir Chartijos 52 straipsnyje nustatytas teisėtų apribojimų sąlygas.

3.1.1. Pateisinamo ribojimo reikalavimai pagal EŽTK

Tvarkant asmens duomenis gali būti ribojama duomenų subjekto teisė į privataus gyvenimo gerbimą. Tačiau teisė į privataus gyvenimo gerbimą nėra absoliuti teisė ir turi būti vertinama atsižvelgiant į kitus teisėtus interesus, nesvarbu, ar tai kitų asmenų interesai (privatūs interesai), ar visuomenės interesai (viešieji interesai).

Toliau nurodomos sąlygos, kuriomis pateisinami valstybės nustatyti apribojimai.

Apribojimai atitinka įstatymą

Vadovaujantis EŽTT jurisprudencija, apribojimas atitinka įstatymą, jeigu jis pagrįstas vidaus teisės nuostata, turinčia tam tikrus požymius. Įstatymas turi būti „prieinamas

atitinkamiems asmenims ir turi būti įmanoma numatyti jo padarinius“[108]. Taisyklė yra numatoma „jeigu ji yra pakankamai tiksliai suformuluota, kad bet kuris asmuo, jei reikalinga, gavęs tinkamą konsultaciją, galėtų atitinkamai elgtis“[109]. „Šiuo atžvilgiu įstatymui keliamas tikslumo reikalavimas priklausys nuo konkretaus dalyko.“[110]

Pavyzdys. Byloje *Rotaru prieš Rumuniją*[111] EŽTT nustatė, kad EŽTK 8 straipsnis buvo pažeistas, nes Rumunijos įstatyme buvo leidžiama rinkti, įrašyti ir archyvuoti su nacionaliniu saugumu susijusią informaciją slaptose rinkmenose, nenustatant šių įgaliojimų įgyvendinimo ribų. Todėl tokiais įgaliojimais valdžios institucijos galėjo naudotis savo nuožiūra. Pavyzdžiui, vidaus teisėje nebuvo apibrėžta informacijos, kuri galėjo būti tvarkoma, rūšis, asmenų, kuriems galėjo būti taikomos stebėjimo priemonės, kategorijos, aplinkybės, kuriomis buvo galima taikyti tokias priemones, arba procedūra, kuria reikėjo vadovautis. Atsižvelgdamas į šiuos trūkumus, EŽTT padarė išvadą, kad vidaus teisė neatitiko nuspėjamumo reikalavimo, nustatyto EŽTK 8 straipsnyje, ir kad šis straipsnis buvo pažeistas.

Pavyzdys. Byloje *Taylor-Sabori prieš Jungtinę Karalystę*[112] policija stebėjo pareiškėją. Pakeitusi pareiškėjo pranešimų gaviklį savu pranešimo gavikliu, policija galėjo perskaityti jam siunčiamas žinutes. Vėliau pareiškėjas buvo suimtas ir jam pateikti kaltinimai dėl bendrininkavimo tiekiant kontroliuojamus vaistus. Prokuroras bylą prieš pareiškėją rengė iš dalies remdamasis tuometiniais rašytiniais pranešimo gaviklio pranešimais, kuriuos buvo perėmusi policija. Tačiau nagrinėjant pareiškėjo bylą Britanijos teisėje nebuvo nuostatos, reglamentuojančios slapto ryšių, perduodamų asmeninėmis telekomunikacijų priemonėmis,

108 2000 m. vasario 16 d. EŽTT sprendimo *Amann prieš Šveicariją* (DK), Nr. 27798/95, 50 punktas; taip pat žr. 1998 m. kovo 25 d. EŽTT sprendimo *Kopp prieš Šveicariją*, Nr. 23224/94, 55 punktą ir 2009 m. vasario 10 d. EŽTT sprendimo *Iordachi ir kiti prieš Moldovą*, Nr. 25198/02, 50 punktą.

109 2000 m. vasario 16 d. EŽTT sprendimo *Amann prieš Šveicariją* (DK), Nr. 27798/95, 56 punktas; taip pat žr. 1985 m. balandžio 26 d. EŽTT sprendimo *Malone prieš Jungtinę Karalystę*, Nr. 8691/79, 66 punktą; 1983 m. kovo 25 d. EŽTT sprendimo *Silver ir kiti prieš Jungtinę Karalystę*, Nr. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 88 punktą.

110 1979 m. balandžio 26 d. EŽTT sprendimo *The Sunday Times prieš Jungtinę Karalystę*, Nr. 6538/74, 49 punktas; taip pat žr. 1983 m. kovo 25 d. EŽTT sprendimo *Silver ir kiti prieš Jungtinę Karalystę*, Nr. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 88 punktą.

111 2000 m. balandžio 4 d. EŽTT sprendimo *Rotaru prieš Rumuniją* (DK), Nr. 28341/95, 57 punktas; taip pat žr. 2007 m. birželio 28 d. EŽTT sprendimą *Association for European Integration and Human Rights ir Ekimdzhiev prieš Bulgariją*, Nr. 62540/00; 2011 m. birželio 21 d. EŽTT sprendimą *Shimovolos prieš Rusiją*, Nr. 30194/09, ir 2005 m. gegužės 31 d. EŽTT sprendimą *Vetter prieš Prancūziją*, Nr. 59842/00.

112 2002 m. spalio 22 d. EŽTT sprendimas *Taylor-Sabori prieš Jungtinę Karalystę*, Nr. 47114/99.

perėmimo tvarką. Todėl šios teisės apribojimai neatitiko įstatymo. EŽTT nusprendė, kad EŽTK 8 straipsnis buvo pažeistas.

Apribojimu siekiama teisėto tikslo

Teisėtas tikslas gali būti vienas iš nurodytų viešųjų interesų arba kitų asmenų teisės ir laisvės.

Pavyzdys. Byloje *Peck prieš Jungtinę Karalystę*[113] pareiškėjas bandė gatvėje persipjauti riešus ir nusižudyti. Pareiškėjas nežinojo, kad jo bandymas nusižudyti buvo filmuojamas AVSS kamera. Policija, kuri stebėjo AVSS kamerų rodomus vaizdus, išgelbėjo pareiškėją ir perdavė AVSS įrašus žiniasklaidai, kuri paskelbė šiuos įrašus neužmaskuodama pareiškėjo veido. EŽTT nustatė, kad šiuo atveju nebuvo jokių susijusių arba pagrįstų priežasčių, kuriomis institucijos būtų galėjusios pagrįstai tiesiogiai atskleisti įrašą visuomenei iš anksto negavusi pareiškėjo sutikimo arba neužmaskavusi jo tapatybės. EŽTT nusprendė, kad EŽTK 8 straipsnis buvo pažeistas.

Apribojimas būtinas demokratinėje visuomenėje

EŽTT nurodė, jog „būtinumo sąvoka reiškia, kad apribojimas yra susijęs su neišvengiamu socialiniu poreikiu ir kad jis visų pirma yra proporcingas siekiamam teisėtam tikslui“[114].

Pavyzdys. Byloje *Khelili prieš Šveicariją*[115] policija, vykdydama patikrinimą, nustatė, kad pareiškėja turėjo korteles, kuriose buvo įrašytas toks tekstas: „Maloni, graži trisdešimtmetė moteris norėtų susitikti su vyru puodeliui kavos arba retkarčiais nueiti į pasimatymą. Tel. <...>.“ Pareiškėja teigė, kad, aptikusi šias korteles, policija įrašė jos vardą ir pavardę į prostituciją 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 jis gali padaryti kitą pažeidimą, tam tikromis aplinkybėmis gali būti pateisinamas. Tačiau pareiškėjos

113 2003 m. sausio 28 d. EŽTT sprendimas *Peck prieš Jungtinę Karalystę*, Nr. 44647/98, visų pirma žr. 85 punktą.

114 1985 m. liepos 11 d. EŽTT sprendimo *Leander prieš Švediją*, Nr. 9248/8185, 58 punktas.

115 2011 m. spalio 18 d. EŽTT sprendimas *Khelili prieš Šveicariją*, Nr. 16188/07.

byloje kaltinimai vertimusi neteisėta prostitucija pasirodė per daug neaiškūs ir abstraktūs, be to, jie nebuvo pagrįsti konkrečiais faktais, nes pareiškėja niekada nebuvo nuteista už vertimąsi neteisėta prostitucija ir todėl tokia padėtis negali būti laikoma „būtinu socialiniu poreikiu“ pagal EŽTK 8 straipsnį. Atsižvelgdamas į tai, kad laikomų duomenų apie pareiškėją tikslumą turėjo įrodyti institucijos, ir į pareiškėjos teisių apribojimo rimtumą, Teismas nusprendė, kad žodžio „prostitutė“ saugojimas policijos rinkmenose daug metų nebuvo būtinas demokratinėje visuomenėje. Teismas nusprendė, kad EŽTK 8 straipsnis buvo pažeistas.

Pavyzdys. Byloje *Leander prieš Švediją*[116] EŽTT nusprendė, kad asmenų, kurie siekia eiti svarbias su nacionaliniu saugumu susijusias pareigas, slaptas patikrinimas pats savaime neprieštaravo būtinumo demokratinėje visuomenėje reikalavimui. Atsižvelgdamas į nacionaliniame įstatyme nustatytas specialias apsaugos priemones, kuriomis siekiama apsaugoti duomenų subjektų interesus (pvz., parlamento ir teisingumo ministro taikomos kontrolės priemonės), EŽTT padarė išvadą, kad Švedijos personalo kontrolės sistema atitiko EŽTK 8 straipsnyje nustatytus reikalavimus. Atsižvelgiant į plačią valstybės atsakovės diskrecijos laisvę, ji turėjo teisę manyti, kad pareiškėjo byloje nacionalinio saugumo interesai buvo viršesni už asmeninius interesus. Teismas nusprendė, kad EŽTK 8 straipsnis nebuvo pažeistas.

3.1.2. Teisėtų apribojimų sąlygos pagal ES chartiją

Chartijos ir EŽTK struktūra ir formuluotė nėra vienoda. Chartijoje nekalbama apie garantuojamų teisių apribojimus, tačiau joje yra nuostata dėl apribojimo (-ų), kuris (-ie) taikomas (-i) įgyvendinant Chartijoje pripažintas teises ir laisves.

Pagal Chartijos 52 straipsnio 1 dalį Chartijoje pripažintų teisių ir laisvių, įskaitant teisės į asmens duomenų apsaugą, pvz., asmens duomenų tvarkymo, įgyvendinimo apribojimai leidžiami tik jeigu:

- apribojimas numatytas įstatyme,
- juo gerbiama teisės į duomenų apsaugą esmė,
- jis yra būtinas atsižvelgiant į proporcingumo principą ir

116 1985 m. liepos 11 d. EŽTT sprendimo *Leander prieš Švediją*, Nr. 9248/81, 59 ir 67 punktai.

- jis atitinka Sąjungos pripažįstamo bendro intereso tikslus arba poreikį apsaugoti kitų asmenų teises ir laisves.

Pavyzdys. Byloje *Volker ir Markus Schecke*[117] ESTT nusprendė, kad Taryba ir Komisija, nustatydamos pareigą skelbti asmens duomenis, susijusius su kiekvienu fiziniu asmeniu, kuris gavo (tam tikrų žemės ūkio fondų) paramą, ir tai darydamos neatskyrė paramos gavėjų remdamosi susijusiais kriterijais, pvz., laikotarpiai, kai tokie asmenys gavo tokią pagalbą, tokios pagalbos intensyvumas arba pobūdis ir suma, viršijo ribas, kurios nustatomos vadovaujantis proporcingumo principu.

Todėl ESTT nusprendė, kad reikia paskelbti negaliojančiomis tam tikras Tarybos reglamento (EB) Nr. 1290/2005 nuostatas ir paskelbti negaliojančiu visą Reglamentą Nr. 259/2008[118].

Nepaisant skirtingos formuluotės, Chartijos 52 straipsnio 1 dalyje nustatytos teisėto duomenų tvarkymo sąlygos yra panašios į nustatytąsias EŽTK 8 straipsnio 2 dalyje. Tiesą sakant, manytina, kad Chartijos 52 straipsnio 1 dalyje nurodytos sąlygos atitinka EŽTK 8 straipsnio 2 dalyje išvardytas sąlygas, nes Chartijos 52 straipsnio 3 dalies pirmajame sakinyje pabrėžiama, kad „šioje Chartijoje nurodytų teisių, atitinkančių Žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos garantuojamas teises, esmė ir taikymo sritis yra tokia, kaip nustatyta toje Konvencijoje“.

Tačiau pagal 52 straipsnio 3 dalies paskutinį sakinį „ši nuostata nekliudo Sąjungos teisėje numatyti didesnę apsaugą“. Šiuo atveju palyginus EŽTK 8 straipsnio 2 dalį ir 52 straipsnio 3 dalies pirmą sakinį, tai gali reikšti tik tai, kad pateisinamų apribojimų pagal EŽTK 8 straipsnio 2 dalį sąlygos yra minimalūs reikalavimai nustatant teisėtus teisės į duomenų apsaugą apribojimus pagal Chartiją. Todėl pagal ES teisę teisėtai tvarkant asmens duomenis reikia, kad būtų tenkinamos bent EŽTK 8 straipsnio 2 dalyje nustatytos sąlygos; vis dėlto ES teisėje konkrečiais atvejais galėtų būti nustatyti papildomi reikalavimai.

117 2010 m. lapkričio 9 d. ESTT sprendimo *Volker ir Markus Schecke GbR (C-92/09) ir Hartmut Eifert (C-93/09) prieš Land Hessen*, sujungtos bylos C-92/09 ir C-93/09, 89 ir 86 punktai.

118 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.

Teisėto duomenų tvarkymo principo pagal ES teisę ir susijusių EŽTK nuostatų ryšys išsamiau aptariamas ES sutarties 6 straipsnio 3 dalyje, kurioje teigiama, kad „pagrindinės teisės, kurias garantuoja Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija <...>, sudaro Sąjungos teisės bendruosius principus“.

3.2. Tikslo įvardijimo ir apribojimo principas

Pagrindiniai faktai

- Prieš pradedant tvarkyti duomenis būtina aiškiai apibrėžti tvarkymo tikslą.
- Pagal ES teisę tvarkymo tikslas turi būti aiškiai apibrėžtas; ET teisėje nustatyta, kad šis klausimas reglamentuojamas vidaus teisėje.
- Tvarkymas neapibrėžtais tikslais neatitinka duomenų apsaugos teisės.
- Tolesnis duomenų naudojimas kitu tikslu turi būti pagrįstas papildomu teisiniu pagrindu, jeigu naujas tvarkymo tikslas neatitinka pradinio tikslo.
- Duomenų perdavimas trečiosioms šalims yra naujas tikslas, kurį reikia pagrįsti papildomu teisiniu pagrindu.

Iš esmės tikslo įvardijimo ir apribojimo principas reiškia, kad asmens duomenų tvarkymo teisėtumas priklausys nuo tvarkymo tikslo[119]. Duomenų valdytojas privalo tiksliai ir aiškiai nurodyti tikslą prieš pradėdamas tvarkyti duomenis[120]. **Pagal ES teisę** tai turi būti atliekama paskelbiant deklaraciją, kitaip tariant, pranešant apie tai atitinkamai priežiūros institucijai arba bent jau tokį pranešimą užfiksuojant vidaus dokumentuose, su kuriais duomenų valdytojas turi leisti susipažinti patikrinimus atliekančioms priežiūros institucijoms ir duomenų subjektui.

Asmens duomenų tvarkymas neapibrėžtais ir (arba) neribotais tikslais yra neteisėtas.

Kiekvienas naujas duomenų tvarkymo tikslas turi būti pagrįstas konkrečiu teisiniu pagrindu. Negalima remtis tuo, kad duomenys iš pradžių buvo įgyti arba tvarkomi kitu teisėtu tikslu. Todėl teisėtam tvarkymui galioja tik konkretus jam nustatytas

119 Konvencijos Nr. 108 5 straipsnio b punktas; Duomenų apsaugos direktyvos 6 straipsnio 1 dalies b punktas.

120 Taip pat žr. 29 straipsnio duomenų apsaugos darbo grupė (2013 m.), 2013 m. balandžio 2 d. *Nuomonė Nr. 3/2013 dėl tikslo ribojimo*, WP 203, Briuselis.

tikslas ir bet koks naujas tvarkymo tikslas turi būti pagrįstas nauju atskiru teisiniu pagrindu. Ypač atidžiai reikės apsvarstyti duomenų atskleidimą trečiosioms šalims, nes atskleidimas paprastai reikš naują tikslą ir turės būti pagrįstas teisiniu pagrindu, kuris skirsis nuo duomenų rinkimo teisinio pagrindo.

Pavyzdys. Oro bendrovė renka duomenis apie savo keleivius, kad, naudodamasi užsakymų duomenimis, galėtų sklandžiai vykdyti skrydžius. Oro bendrovei reikės duomenų apie: keleivių vietų numerius; specialius fizinius sutrikimus, pvz., vežimėlis neįgaliesiems, ir specialaus maisto, pvz., košerinio arba musulmonų maisto, poreikius. Jeigu oro bendrovės būtų prašoma teikti šiuos PNR duomenis atvykimo oro uosto valstybės imigracijos institucijoms, šie duomenys būtų naudojami imigracijos kontrolės tikslais, ir šis tikslas neatitiktų pradinio duomenų rinkimo tikslo. Todėl šiems duomenims teikti imigracijos institucijai reikės naujo atskiro teisinio pagrindo.

Kalbant apie konkretaus tikslo taikymo sritį ir ribas, reikia atkeipti dėmesį į Konvencijoje Nr. 108 ir Duomenų apsaugos direktyvoje nurodytą suderinamumo sąvoką: duomenis naudoti suderinamais tikslais leidžiama tuo atveju, jeigu jie pagrįsti pradiniu teisiniu pagrindu. Vis dėlto pati sąvoka „suderinamas“ nėra apibrėžta ir kiekvienu konkrečiu atveju ji aiškinama atskirai.

Pavyzdys. Įmonė „Sunshine“, parduodama klientų duomenis, kuriuos įgijo palaikydama ryšius su klientais, tiesiogine rinkodara užsiimančiai įmonei „Moonligth“, kuri, naudodamasi šiais duomenimis, nori palengvinti su trečiosiomis šalimis susijusias rinkodaros kampanijas, siekia naujo tikslo, kuris nesuderinamas su CRM, t. y. pradiniu įmonės „Sunshine“ duomenų apie klientus rinkimo tikslu. Todėl norint parduoti duomenis įmonei „Moonlight“, reikalingas naujas teisinis pagrindas.

Priešingai, kai įmonė „Sunshine“ naudoja CMR duomenis siekdama savo rinkodaros tikslų, t. y. siunčia reklamos pranešimus, susijusius su jos produktais, savo klientams, tokie CMR duomenys laikomi naudojamais suderinamu tikslu.

Duomenų apsaugos direktyvoje aiškiai nurodyta, kad „duomenų tvarkymas istoriniais, statistiniais ar moksliniais tikslais laikomas suderinamu dalyku, su sąlyga, kad valstybės narės numato atitinkamas apsaugos priemones“[121].

Pavyzdys. Įmonė „Sunshine“ rinko ir saugojo CRM duomenis apie savo klientus. Įmonei „Sunshine“ leidžiama toliau naudoti šiuos duomenis savo klientų pirkimo įpročių statistinei analizei atlikti, nes statistikos sudarymas yra suderinamas tikslas. Papildomo teisinio pagrindo, pvz., duomenų subjektų sutikimo, šiuo atveju nereikia.

Šiuos duomenis vien statistiniais tikslais būtų leidžiama teikti įmonei „Starlight“ ir tam nereikėtų papildomo teisinio pagrindo, tačiau tik tuo atveju, jeigu būtų taikomos tinkamos apsaugos priemonės, pvz., duomenų subjektų tapatybių užmaskavimas, nes tvarkant duomenis statistiniais tikslais nebūtina žinoti asmenų tapatybes.

3.3. Duomenų kokybės principai

Pagrindiniai faktai

- Duomenų valdytojas duomenų kokybės principų turi laikytis atlikdamas visas tvarkymo operacijas.
- Vadovaujantis riboto duomenų saugojimo principu, duomenis būtina ištrinti iš karto, kai jų nebereikia tikslams, dėl kurių jie buvo surinkti.
- Riboto duomenų saugojimo principo išimtys turi būti nustatytos įstatyme užtikrinant specialias duomenų subjektų apsaugos priemonės.

3.3.1. Duomenų aktualumo principas

Tvarkomi tik tokie duomenys, kurie yra „adekvatūs, susiję ir savo apimtimi neviršijantys tikslų, kuriems jie renkami ir (arba) vėliau tvarkomi“[122]. Tvarkymui atrinktų

121 Tokių nacionalinių nuostatų pavyzdžių galima rasti Austrijos duomenų apsaugos įstatyme (vok. *Datenschutzgesetz*), Federalinis oficialusis leidinys I, Nr. 165/1999, 46 punktas. Įstatymas anglų kalba skelbiamas adresu www.dsk.gv.at/DocView.axd?CobId=41936.

122 Konvencijos Nr. 108 5 straipsnio c punktas ir Duomenų apsaugos direktyvos 6 straipsnio 1 dalies c punktas.

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.

Šiuolaikinėje visuomenėje duomenų aktualumo principas yra aplinkybė, į kurią reikia papildomai atsižvelgti: naudojant specialias didesnę privatumo apsaugą padedančias užtikrinti technologijas, kartais įmanoma apskritai išvengti asmens duomenų naudojimo arba naudoti pseudoniminius duomenis, o tai yra privatumo nepažeidžianti priemonė. 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. Ši informacija elektronine forma taip pat įrašoma kortelės luste. Įlipus į autobusą arba tramvajų, lustinę kortelę reikia priglausti prie, pvz., 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 nevisiškai atitinka duomenų aktualumo principą: 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, pvz., 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. Tokiu atveju asmens duomenys nebūtų renkami ir minėta sistema būtų optimali priemonė atsižvelgiant į duomenų aktualumo principą, nes pagal jį reikalaujama rinkti kuo mažiau duomenų.

3.3.2. Duomenų tikslumo principas

Asmens informaciją turintis duomenų valdytojas naudoja šią informaciją tik tuomet, kai imasi priemonių, kurios padeda užtikrinti pagrįstą tikrumą dėl duomenų tikslumo ir naujumo.

Pareiga užtikrinti duomenų tikslumą turi būti vertinama atsižvelgiant į duomenų tvarkymo tikslą.

Pavyzdys. Baldus parduodanti įmonė rinko klientų tapatybės duomenis ir adresus, kad galėtų nusiųsti jiems sąskaitas. Po šešių mėnesių ta pati įmonė planuoja pradėti rinkodaros kampaniją ir nori susisiekti su savo buvusiais klientais. Kad su jais susisiektų, įmonė nori gauti leidimą susipažinti su nacionaliniu gyventojų registru, kuriame, tikėtina, bus pateikiami naujausi adresai, nes gyventojai yra teisiškai įpareigoti informuoti registrą apie savo dabartinį adresą. Su šio registro duomenimis gali susipažinti tik pateisinamą priežastį nurodę fiziniai ir juridiniai asmenys.

Šiuo atveju įmonė negali remtis argumentu, kad reikia užtikrinti duomenų tikslumą ir naujumą ir taip pagrįsti savo teisę rinkti gyventojų registre naujus su adresais susijusius duomenis apie visus savo buvusius klientus. Duomenys buvo renkami išrašant sąskaitas; šiuo tikslu pardavimo metu svarbu žinoti adresą. Teisinio pagrindo rinkti naujus su adresu susijusius duomenis nėra, nes rinkodaros kampanijos vykdymas nėra už teisę į duomenų apsaugą svarbesnis tikslas ir todėl juo negalima pagrįsti teisės susipažinti su registro duomenimis.

Taip pat gali būti atvejų, kai saugomus duomenis atnaujinti teisiškai draudžiama, nes duomenų saugojimo tikslas iš esmės yra tam tikrų įvykių dokumentavimas.

Pavyzdys. Medicininės operacijos pažyma negali būti keičiama, t. y. atnaujinama, net jeigu vėliau paaiškėja, kad joje nurodytos išvados yra klaidingos. Tokiomis aplinkybėmis galima įrašyti tik papildomas pastabas, nes jos aiškiai parodo vėliau padarytus įrašus.

Kita vertus, yra atvejų, kai reguliariai tikrinti duomenų tikslumą ir juos atnaujinti, būtina dėl žalos, kurią galėtų patirti duomenų subjektas dėl netikslių duomenų.

Pavyzdys. Jei kuris nors asmuo nori sudaryti sutartį su banko institucija, bankas paprastai patikrins būsimo kliento kreditingumą. Šiuo tikslu galima pasinaudoti specialiomis duomenų bazėmis, kuriose pateikiama privačių asmenų kredito istorija. Jeigu tokioje duomenų bazėje pateikiami netikslūs arba pasenę duomenys apie asmenį, jis gali susidurti su rimtomis problemomis. Todėl tokių duomenų bazių valdytojai, turi dėti ypatingas pastangas siekdami laikytis duomenų tikslumo principo.

Be to, ne su faktais, o įtarimais susiję duomenys, pvz., baudžiamųjų tyrimų duomenys, gali būti renkami ir saugojami tol, kol duomenų valdytojas, rinkdamas tokią

informaciją, gali remtis teisiniu pagrindu ir toks rinkimas yra tinkamai pagrįstas atsižvelgiant į įtarimų rimtumą.

3.3.3. Riboto duomenų saugojimo principas

Duomenų apsaugos direktyvos 6 straipsnio 1 dalies e punkte ir Konvencijos Nr. 108 5 straipsnio e punkte valstybėms narėms nustatytas reikalavimas užtikrinti, kad asmens duomenys būtų „laikomi tokio pavidalo, kad duomenų subjektų tapatybės būtų galima nustatyti ne ilgiau, nei tai yra reikalinga tais tikslais, dėl kurių duomenys buvo surinkti arba po to tvarkomi“. Todėl pasiekus šiuos tikslus duomenys turi būti sunaikinti.

Byloje *S. ir Marper* EŽTT padarė išvadą, kad, vadovaujantis pagrindiniais Europos Tarybos susijusių priemonių ir kitų susitariančiųjų šalių teisės ir praktikos principais, duomenų saugojimas turi būti proporcingas tikslui, dėl kurio jie buvo surinkti, o saugojimo terminas turi būti ribotas, visų pirma policijos sektoriuje[123].

Vis dėlto ribotas asmens duomenų saugojimo terminas taikomas tik tokiems duomenims, kurių forma leidžia nustatyti duomenų subjektų tapatybę. Todėl teisėtas nebereikalingų duomenų saugojimas galėtų būti atliekamas tokius duomenis anonimizuojant arba pseudonimizuojant.

Duomenų apsaugos direktyvoje nustatyta, kad riboto duomenų saugojimo principas netaikomas duomenų laikymui atsižvelgiant į jų panaudojimą ateityje mokslo, istoriniais arba statistiniais tikslais[124]. Tačiau taip nuolat saugant ir naudojant asmens duomenis turi būti taikomos nacionalinėje teisėje numatytos specialios apsaugos priemonės.

3.4. Sąžiningo duomenų tvarkymo principas

Pagrindiniai faktai

- Sąžiningas duomenų tvarkymas reiškia skaidrų tvarkymą, visų pirma duomenų subjektų atžvilgiu.

123 2008 m. gruodžio 4 d. EŽTT sprendimas *S. ir Marper prieš Jungtinę Karalystę*, Nr. 30562/04 ir 30566/04; taip pat žr., pvz., 2012 m. lapkričio 13 d. EŽTT sprendimą *M. M. prieš Jungtinę Karalystę*, Nr. 24029/07.

124 Duomenų apsaugos direktyvos 6 straipsnio 1 dalies e punktas.

- Duomenų valdytojai, prieš pradėdami tvarkyti duomenų subjektų duomenis, turi nurodyti jiems duomenų tvarkymo tikslą ir duomenų valdytojo tapatybę ir adresą.
- Asmens duomenų negalima tvarkyti slaptai ir užmaskuotai, išskyrus atvejus, kai tokia galimybė aiškiai numatyta įstatyme.
- Duomenų subjektai turi teisę susipažinti su visais savo tvarkomais duomenimis.

Sąžiningo duomenų tvarkymo principas visų pirma reglamentuoja duomenų valdytojo ir duomenų subjekto santykius.

3.4.1. Skaidrumas

Šiuo principu duomenų valdytojas įpareigojamas informuoti duomenų subjektus apie tai, kaip naudojami jų duomenys.

Pavyzdys. Byloje *Haralambie prieš Rumuniją*[125] pareiškėjas prašė leisti susipažinti su savo byla, kurią saugojo žvalgybos tarnyba, tačiau jo prašymas buvo patenkintas tik po penkerių metų. EŽTT pakartojo, kad asmenys, kurių bylas turėjo institucijos, yra ypač suinteresuoti susipažinti su tokiomis bylomis. Valdžios institucijos turėjo pareigą numatyti veiksmingą leidimo susipažinti su tokia informacija išdavimo procedūrą. EŽTT nuomone, aplinkybės, kad pareiškėjo prašymas susipažinti su savo asmens byla buvo patenkintas tik po penkerių metų, nebuvo galima pateisinti nei bylos medžiagos kiekiu, kurį reikėjo perduoti, nei archyvų sistemos trūkumais. Institucijos nesudarė sąlygų pareiškėjui pasinaudoti veiksmingomis ir prieinamomis procedūromis, kurios leistų jam per pagrįstą terminą susipažinti su savo asmens bylos medžiaga. Teismas nusprendė, kad EŽTK 8 straipsnis buvo pažeistas.

Duomenų tvarkymo operacijos duomenų subjektams turi būti išaiškinamos lengvai prieinamu būdu, padedančiu duomenų subjektams suprasti, kas bus daroma su jų duomenims. Duomenų subjektas taip pat turi teisę, kad jo prašymu duomenų valdytojas jį informuotų, ar jo duomenys tvarkomi ir, jei taip, kokie duomenys tvarkomi.

3.4.2. Pasitikėjimo įgijimas

Duomenų valdytojai, atsižvelgdami į duomenų subjektų ir plačiosios visuomenės interesus, turėtų dokumentuoti savo įsipareigojimą teisėtai ir skaidriai tvarkyti

125 2009 m. spalio 27 d. EŽTT sprendimas *Haralambie prieš Rumuniją*, Nr. 21737/03.

duomenis. Duomenų tvarkymo operacijos neturi būti atliekamos slaptai ir neturėtų sukelti nenumatytų neigiamų pasekmių. Duomenų valdytojai turėtų užtikrinti, kad pirkėjai, klientai arba piliečiai būtų informuojami apie jų duomenų naudojimą. Be to, duomenų valdytojai, kiek tai įmanoma, turi veikti taip, kad galėtų nedelsdami patenkinti duomenų subjektų pageidavimus, visų pirma tais atvejais, kai duomenų tvarkymo teisinis pagrindas yra duomenų subjekto sutikimas.

Pavyzdys. Byloje *K. H. ir kiti prieš Slovakiją*[126] pareiškėjos buvo aštuonios romų kilmės moterys, kurios nėštumo ir gimdymo laikotarpiu buvo gydomos dviejose Rytų Slovakijos ligoninėse. Vėliau nė viena iš šių moterų negalėjo pastoti net po kelių bandymų. Nacionaliniai teismai nurodė ligoninėms leisti pareiškėjoms ir jų atstovams nusirašyti medicininių įrašų informaciją, tačiau atmetė jų prašymą daryti dokumentų fotokopijas, kad būtų užkirstas kelias netinkamam jų naudojimui. EŽTK 8 straipsnyje valstybėms numatyti pozityvūs įpareigojimai, be abejo, apima pareigą leisti duomenų subjektui daryti savo asmens bylos kopijas. Būtent valstybės turėjo nustatyti asmens duomenų bylų kopijų darymo tvarką arba, kai tinkama, nurodyti pagrįstas tokio leidimo išimtis. Nagrinėdami pareiškėjų bylą, vidaus teismai pritarė draudimui daryti medicininių įrašų kopijas ir šiuo atveju iš esmės rėmėsi poreikiu užtikrinti, kad nebūtų piktnaudžiaujama susijusia informacija. Vis dėlto EŽTT nebuvo aišku, kaip pareiškėjos, kurioms bet kuriuo atveju buvo leista be apribojimų susipažinti su medicininėmis bylomis, galėjo netinkamai naudoti informaciją apie save. Be to, tokiam netinkamam naudojimui buvo galima užkirsti kelią ir kitomis priemonėmis, o ne vien draudžiant pareiškėjams daryti bylų kopijas. Valstybė nesugebėjo nurodyti tinkamai pagrįstų priežasčių, kuriomis būtų galima pateisinti draudimą pareiškėjams tinkamai susipažinti su informacija apie savo sveikatą. Teismas nusprendė, kad 8 straipsnis buvo pažeistas.

Kalbant apie internetu teikiamas paslaugas pažymėtina, kad duomenų subjektai, susipažindami su duomenų tvarkymo sistemos ypatybėmis, turi aiškiai suprasti, kaip tvarkomi jų duomenys.

Sąžiningas duomenų tvarkymas taip pat reiškia, kad duomenų valdytojai turi būti pasirengę užtikrinti aukštesnio lygio duomenų subjektams teikiamų paslaugų kokybę, palyginti su minimaliais teisiniais reikalavimais, jeigu tai yra būtina atsižvelgiant į teisėtus duomenų subjekto interesus.

126 2009 m. lapkričio 6 d. EŽTT sprendimas *K. H. ir kiti prieš Slovakiją*, Nr. 32881/04.

3.5. Atskaitomybės principas

Pagrindiniai faktai

- Atskaitomybė reiškia, kad duomenų valdytojai, vykdydami duomenų tvarkymo veiklą, turi aktyviai įgyvendinti priemones, kurios padeda didinti duomenų apsaugą ir ją užtikrinti.
- Duomenų valdytojai atsako už tai, kad jų atliekamos duomenų tvarkymo operacijos atitiktų duomenų apsaugos teisę.
- Duomenų valdytojai bet kuriuo metu turi sugebėti plačiajai visuomenei ir priežiūros institucijoms įrodyti, kad laikosi su duomenų subjektais susijusių duomenų apsaugos nuostatų.

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 apibūdinant atskaitomybės principą nurodoma, kad „duomenų valdytojas turėtų būti atsakingas už tai, kad būtų laikomasi priemonių, kuriomis įgyvendinami pirmiau nurodyti (esminiai) principai“[127].

Konvencijoje Nr. 108 duomenų valdytojų atskaitomybė neminima, todėl tai iš esmės turi būti nustatoma vidaus teisėje. Tuo tarpu Duomenų apsaugos direktyvos 6 straipsnio 2 dalyje nurodyta, jog duomenų valdytojas turėtų užtikrinti, kad būtų laikomasi 6 straipsnio 1 dalyje nurodytų duomenų kokybės principų.

Pavyzdys. E. privatumo direktyvos 2002/58/EB 2009 m. pakeitimas[128] yra teisės akto, kuriame pabrėžiama atskaitomybės principo svarba, pavyzdys. Pagal iš dalies pakeistos direktyvos 4 straipsnį nustatoma pareiga įgyvendinti saugumo politiką, t. y. „užtikrinti, kad būtų įgyvendinama saugumo politika asmens duomenų tvarkymo srityje“. Todėl kalbant apie šios direktyvos saugumo

127 2013 m. EBPO *Gairių dėl privatumo ir tarpvalstybinių asmens duomenų apsaugos srautų apsaugos* 14 straipsnis.

128 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.

nuostatas pažymėtina, kad teisės aktų leidėjas nusprendė, jog būtina įtvirtinti aiškų reikalavimą nustatyti ir įgyvendinti saugumo politiką.

29 straipsnio duomenų apsaugos darbo grupės nuomonėje[129] nurodyta, kad iš esmės atskaitomybė – tai duomenų valdytojo pareiga:

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

- turėti parengtus dokumentus, kuriais duomenų subjektams ir priežiūros institucijoms būtų parodoma, kokių priemonių imtasi siekiant užtikrinti atitiktį duomenų apsaugos taisyklėms.

Todėl pagal atskaitomybės principą reikalaujama, kad duomenų valdytojai aktyviais veiksmais įrodytų atitiktį, o ne vien lauktų, kad duomenų subjektai arba priežiūros institucijos nurodytų trūkumus.

129 29 straipsnio duomenų apsaugos darbo grupė (2010 m.), 2010 m liepos 13 d. *Nuomonė Nr. 3/2010 dėl atskaitomybės principo*, WP 173, Briuselis.

4

Europos duomenų apsaugos teisės taisyklės

ES	Aptariami klausimai	ET
Teisėto neypatingų duomenų tvarkymo taisyklės		
Duomenų apsaugos direktyvos 7 straipsnio a punktas.	**Sutikimas.**	Rekomendacijos dėl profiliavimo 3.4 straipsnio b punktas ir 3.6 straipsnis.
Duomenų apsaugos direktyvos 7 straipsnio b punktas.	**Ikisutartiniai ir sutartiniai santykiai.**	Rekomendacijos dėl profiliavimo 3.4 straipsnio b punktas.
Duomenų apsaugos direktyvos 7 straipsnio c punktas.	**Duomenų valdytojo teisinės pareigos.**	Rekomendacijos dėl profiliavimo 3.4 straipsnio a punktas.
Duomenų apsaugos direktyvos 7 straipsnio d punktas.	**Gyvybiniai duomenų subjekto interesai.**	Rekomendacijos dėl profiliavimo 3.4 straipsnio b punktas.
Duomenų apsaugos direktyvos 7 straipsnio e punktas ir 8 straipsnio 4 dalis. 2008 m. gruodžio 16 d. ESTT sprendimas *Huber prieš Vokietiją*, C-524/06.	**Viešasis interesas ir oficialių įpareigojimų vykdymas.**	Rekomendacijos dėl profiliavimo 3.4 straipsnio b punktas.
Duomenų apsaugos direktyvos 7 straipsnio f punktas, 8 straipsnio 2 ir 3 dalys. 2011 m. lapkričio 24 d. ESTT sprendimas *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C-468/10) ir Federación de Comercio Electrónico y Marketing Directo (FECEMD) (C-469/10) prieš Administración del Estado*, sujungtos bylos C-468/10 ir C-469/10.	**Teisėti kitų asmenų interesai.**	Rekomendacijos dėl profiliavimo 3.4 straipsnio b punktas.

ES	Aptariami klausimai	ET
Teisėto ypatingų duomenų tvarkymo taisyklės		
Duomenų apsaugos direktyvos 8 straipsnio 1 dalis.	Bendras draudimas tvarkyti duomenis.	Konvencijos Nr. 108 6 straipsnis.
Duomenų apsaugos direktyvos 8 straipsnio 2–4 dalys.	Bendro draudimo išimtys.	Konvencijos Nr. 108 6 straipsnis.
Duomenų apsaugos direktyvos 8 straipsnio 5 dalis.	Duomenų apie (apkaltinamuosius) nuosprendžius tvarkymas.	Konvencijos Nr. 108 6 straipsnis.
Duomenų apsaugos direktyvos 8 straipsnio 7 dalis.	Identifikacinių numerių (asmens kodų) tvarkymas.	
Saugaus duomenų tvarkymo taisyklės		
Duomenų apsaugos direktyvos 17 straipsnis.	Pareiga užtikrinti saugų duomenų tvarkymą.	Konvencijos Nr. 108 7 straipsnis. 2008 m. liepos 17 d. EŽTT sprendimas *I. prieš Suomiją*, Nr. 20511/03.
E. privatumo direktyvos 4 straipsnio 2 dalis.	Pranešimai apie duomenų saugumo pažeidimą.	
Duomenų apsaugos direktyvos 16 straipsnis.	Pareiga laikytis konfidencialumo.	
Skaidraus duomenų tvarkymo taisyklės		
	Bendros nuostatos dėl skaidrumo.	Konvencijos Nr. 108 8 straipsnio a punktas.
Duomenų apsaugos direktyvos 10 ir 11 straipsniai.	Informavimas.	Konvencijos Nr. 108 8 straipsnio a punktas.
Duomenų apsaugos direktyvos 10 ir 11 straipsniai.	Pareigos teikti informaciją išimtys.	Konvencijos Nr. 108 8 straipsnis.
Duomenų apsaugos direktyvos 18 ir 19 straipsniai.	Pranešimas.	Rekomendacijos dėl profiliavimo 9.2 straipsnio a punktas.
Taisyklės dėl skatinimo laikytis duomenų apsaugos teisės		
Duomenų apsaugos direktyvos 20 straipsnis.	Išankstinė patikra.	
Duomenų apsaugos direktyvos 18 straipsnio 2 dalis.	Asmens duomenų apsaugos pareigūnai.	Rekomendacijos dėl profiliavimo 8.3 straipsnis.
Duomenų apsaugos direktyvos 27 straipsnis.	Elgesio kodeksas.	

Principai iš esmės yra bendro pobūdžio. Šiuos principus taikant konkrečiose situacijose paliekama tam tikra laisvė savo nuožiūra juos aiškinti ir pasirinkti priemones. Pagal **ET teisę** Konvencijos Nr. 108 šalys gali naudotis šia laisve savo vidaus teisėje aiškindamos šiuos principus. **ET teisėje** padėtis yra kitokia: siekiant užtikrinti duomenų apsaugą vidaus rinkoje, buvo manoma, kad būtina nustatyti jau galiojančias išsamias taisykles ES lygmeniu, kad būtų suderintas valstybių narių nacionaliniuose įstatymuose nustatytas duomenų apsaugos lygis. Duomenų apsaugos direktyvos 6 straipsnyje įtvirtintais principais nustatomas išsamių taisyklių rinkinys, kuris turi būti tiksliai perkeltas į nacionalinę teisę. Todėl toliau nurodytos pastabos dėl išsamių Europos duomenų apsaugos taisyklių iš esmės susijusios su ES teise.

4.1. Teisėto duomenų tvarkymo taisyklės

Pagrindiniai faktai

- Asmens duomenys gali būti teisėtai tvarkomi, jeigu:
  - duomenų tvarkymas yra pagrįstas duomenų subjekto sutikimu arba
  - asmens duomenis tvarkyti būtina atsižvelgiant į gyvybinius duomenų subjektų interesus, arba
  - duomenų tvarkymas pateisinamas kitų asmenų teisėtais interesais, tačiau tik tuo atveju, kai toks tvarkymas nepažeidžia duomenų subjektų interesų, susijusių su jų pagrindinių teisių apsauga.
- Teisėtam ypatingų asmens duomenų tvarkymui taikoma speciali, griežtesnė tvarka.

Duomenų apsaugos direktyvoje nustatyti du skirtingi teisėto duomenų tvarkymo taisyklių rinkiniai: 7 straipsnyje aptariamas neypatingų duomenų tvarkymo taisyklių rinkinys, o 8 straipsnyje – ypatingų duomenų tvarkymo taisyklių rinkinys.

4.1.1. Teisėtas neypatingų duomenų tvarkymas

Direktyvos 95/46 II skirsnyje „Duomenų tvarkymo teisėtumo kriterijai“ nustatyta, kad, atsižvelgiant į 13 straipsnyje numatytas išimtis, visi asmens duomenys turi būti tvarkomi, pirma, laikantis Duomenų apsaugos direktyvos 6 straipsnyje nurodytų duomenų kokybės principų ir, antra, laikantis vieno iš 7 straipsnyje nurodyto teisėto

duomenų tvarkymo kriterijų[130]. Remiantis šia taisykle galima nustatyti atvejus, kai neypatingi asmens duomenys yra tvarkomi teisėtai.

Sutikimas

ET teisėje sutikimas nėra minimas EŽTK 8 straipsnyje arba Konvencijoje Nr. 108. Tačiau ši sąvoka nurodyta EŽTT jurisprudencijoje ir keliose ET rekomendacijose. Pagal **ES teisę** sutikimas yra teisėtas duomenų tvarkymo pagrindas, kuris griežtai įtvirtintas Duomenų apsaugos direktyvos 7 straipsnio a punkte ir, be to, aiškiai nurodomas Chartijos 8 straipsnyje.

Sutartiniai santykiai

Kitas **ES teisėje** numatytas Duomenų apsaugos direktyvos 7 straipsnio b punkte nurodyto teisėto asmens duomenų tvarkymo pagrindas yra taikomas tais atvejais, kai duomenis tvarkyti „reikia vykdant sutartį, kurią duomenų subjektas yra sudaręs kaip viena iš šalių“. Ši nuostata taip pat taikoma ikisutartiniams santykiams. Pavyzdžiui, šalis ketina sudaryti sutartį, tačiau tikėtina, kad ji to dar nepadarė, nes neišsiaiškino tam tikrų klausimų. Jeigu vienai šaliai reikia šiuo tikslu tvarkyti duomenis, toks tvarkymas yra teisėtas atsižvelgiant į „duomenų subjekto reikalavimą norint imtis priemonių prieš sudarant sutartį“.

Kalbant apie ET teisę pažymėtina, kad pagal EŽTK 8 straipsnio 2 dalį teisė į duomenų apsaugą gali būti teisėtai apribojama, kai to reikia „kitų asmenų teisėms ir laisvėms apsaugoti“.

Duomenų valdytojo teisinės pareigos

Tuo tarpu **ES teisėje** aiškiai nurodomas kitas teisėto duomenų tvarkymo kriterijus, t. y. jei to „reikia vykdant teisinę prievolę, kuri privaloma duomenų valdytojui“ (Duomenų apsaugos direktyvos 7 straipsnio c punktas). Šioje nuostatoje minimi privačiajame sektoriuje veikiantys duomenų valdytojai; viešojo sektoriaus duomenų valdytojų teisinės pareigos aprašytos direktyvos 7 straipsnio e punkte. Yra daugybė atvejų, kai privačiojo sektoriaus duomenų valdytojai įstatymu įpareigojami tvarkyti

130 2003 m. gegužės 20 d. ESTT sprendimo *Österreichischer Rundfunk ir kiti*, sujungtos bylos C-465/00, C-138/01 ir C-139/01, 65 punktas; 2008 m. gruodžio16 d. ESTT sprendimo *Huber prieš Vokietiją*, C-524/06, 48 punktas; 2011 m. lapkričio 24 d. ESTT sprendimas *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C-468/10) ir Federación de Comercio Electrónico y Marketing Directo (FECEMD) (C-469/10) prieš Administración del Estado*, sujungtos bylos C-468/10 ir C-469/10, 26 punktas.

kitų asmenų duomenis; pvz., gydytojai ir ligoninės turi teisinę pareigą keletą metų saugoti duomenis apie pacientų gydymą, darbdaviai turi tvarkyti duomenis apie savo darbuotojus socialinės apsaugos ir mokesčių sumokėjimo tikslais, o įmonės turi tvarkyti duomenis apie savo klientus mokestiniais tikslais.

Atsižvelgiant į oro bendrovių pareigą teikti keleivių duomenis imigracijos kontrolės institucijoms, iškilo klausimas, ar *užsienio* teisėje nustatytos teisinės pareigos gali būti teisėtu pagrindu tvarkyti asmens duomenis pagal ES teisę (šis klausimas išsamiau aptariamas 6.2 dalyje).

Duomenų valdytojo teisinės pareigos yra teisėto duomenų tvarkymo **pagal ET teisę** pagrindas. Kaip jau nurodyta, privačiojo sektoriaus duomenų valdytojo teisinės pareigos yra tik vienas iš konkrečių kitų subjektų teisėtų interesų, kaip nurodyta EŽTK 8 straipsnio 2 dalyje. Todėl pirmiau nurodytas pavyzdys taip pat taikomas ET teisėje.

Gyvybiniai duomenų subjekto interesai

Pagal **ES teisę Duomenų apsaugos direktyvos** 7 straipsnio d punkte nustatyta, kad asmens duomenų tvarkymas yra teisėtas, jeigu juos „tvarkyti reikia norint apsaugoti gyvybinius duomenų subjekto interesus“. Tokie interesai, kurie yra glaudžiai susiję su duomenų subjektų gyvybe, galėtų būti teisėto, pvz., asmens sveikatos duomenų arba duomenų apie dingusius asmenis naudojimo pagrindas.

Kalbant apie **ET teisę** pažymėtina, kad apie gyvybinius duomenų subjekto interesus, kuriais gali būti pateisinamas teisės į duomenų apsaugą apribojimas, EŽTK 8 straipsnyje neužsimenama. Tačiau kai kuriose ET rekomendacijose, kuriomis papildomos kai kurios Konvencijos Nr. 108 reguliavimo sritys, aiškiai nurodoma, kad teisėtas duomenų tvarkymas gali būti pateisinamas duomenų subjekto gyvybiniais interesais[131]. Gyvybiniai duomenų subjekto interesai laikomi neabejotinai patenkančiais į priežasčių, kuriomis pateisinamas duomenų tvarkymas, rinkinį: dėl pagrindinių teisių apsaugos niekada neturėtų kilti pavojus saugomo asmens gyvybiniams interesams.

Viešasis interesas ir oficialių įgaliojimų vykdymas

Atsižvelgiant į įvairius viešųjų reikalų tvarkymo būdus, Duomenų apsaugos direktyvos 7 straipsnio e punkte nustatyta, kad asmens duomenys gali būti teisėtai

131 Rekomendacijos dėl profiliavimo 3.4 straipsnio b punktas.

tvarkomi, jeigu juos tvarkyti „reikia vykdant užduotį, atliekamą visuomenės labui arba įgyvendinant oficialius įgaliojimus, suteiktus duomenų valdytojui arba trečiajai šaliai, kuriai atskleidžiami duomenys <...>“[132].

Pavyzdys. Byloje *Huber prieš Vokietiją*[133] Vokietijoje gyvenantis Austrijos pilietis H. Huber prašė, kad Federalinė migracijos ir pabėgėlių tarnyba iš Centrinio užsienio piliečių registro (vok. AZR) ištrintų jo duomenis. Šis registras, kuriame kaupiami ne Vokietijos ES piliečių, gyvenančių Vokietijoje ilgiau nei tris mėnesius, asmens duomenys, naudojamas statistiniais tikslais. Šiuos duomenis taip pat naudoja teisėsaugos ir teisminės institucijos tirdamos nusikalstamas veikas arba veikas, kurios kelią grėsmę visuomenės saugumui, ir vykdydamos tokių veikų baudžiamąjį persekiojimą. Prašymą priimti prejudicinį sprendimą pateikęs teismas klausė, ar asmens duomenų tvarkymas, pvz., tokiame registre kaip Centrinis užsienio piliečių registras, kuriuo taip pat gali naudotis kitos valdžios institucijos, atitinka ES teisę atsižvelgiant į tai, kad toks registras nėra sukurtas Vokietijos piliečiams.

ESTT nustatė, kad, pirma, pagal direktyvos 7 straipsnio e punktą asmens duomenys gali būti teisėtai tvarkomi tik jeigu juos tvarkyti reikia vykdant užduotį, atliekamą visuomenės labui arba įgyvendinant oficialius įgaliojimus.

Teismo manymu, „atsižvelgiant į tikslą užtikrinti lygiaverčio lygio apsaugą visose valstybėse narėse, Direktyvos 95/46 7 straipsnio e punkte minimos būtinumo sąvokos <...> 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“[134].

Teismas atkreipia dėmesį į tai, kad Sąjungos piliečio teisė laisvai judėti valstybėje narėje, kurios pilietybės jis neturi, nėra besąlyginė ir jai gali būti taikomi Sutartyje nustatyti apribojimai ir sąlygos, ir šiuo tikslu nustatytos priemonės. Todėl jei valstybė narė iš esmės gali teisėtai naudoti registrą, pvz., AZR, kad padėtų atsakingoms institucijoms taikyti teisės aktus, susijusius su teise turėti gyvenamąją vietą, tokiame registre negali būti informacijos, kuri nėra reikalinga siekiant šio konkretaus tikslo. Teismas daro išvadą, kad tokia asmens duomenų tvarkymo sistema atitinka ES teisę, jeigu joje yra tik tie duomenys, kurių reikia

132 Taip pat žr. Duomenų apsaugos direktyvos 32 konstatuojamąją dalį.

133 2008 m. gruodžio 16 d. ESTT sprendimas *Huber prieš Vokietiją*, C-524/06.

134 *Ibid.*, 52 punktas.

taikant tą teisės aktą ir jeigu dėl centralizuoto sistemos pobūdžio šis teisės aktas taikomas veiksmingiau. Nacionalinis teismas turi įvertinti, ar šios sąlygos tenkinamos šioje konkrečioje byloje. Priešingu atveju asmens duomenų saugojimas ir tvarkymas tokiame registre kaip AZR statistiniais tikslais bet kuriuo atveju negali būti laikomas būtinu pagal Direktyvos 95/46/EB 7 straipsnio e punktą[135].

Galiausiai registre esančių duomenų naudojimo kovos su nusikalstamumu tikslais klausimu Teismas konstatuoja, kad šis tikslas „reikalauja tirti padarytus nusikaltimus ir pažeidimus, neatsižvelgiant į juos padariusių asmenų pilietybę". Aptariamame registre nėra asmens duomenų, susijusių su atitinkamos valstybės narės piliečiais, ir šis skirtingas požiūris yra diskriminacinis, o tai draudžia SESV 18 straipsnis. Todėl ši nuostata, kaip ją aiškina Teismas, „draudžia valstybei narei kovos su nusikalstamumu tikslu įdiegti specialiai šios valstybės narės pilietybės neturintiems Europos Sąjungos piliečiams skirtą asmens duomenų tvarkymo sistemą"[136].

Viešajame sektoriuje veikiančioms institucijoms, kurios naudoja asmens duomenis, taip pat taikomas EŽTK 8 straipsnis.

Duomenų valdytojo arba trečiosios šalies teisėti interesai

Teisėtus interesus turi ne tik duomenų subjektas. Duomenų apsaugos direktyvos 7 straipsnio f punkte nustatyta, kad asmens duomenis galima teisėtai tvarkyti, jeigu juos tvarkyti „reikia dėl teisėtų interesų, kurių siekia duomenų valdytojas arba trečioji šalis (šalys), kurioms atskleidžiami duomenys, išskyrus atvejus, kai duomenų subjekto, kuriam <...> reikalinga apsauga, teisės ir laisvės yra viršesnės nei šie interesai".

Toliau nurodytame sprendime ESTT išsakė aiškią nuomonę dėl direktyvos 7 straipsnio f punkto.

Pavyzdys. Byloje *ASNEF ir FECEMD*[137] ESTT paaiškino, kad nacionalinėje teisėje negalima nustatyti papildomų teisėto duomenų tvarkymo sąlygų nei tos, kurios

135 *Ibid.*, 54, 58, 59, 66–68 punktai.

136 *Ibid.*, 78 ir 81 punktai.

137 2011 m. lapkričio 24 d. ESTT sprendimas *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C-468/10) ir Federación de Comercio Electrónico y Marketing Directo (FECEMD) (C-469/10) prieš Administración del Estado*, sujungtos bylos C-468/10 ir C-469/10.

numatytos direktyvos 7 straipsnio f punkte. Nagrinėjama situacija buvo susijusi su Ispanijos duomenų apsaugos įstatymo nuostata, pagal kurią kitos privačios šalys galėjo tvarkyti duomenis remdamosi teisėtu interesu, jeigu informacija buvo paskelbta viešosiose rinkmenose.

Teismas pirmiausia atkreipė dėmesį į tai, kad Direktyva 95/46 siekiama visose valstybėse narėse užtikrinti vienodą asmenų, kurių asmens duomenys tvarkomi, teisių ir laisvių apsaugos lygį. Todėl derinant šioje srityje taikytinus nacionalinius įstatymus negali būti nustatyta mažesnė šiais įstatymais užtikrinama apsauga. Jais turi būti siekiama užtikrinti aukštą apsaugos lygį ES[138]. Todėl ESTT nusprendė, jog „iš tikslo užtikrinti visose valstybėse narėse lygiavertį apsaugos lygį matyti, kad Direktyvos 95/46 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 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“[139]. Teismas taip pat nurodė, kad „atliekant palyginimą, būtiną pagal Direktyvos 95/46 7 straipsnio f punktą, galima atsižvelgti į tai, kad duomenų subjekto pagrindinių teisių apribojimo, kurį lemia jo duomenų tvarkymas, sunkumas gali skirtis, nelygu, ar atitinkami duomenys jau įtraukti į viešąją rinkmeną“.

Vis dėlto „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 interesų“.

Atsižvelgdamas į šiuos argumentus, Teismas padarė išvadą, jog „Direktyvos 95/46 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“[140].

138 *Ibid.*, 28 punktas. Žr. Duomenų apsaugos direktyvos 8 ir10 konstatuojamąsias dalis.

139 2011 m. lapkričio 24 d. ESTT sprendimo *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C-468/10) ir Federación de Comercio Electrónico y Marketing Directo (FECEMD) (C-469/10) prieš Administración del Estado*, sujungtos bylos C-468/10 ir C-469/10, 30 ir 32 punktai.

140 *Ibid.*, 40, 44, 48 ir 49 punktai.

Panašias formuluotes galima rasti ET rekomendacijose. Rekomendacijoje dėl profiliavimo pripažįstama, kad duomenų tvarkymas profiliavimo tikslais yra teisėtas, jei duomenis tvarkyti būtina siekiant kitų asmenų teisėtų interesų, „išskyrus atvejus, kai su duomenų subjektų pagrindinėmis teisėmis ir laisvėmis susiję interesai yra viršesni už tokius interesus“[141].

4.1.2. Teisėtas ypatingų duomenų tvarkymas

Pagal **ET teisę** tinkama naudojamų ypatingų duomenų apsauga nustatoma vidaus teisėje, o kalbant apie **ES teisę** pažymėtina, kad Duomenų apsaugos direktyvos 8 straipsnyje nustatytas išsamus duomenų, kurie atskleidžia rasinę arba etninę kilmę, politines, religines ar filosofines pažiūras, priklausymą profesinėms sąjungoms arba informaciją apie sveikatą ar intymų gyvenimą, kategorijų tvarkymo režimas. Iš esmės ypatingus duomenis tvarkyti draudžiama[142]. Tačiau direktyvos 8 straipsnio 2 ir 3 dalyse pateikiamas išsamus šio draudimo išimčių sąrašas. Šiose išimtyse nurodomas aiškus duomenų subjekto sutikimas, gyvybiniai interesai, kitų asmenų teisėti interesai arba viešasis interesas.

Kitaip nei neypatingų duomenų tvarkymo atveju, tariama, kad duomenų subjekto sutartiniais santykiais iš esmės negalima pagrįsti teisėto ypatingų duomenų tvarkymo. Todėl jeigu ypatingi duomenys turi būti tvarkomi atsižvelgiant į sutartį su duomenų subjektu, be sutikimo sudaryti sutartį, duomenų subjektas taip pat turi duoti aiškų sutikimą naudoti ypatingus duomenis. Tačiau aiškus duomenų subjekto prašymas dėl prekių ir paslaugų, kurias pristatant arba suteikiant būtina atskleisti ypatingus duomenis, turėtų būti prilyginamas aiškiam sutikimui.

Pavyzdys. Jeigu lėktuvu keliaujantis keleivis, užsakydamas skrydžio bilietus, prašo, kad oro bendrovė parūpintų vežimėlį neįgaliajam ir košerinį maistą, oro bendrovei leidžiama naudoti šiuos duomenis, net jeigu keleivis nepatvirtino papildomo sutikimo sąlygos, pagal kurią jis sutinka, kad būtų naudojama informacija, kuri atskleidžia jo sveikatą ir religines pažiūras.

Aiškus duomenų subjekto sutikimas

Pirmoji teisėto bet kokių duomenų (nepaisant to, ar tai neypatingi, ar ypatingi duomenys) tvarkymo sąlyga – duomenų subjekto sutikimas. Ypatingų duomenų atveju

141 Rekomendacijos dėl profiliavimo 3.4 straipsnio b punktas.

142 Duomenų apsaugos direktyvos 8 straipsnio 1 dalis.

toks sutikimas turi būti aiškus. Tačiau nacionalinėje teisėje gali būti numatyta, kad sutikimas naudoti ypatingus duomenis nėra pakankamas teisinis pagrindas, leidžiantis juos tvarkyti[143], pvz., kai išimtiniais atvejais dėl duomenų tvarkymo duomenų subjektui kyla neįprastas pavojus.

Vienu konkrečiu atveju pripažįstama, kad net ir netiesioginis sutikimas gali būti laikomas teisiniu pagrindu tvarkyti ypatingus duomenis: direktyvos 8 straipsnio 2 dalies e punkte nustatyta, kad nedraudžiama tvarkyti tokių duomenų, jei jie susiję su duomenimis, kuriuos duomenų subjektas yra akivaizdžiai paskelbęs viešai. Remiantis šia nuostata galima daryti aiškią prielaidą, kad duomenų subjekto veiksmas, kuriuo jis viešai paskelbia savo duomenis, turi būti aiškinamas kaip duomenų subjekto sutikimas naudoti tokius duomenis.

Gyvybiniai duomenų subjekto interesai

Kaip ir neypatingų duomenų atveju, ypatingus duomenis galima tvarkyti siekiant apsaugoti gyvybinius duomenų subjekto interesus[144].

Norint šiuo pagrindu teisėtai tvarkyti ypatingus duomenis, būtina tokia situacija, kai duomenų subjektui negalima pateikti klausimo dėl tokio duomenų tvarkymo, nes, pvz., jis buvo be sąmonės, jo nebuvo arba nebuvo įmanoma su juo susisiekti.

Teisėti kitų asmenų interesai

Kaip ir neypatingų duomenų atveju, kitų asmenų teisėti interesai gali būti pagrindu tvarkyti ypatingus duomenis. Tačiau Duomenų apsaugos direktyvos 8 straipsnio 2 dalyje nurodyta, kad ypatingi duomenys tokiomis aplinkybėmis gali būti tvarkomi tik šiais atvejais:

- kai duomenis tvarkyti būtina, kad būtų apsaugoti kito asmens gyvybiniai interesai[145], kai duomenų subjektas fiziškai neįgali arba yra juridiškai neveiksnus duoti sutikimą;

143 *Ibid.*, 8 straipsnio 2 dalies a punktas.

144 *Ibid.*, 8 straipsnio 2 dalies c punktas.

145 *Ibid.*

- kai ypatingi duomenys yra svarbūs darbo teisėje, pvz., sveikatos duomenys atsižvelgiant į ypač pavojingą darbą, arba duomenys apie religines pažiūras, kurie gali būti svarbūs darbuotojui suteikiant atostogas[146];

- kai fondas, asociacija ar kita pelno nesiekianti organizacija politiniais, filosofiniais, religiniais ar su profesinėmis sąjungomis susijusiais tikslais tvarko duomenis apie savo narius, rėmėjus ar kitas suinteresuotąsias šalis (tokie duomenys yra ypatingi, nes tikėtina, kad jie gali atskleisti atitinkamo asmens religines arba politines pažiūras)[147];

- kai ypatingi duomenys naudojami teismo arba administracinės institucijos nagrinėjamoje byloje siekiant nustatyti, įvykdyti ar apginti teisinį ieškinį[148].

- Be to, pagal Duomenų apsaugos direktyvos 8 straipsnio 3 dalį, kai duomenis apie sveikatą sveikatos priežiūros paslaugų teikėjai naudoja medicininės diagnostikos ir gydymo tikslais, šių paslaugų valdymas įtraukiamas į šią išimtį. Šioje nuostatoje įtvirtinta konkreti apsaugos priemonė, pagal kurią „sveikatos priežiūros paslaugas“ teikiantys asmenys tokiais pripažįstami tik tuo atveju, jeigu jiems taikomos konkrečios su konfidencialumo išsaugojimu susijusios profesinės pareigos.

Viešasis interesas

Be to, pagal Duomenų apsaugos direktyvos 8 straipsnio 4 dalį valstybės narės gali nustatyti papildomus tikslus, kuriais gali būti tvarkomi ypatingi duomenys, jeigu:

- duomenys tvarkomi dėl svarbaus viešojo intereso ir

- tokie tikslai numatyti nacionaliniame įstatyme arba priežiūros institucijos sprendime,

- nacionaliniame įstatyme arba priežiūros institucijos sprendime numatytos būtinos apsaugos priemonės, padedančios veiksmingai užtikrinti duomenų subjektų interesus[149].

146 *Ibid.*, 8 straipsnio 2 dalies b punktas.

147 *Ibid.*, 8 straipsnio 2 dalies d punktas.

148 *Ibid.*, 8 straipsnio 2 dalies e punktas.

149 *Ibid.*, 8 straipsnio 4 dalis.

Elektroninių sveikatos istorijų sistemos, kurias planuojama įdiegti daugumoje valstybių narių, yra geras pavyzdys. Tokiose sistemose su sveikatos priežiūros paslaugų teikėjų sveikatos duomenimis, surinktais gydant pacientą, gali susipažinti kiti sveikatos priežiūros paslaugų teikėjai. Iš esmės su šiais duomenimis gali susipažinti visi atitinkamos valstybės narės sveikatos priežiūros paslaugų teikėjai.

29 straipsnio duomenų apsaugos darbo grupė padarė išvadą, kad tokios sistemos, atsižvelgiant į galiojančias Duomenų apsaugos direktyvos 8 straipsnio 3 dalimi pagrįstas pacientų duomenų tvarkymo taisykles, negali būti kuriamos. Vis dėlto darant prielaidą, kad tokios elektroninių sveikatos istorijų sistemos atitinka svarbų viešąjį interesą, jas būtų galima pagrįsti direktyvos 8 straipsnio 4 dalimi ir reikalauti, kad jas kuriant būtų numatytas aiškus teisinis pagrindas, įskaitant būtinas apsaugos priemones, padedančias užtikrinti saugų sistemos veikimą[150].

4.2. Taisyklės duomenų tvarkymo saugumo

Pagrindiniai faktai

- Taisyklėse dėl tvarkymo saugumo duomenų valdytojui ir duomenų tvarkytojui nustatyta pareiga įgyvendinti tinkamas technines ir organizacines priemones, užkertančias kelią bet kokiam neteisėtam kišimuisi į duomenų tvarkymo operacijas.
- Būtinas duomenų saugumo lygis nustatomas atsižvelgiant į:
  - rinkoje prieinamas konkrečios duomenų tvarkymo rūšies saugumo priemones,
  - išlaidas ir
  - tvarkomų duomenų jautrumą.
- duomenų tvarkymo saugumas užtikrinamas bendra visiems asmenims, duomenų valdytojams arba duomenų tvarkytojams, išsaugoti duomenų konfidencialumą.

Todėl duomenų valdytojų ir duomenų tvarkytojų pareiga nustatyti tinkamas priemones, užtikrinančias duomenų saugumą, numatyta **ET ir ES duomenų apsaugos teisėje**.

150 29 straipsnio duomenų apsaugos darbo grupė (2007 m.), 2007 m. vasario 15 d. *Darbinis dokumentas dėl asmens sveikatos duomenų tvarkymo elektroninėse sveikatos istorijose (ESI)*, WP 131, Briuselis.

4.2.1. Duomenų saugumo aspektai

Atitinkamose **ES teisės** nuostatose nustatyta:

> *„Valstybės narės numato, kad duomenų valdytojas privalo įgyvendinti tinkamas technines ir organizacines priemones, skirtas apsaugoti, kad asmens duomenys nebūtų netyčia ar neteisėtai sunaikinti ar netyčia prarasti, pakeisti, neleistinai atskleisti ar palikti prieinami, ypač kai tvarkomus duomenis tenka perduoti tinklu, taip pat apsaugoti nuo bet kokių kitų neteisėtų tvarkymo būdų.“*[151]

Panaši nuostata įtvirtinta ir **ET teisėje**:

> *„Automatizuotai kaupiamiems asmens duomenims apsaugoti turi būti imtasi tinkamų apsaugos priemonių, kurios neleistų jų netyčia ar neteisėtai sunaikinti, netyčia prarasti, neleistinai palikti juos prieinamus, keisti ar platinti.“*[152]

Dažnai taip pat taikomi saugaus duomenų tvarkymo pramoniniai, nacionaliniai ir tarptautiniai standartai. Pavyzdžiui, Europos privatumo saugos ženklas (angl. EuroPriSe) yra ES eTEN (Transeuropinis telekomunikacijų tinklas) projekto dalis, kurį įgyvendinant nagrinėjamos produktų, visų pirma programinės įrangos, sertifikavimo galimybės, kurios atitiktų Europos duomenų apsaugos teisę. Europos tinklų ir informacijos apsaugos agentūra (angl. ENISA) sukurta siekiant padidinti ES, ES valstybių narių ir įmonių bendruomenės gebėjimus užkirsti kelią informacijos saugumo problemoms ir jas spręsti[153]. ENISA nuolat skelbia naujausių saugumo grėsmių analizes ir pataria, kaip jų išvengti.

Duomenų saugumas užtikrinamas ne tik turima tinkama – kompiuterine ir programine – įranga. Duomenų saugumui užtikrinti taip pat reikalingos tinkamos vidaus organizacinės taisyklės. Geriausiu atveju tokios vidaus taisyklės turėtų apimti šiuos klausimus:

151 Duomenų apsaugos direktyvos 17 straipsnio 1 dalis.

152 Konvencijos Nr. 108 7 straipsnis.

153 2004 m. kovo 10 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 460/2004, įsteigiantis Europos tinklų ir informacijos apsaugos agentūrą, OL L 77, 2004.

- reguliarų visų darbuotojų informavimą apie duomenų saugumo taisykles ir jų pareigas, nustatytas duomenų apsaugos teisėje, visų pirma susijusias su konfidencialumo išsaugojimu;

- aiškų atsakomybės padalijimą ir kompetencijos sprendžiant duomenų tvarkymo klausimus paskirstymą, visų pirma atsižvelgiant į sprendimus tvarkyti asmens duomenis ir teikti duomenis trečiosioms šalims;

- asmens duomenų naudojimą griežtai laikantis kompetentingo asmens nurodymų arba nustatytų bendrųjų taisyklių;

- patekimą į duomenų valdytojo arba duomenų tvarkytojo patalpas ir naudojimosi jo kompiuterine ir programine įranga apsaugą, įskaitant leidimų patekti į patalpas arba naudotis kompiuterine ir programine įranga patikrą;

- užtikrinimą, kad leidimus susipažinti su asmens duomenimis išduotų kompetentingas asmuo, ir reikalavimą, kad tokie leidimai būtų tinkamai fiksuojami dokumentuose;

- elektroniniais būdais suteikiamus automatizuotus galimybės susipažinti su asmens duomenimis protokolus ir reguliarias tokių protokolų patikras, kurias atlieka vidaus priežiūros pareigūnas;

- išsamų kitų duomenų atskleidimo formų (išskyrus automatizuotą galimybę susipažinti su duomenimis) dokumentavimą siekiant sudaryti sąlygas įrodyti, kad duomenys nebuvo teikiami neteisėtai.

Tinkamas darbuotojų mokymas ir švietimas duomenų saugumo tema taip pat yra veiksminga saugumo priemonių dalis. Taip pat turi būti nustatytos patikrinimo procedūros (pvz., vidaus arba išorės auditas) siekiant užtikrinti, kad tinkamos priemonės būtų ne tik nustatytos dokumentuose, bet ir praktiškai įgyvendinamos ir veiktų.

Duomenų valdytojas arba duomenų tvarkytojas, siekdamas didinti saugumo lygį, be kita ko, gali naudoti tokias priemones kaip asmens duomenų apsaugos pareigūnų pareigybės nustatymas, darbuotojų švietimas duomenų saugumo tema, reguliaraus audito atlikimas, įsibrovimo į saugumo sistemas bandymai ir kokybės antspaudai.

Pavyzdys. Byloje *I. prieš Suomiją*[154] pareiškėja negalėjo įrodyti, kad kiti ligoninės, kurioje ji dirbo, darbuotojai, neteisėtai susipažino su jos ligos istorija. Todėl vidaus teismas atmetė jos ieškinį dėl teisės į duomenų apsaugą pažeidimo. EŽTT nusprendė, jog EŽTK 8 straipsnis buvo pažeistas, nes ligoninėje naudojama 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“. Pagrindinė aplinkybė, į kurią atsižvelgė Teismas, buvo tai, kad ligoninėje veikianti ligos istorijų sistema akivaizdžiai neatitiko vidaus teisėje nustatytų teisinių reikalavimų, ir vidaus teismai tinkamai neatsižvelgė į šią aplinkybę.

Pranešimai apie duomenų saugumo pažeidimą

Keliose Europos šalyse nustatyta nauja priemonė, susijusi su duomenų saugumo pažeidimais, t. y. elektroninių ryšių paslaugų teikėjų pareiga pranešti tikėtinoms aukoms ir priežiūros institucijoms apie duomenų saugumo pažeidimus. Tai yra ES teisėje telekomunikacijų paslaugų teikėjams nustatyta pareiga[155]. Duomenų subjektams teikiant pranešimus apie duomenų saugumo pažeidimą siekiama išvengti žalos: pranešimas apie duomenų saugumo pažeidimus ir tikėtinas jų pasekmes padeda sumažinti neigiamų padarinių duomenų subjektui pavojų. Paslaugų teikėjams taip pat gali būti skiriamos baudos už didelį neatsargumą.

Siekiant veiksmingai valdyti pranešimus apie duomenų saugumo pažeidimus ir juos teikti, reikės iš anksto nustatyti vidaus procedūras, nes nacionalinėje teisėje nustatytas terminas, per kurį reikia informuoti duomenų subjektus ir (arba) priežiūros instituciją, yra gana trumpas.

154 2008 m. liepos 17 d. EŽTT sprendimas *I. prieš Suomiją*, Nr. 20511/03.

155 Žr. 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyvos 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (*Direktyva dėl privatumo ir elektroninių ryšių*), OL L 201, 2002, 4 straipsnio 3 dalį, iš dalies pakeistą 2009 m. lapkričio 25 d. Europos Parlamento ir Tarybos direktyva 2009/136/EB, iš dalies keičiančia 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.

4.2.2. Konfidencialumas

Pagal ES teisę saugus duomenų tvarkymas yra papildomai užtikrinamas visiems asmenims, duomenų valdytojams arba duomenų tvarkytojams, nustačius bendrą pareigą užtikrinti duomenų konfidencialumą.

Pavyzdys. Draudimo bendrovės darbuotojui darbo metu paskambina asmuo, kuris teigia esąs bendrovės klientas, ir prašo pateikti informaciją apie savo draudimo sutartį.

Vadovaudamasis pareiga išsaugoti kliento duomenų konfidencialumą, darbuotojas, prieš atskleisdamas asmens duomenis, turi taikyti bent minimalias saugumo priemones. Tai, pvz., galima padaryti pasiūlant perskambinti kliento draudimo sutartyje nurodytu telefonu.

Duomenų apsaugos direktyvos 16 straipsnyje konfidencialumo pareiga aptariama atsižvelgiant tik į duomenų valdytojo ir duomenų tvarkytojo santykius. Direktyvos 7 ir 8 straipsniuose aptariama, ar duomenų valdytojai turi išsaugoti duomenų konfidencialumą, atsižvelgiant į tai, kad jie tokių duomenų negali atskleisti trečiosioms šalims.

Konfidencialumo pareiga netaikoma tais atvejais, kai asmuo su asmens duomenimis susipažįsta kaip privatus asmuo, o ne duomenų valdytojo arba duomenų tvarkytojo darbuotojas. Šiuo atveju Duomenų apsaugos direktyvos 16 straipsnis netaikomas, nes direktyva apskritai netaikoma, kai asmens duomenis naudoja privatūs asmenys ir toks naudojimas patenka į šeimai taikomos išimties taikymo sritį[156]. Šeimai taikoma išimtis yra susijusi su asmens duomenų naudojimu, kai „duomenis tvarko fizinis asmuo, užsiimdamas tik asmenine ar namų ūkio veikla“[157]. Tačiau, atsižvelgiant į ESTT sprendimą byloje *Bodil Lindqvist*[158], ši išimtis turi būti aiškinama siaurai, visų pirma kai kalbama apie duomenų atskleidimą. Pažymėtina, kad šeimai taikoma išimtis nebus taikoma asmens duomenis paskelbiant neribotam duomenų gavėjų skaičiui internete (išsamesnė informacija apie bylą pateikiama 2.1.2, 2.2, 2.3.1 ir 6.1 dalyse).

156 Duomenų apsaugos direktyvos 3 straipsnio 2 dalies antra įtrauka.

157 *Ibid.*

158 2003 m. lapkričio 6 d. ESTT sprendimas *Bodil Lindqvist*, C-101/01.

ET teisėje konfidencialumo pareiga netiesiogiai įtvirtinta Konvencijos Nr. 108 7 straipsnio, reglamentuojančio duomenų saugumą, duomenų saugumo sąvokoje.

Duomenų tvarkytojų konfidencialumo pareiga reiškia, kad jie gali naudoti jiems duomenų valdytojo pateiktus asmens duomenis tik laikydamiesi duomenų valdytojo nurodymų. Duomenų valdytojo arba duomenų tvarkytojo darbuotojų konfidencialumo pareiga reiškia, kad jie asmens duomenis turi naudoti vadovaudamiesi tik kompetentingų savo vadovų nurodymais.

Konfidencialumo pareiga 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 konfidencialumo pareigą. Paprastai ši pareiga nustatoma į darbuotojo darbo sutartį įtraukiant konfidencialumo sąlygas.

Daugumos ES valstybių narių ir Konvencijos Nr. 108 šalių baudžiamojoje teisėje numatyta atsakomybė už profesinių konfidencialumo pareigų pažeidimą.

4.3. Skaidraus duomenų tvarkymo taisyklės

Pagrindiniai faktai

- Prieš pradėdamas tvarkyti asmens duomenis duomenų valdytojas turi bent jau pranešti duomenų subjektams savo pavadinimą ir duomenų tvarkymo tikslą, išskyrus atvejus, kai duomenų subjektas jau turi tokią informaciją.
- Kai duomenys renkami iš trečiųjų šalių, pareiga pranešti netaikoma, jeigu:
  - duomenų tvarkymas numatytas įstatyme arba
  - paaiškėja, kad neįmanoma pateikti informacijos arba tam prireiktų neproporcingų pastangų.
- Be to, prieš pradėdamas tvarkyti asmens duomenis duomenų valdytojas turi:
  - informuoti priežiūros instituciją apie ketinamas atlikti tvarkymo operacijas arba
  - nustatyti, kad nepriklausomas asmens duomenų apsaugos pareigūnas organizacijos viduje dokumentuos tvarkymo operacijas, jeigu nacionaliniame įstatyme numatyta tokia procedūra.

Pagal sąžiningo duomenų tvarkymo principą reikalaujama užtikrinti skaidrų tvarkymą. Šiuo tikslu **ET teisėje** nustatyta, kad visiems asmenims turi būti suteikta galimybė žinoti, ar yra duomenų tvarkymo rinkmena, jos tikslą ir atsakingą duomenų valdytoją[159]. Tokios galimybės suteikimo tvarka turėtų būti nustatoma vidaus teisėje. **ES teisėje** šis klausimas reglamentuojamas išsamiau: skaidrumas duomenų subjekto atžvilgiu užtikrinamas nustačius duomenų valdytojui pareigą informuoti duomenų subjektą ir visuomenę apskritai.

Vadovaujantis abiem teisinėmis sistemomis, nacionalinėje teisėje galima nustatyti duomenų valdytojo skaidrumo pareigų išimtis ir apribojimus, jei toks apribojimas yra būtinas siekiant apsaugoti tam tikrus viešuosius interesus, duomenų subjektą arba kitų asmenų teises ir laisves ir jeigu tai yra būtina demokratinėje visuomenėje[160]. Tokios išimtys, pvz., gali būti reikalingos tiriant nusikaltimą, tačiau jos gali būti pateisinamos ir kitokiomis aplinkybėmis.

4.3.1. Informavimas

Pagal ET ir ES teisę tvarkymo operacijas atliekantys duomenų valdytojai turi pareigą iš anksto informuoti duomenų subjektą apie tai, kad jie ketina tvarkyti duomenis[161]. Ši pareiga nepriklauso nuo duomenų subjekto prašymo ir duomenų valdytojas turi aktyviai jos laikytis, nepaisant to, ar duomenų subjektas rodo suinteresuotumą gauti informaciją, ar ne.

Informacijos turinys

Pateikiant informaciją turi būti nurodomas duomenų tvarkymo tikslas, taip pat duomenų valdytojo tapatybė ir kontaktiniai duomenys[162]. Duomenų apsaugos direktyvoje reikalaujama pateikti išsamesnę informaciją, kai jos „reikia, atsižvelgus į specifines duomenų tvarkymo aplinkybes, kad būtų garantuotas teisingas subjekto duomenų tvarkymas“. Direktyvos 10 ir 11 straipsniuose, be kita ko, nurodomos tvarkomų duomenų kategorijos ir tokių duomenų gavėjai, taip pat teisė susipažinti su savo asmens duomenimis ir juos ištaisyti. Kai duomenys renkami iš duomenų

159 Konvencijos Nr. 108 8 straipsnio a punktas.

160 *Ibid.*, 9 straipsnio 2 dalis ir Duomenų apsaugos direktyvos 13 straipsnio 1 dalis.

161 Konvencijos Nr. 108 8 straipsnio a punktas ir Duomenų apsaugos direktyvos 10 ir 11 straipsniai.

162 Konvencijos Nr. 108 8 straipsnio a punktas ir Duomenų apsaugos direktyvos 10 straipsnio a ir b punktai.

subjektų, pateikiamoje informacijoje turėtų būti paaiškinama, ar būtina atsakyti į pateiktus klausimus, taip pat pasekmės, galinčios atsirasti nepateikus atsakymų[163].

Pagal **ET teisę** tokios informacijos teikimas gali būti laikomas gerąja patirtimi, atsižvelgiant į sąžiningo duomenų tvarkymo principą, ir šiuo požiūriu toks informacijos teikimas yra ET teisės sudedamoji dalis.

Sąžiningo duomenų tvarkymo principas reiškia, kad duomenų subjektams turi būti pateikiama lengvai suprantama informacija. Vartojama kalba turi būti pritaikyta tikslinei grupei. Vartojamos kalbos pobūdis ir rūšis turėtų būti kitokia atsižvelgiant į tai, ar tikslinė grupė yra, pvz., suaugę asmenys ar vaikai, visuomenė apskritai ar aukštąjį išsilavinimą turintys ekspertai.

Kai kurie duomenų subjektai gali pageidauti gauti tik glaustą informaciją apie tai, kaip ir kodėl tvarkomi jų duomenys, o kiti prašys pateikti išsamų paaiškinimą. Šis sąžiningo informacijos pateikimo aspektas aptartas 29 straipsnio duomenų apsaugos darbo grupės nuomonėje, kurioje raginama naudoti keliais lygmenimis pateikiamą informaciją[164], nes toks informacijos pateikimo būdas sudaro sąlygas duomenų subjektui pačiam pasirinkti norimą informacijos išsamumo lygį.

Informacijos pateikimo laikas

Duomenų apsaugos direktyvoje nustatytos šiek tiek kitokios nuostatos, susijusios su informacijos pateikimo laiku. Tai priklauso nuo to, ar duomenys renkami iš duomenų subjektų (10 straipsnis) ar trečiosios šalies (11 straipsnis). Kai duomenys renkami iš duomenų subjekto, informacija turi būti pateikiama ne vėliau kaip duomenų rinkimo metu. Kai duomenys renkami iš trečiųjų šalių, informacija turi būti pateikiama ne vėliau kaip iki to laiko, kai duomenys imami užrašinėti arba prieš atskleidžiant duomenis trečiajai šaliai pirmą kartą.

Pareigos teikti informaciją išimtys

ES teisėje numatyta bendra pareigos informuoti duomenų subjektą išimtis, kuri taikoma tuomet, kai duomenų subjektas jau turi informaciją[165]. Tai apima atvejus, kai

163 Duomenų apsaugos direktyvos 10 straipsnio c punktas.

164 29 straipsnio duomenų apsaugos darbo grupė (2004 m.), 2004 m. lapkričio 29 d. *Nuomonė Nr. 10/2004 dėl labiau suderintų informacijos nuostatų*, WP 100, Briuselis.

165 Duomenų apsaugos direktyvos 10 straipsnis ir 11 straipsnio 1 dalis.

duomenų subjektas, atsižvelgdamas į konkretaus atvejo aplinkybes, žino, kad tam tikras duomenų valdytojas jo duomenis tvarkys tam tikru tikslu.

Direktyvos 11 straipsnyje, kuris susijęs su pareiga informuoti duomenų subjektą tuo atveju, kai duomenys gauti ne iš jo, taip pat nurodyta, kad tokia pareiga netaikoma, visų pirma duomenis tvarkant statistikos, istoriniais arba mokslo tikslais, kai:

- paaiškėja, kad tokios informacijos pateikti neįmanoma, arba
- informacijai pateikti prireiktų neproporcingų pastangų, arba
- duomenų užrašymo arba atskleidimo atvejai aiškiai nustatyti įstatyme[166].

Tik Duomenų apsaugos direktyvos 11 straipsnio 2 dalyje nurodyta, kad duomenų subjektų nereikia informuoti apie tvarkymo operacijas, jeigu jos numatytos įstatyme. Atsižvelgiant į bendrąją teisinę prielaidą, kad asmenys žino apie jiems taikomą įstatymą, būtų galima teigti, kad tais atvejais, kai duomenys iš duomenų subjekto renkami pagal direktyvos 10 straipsnį, duomenų subjektas apie tai žino. Tačiau, atsižvelgiant į tai, kad žinojimas apie įstatymą tėra numanomas, vadovaujantis sąžiningo duomenų tvarkymo principu, reikėtų teigti, kad pagal 10 straipsnį duomenų subjektas turi būti informuojamas net jeigu tvarkymo operacijos numatytos įstatyme. Šiuo atveju būtina atsižvelgti į tai, kad duomenų subjekto informavimui nereikia ypač daug pastangų, nes duomenys renkami tiesiogiai iš duomenų subjekto.

Kalbant apie ET teisę pažymėtina, kad Konvencijoje Nr. 108 aiškiai numatytos šios Konvencijos 8 straipsnio išimtys. Be to, galima teigti, kad Duomenų apsaugos direktyvos 10 ir 11 straipsniuose numatytomis išimtimis gali būti vadovaujamasi kaip gerosios patirties pavyzdžiais taikant Konvencijos Nr. 108 9 straipsnyje numatytas išimtis.

Skirtingi informacijos teikimo būdai

Idealiausiu atveju žodinė arba rašytinė informacija turėtų būti teikiama kiekvienam duomenų subjektui. Jeigu duomenys renkami iš duomenų subjekto, informacija turėtų būti teikiama tuo metu, kai renkami duomenys. Tačiau kai duomenys renkami iš trečiųjų šalių, atsižvelgiant į akivaizdžias praktines problemas bandant asmeniškai

166 *Ibid.*, 40 konstatuojamoji dalis ir 11 straipsnio 2 dalis.

susisiekti su duomenų subjektais, informacija taip pat gali būti pateikiama atitinkamame leidinyje.

Vienas veiksmingiausių būdų teikti informaciją – duomenų valdytojo pradžios tinklalapyje pateikti tinkamas informacijos naudojimo sąlygas, pvz., nurodyti svetainės privatumo taisykles. Vis dėlto nemažai gyventojų nesinaudoja internetu, todėl įmonė arba valdžios institucija, rengdama savo informacijos naudojimo t, turėtų į tai atsižvelgti.

4.3.2. Pranešimas

Nacionalinėje teisėje duomenų valdytojams gali būti nustatyta pareiga informuoti kompetentingą priežiūros instituciją apie duomenų valdytojo atliekamas tvarkymo operacijas, kad jas būtų galima paskelbti. Kita vertus, nacionalinėje teisėje gali būti nustatyta, kad duomenų valdytojai gali įdarbinti asmens duomenų apsaugos pareigūną, kuris visų pirma atsako už duomenų valdytojo atliekamų tvarkymo operacijų registro tvarkymą[167]. Gyventojo prašymu jam turi būti leidžiama susipažinti su šiuo vidaus registru.

Pavyzdys. Vidaus asmens duomenų apsaugos pareigūno pranešime ir dokumentuose būtina aprašyti pagrindinius atitinkamos duomenų tvarkymo operacijos požymius. Tai informacija apie duomenų valdytoją, duomenų tvarkymo tikslą, tvarkymo teisinį pagrindą, tvarkomų duomenų kategorijas, tikėtinas trečiąsias šalis, kurioms gali būti teikiami duomenys, taip pat tai, ar numatyti valstybės sienas kertančių duomenų srautai, ir, jei taip, kokie jie bus.

Priežiūros institucija pranešimus turi skelbti specialiame registre. Siekiant šio tikslo, reikia užtikrinti paprastą ir nemokamą galimybę susipažinti su registru. Tą patį galima pasakyti apie duomenų valdytojo asmens duomenų apsaugos pareigūno laikomus dokumentus.

Pareigos pranešti kompetentingai priežiūros institucijai arba įdarbinti vidaus duomenų apsaugos pareigūną išimtys, atsižvelgiant į Duomenų apsaugos direktyvos 18 straipsnio 2 dalį, gali būti numatytos nacionaliniame įstatyme. Šios išimtys gali būti taikomos duomenų tvarkymo operacijoms, dėl kurių, kaip tikimasi, duomenų subjektams nekils konkretaus pavojaus[168].

167 *Ibid.*, 18 straipsnio 2 dalies antra įtrauka.

168 *Ibid.*, 18 straipsnio 2 dalies pirma įtrauka.

4.4. Atitikties skatinimo taisyklės

Pagrindiniai faktai

- Plėtojant atskaitomybės principą, Duomenų apsaugos direktyvoje nurodomos kelios priemonės, padedančios skatinti atitiktį:
  - nacionalinės priežiūros institucijos atliekama išankstinė planuojamų duomenų tvarkymo operacijų patikra;
  - asmens duomenų apsaugos pareigūnai, kurie teikia duomenų valdytojui specialiąsias žinias duomenų apsaugos srityje;
  - elgesio kodeksai, kuriuose konkrečiai nurodomos galiojančios duomenų apsaugos taisyklės, kurias taiko konkreti visuomenės grupė, pvz., verslininkai.
- ET teisėje, pvz., Rekomendacijoje dėl profiliavimo, numatytos panašios atitikties skatinimo priemonės.

4.4.1. Išankstinė patikra

Pagal Duomenų apsaugos direktyvos 20 straipsnį priežiūros institucija, prieš pradėdama atlikti duomenų tvarkymo operacijas, turi patikrinti tas tvarkymo operacijas, kurios dėl tvarkymo tikslo arba aplinkybių gali kelti konkretų pavojų duomenų subjektų teisėms ir laisvėms. Nacionalinėje teisėje turi būti nustatyta, kurios duomenų tvarkymo operacijos turi būti iš anksto tikrinamos. Atlikus tokias patikras, tvarkymo operacijas gali būti draudžiama atlikti arba tai gali būti daroma siekiant pakeisti siūlomos tvarkymo operacijos pobūdį. Direktyvos 20 straipsnio tikslas – atsižvelgiant į tai, kad priežiūros institucija turi įgaliojimus uždrausti duomenų tvarkymo operacijas, užtikrinti, kad nepagrįstai pavojingos operacijos net nebūtų pradedamos. Kad šis mechanizmas būtų veiksmingas, būtina laikytis vienos sąlygos, t. y. faktiškai informuoti priežiūros instituciją. Siekiant užtikrinti, kad duomenų valdytojai vykdytų pareigą pranešti, priežiūros institucijoms turės būti suteikti įgaliojimai taikyti priverstines priemones, pvz., skirti baudas duomenų valdytojams.

Pavyzdys. Jeigu įmonė atlieka tvarkymo operacijas, kurioms pagal nacionalinę teisę taikoma išankstinė patikra, ji turi pateikti priežiūros institucijai dokumentus, susijusius su planuojamomis tvarkymo operacijomis. Įmonei neleidžiama pradėti tvarkymo operacijų, kol joms nepritarė priežiūros institucija.

Kai kurių valstybių narių nacionalinėje teisėje taip pat numatyta, kad tvarkymo operacijos gali būti pradedamos, jeigu per tam tikrą terminą, pvz., tris mėnesius, priežiūros institucija nepateikia jokio atsakymo.

4.4.2. Asmens duomenų apsaugos pareigūnai

Duomenų apsaugos direktyvoje nustatyta galimybė nacionalinėje teisėje numatyti, kad duomenų valdytojai gali paskirti pareigūną, einantį asmens duomenų apsaugos pareigūno pareigas[169]. Šios pareigybės tikslas – užtikrinti, kad duomenų tvarkymo operacijos nedarytų neigiamo poveikio duomenų subjektų teisėms ir laisvėms[170].

Pavyzdys. Pagal Vokietijos federalinio duomenų apsaugos įstatymo (vok. *Bundesdatenschutzgesetz*) 4f straipsnio 1 dalį reikalaujama, kad privačios įmonės paskirtų vidaus asmens duomenų apsaugos pareigūną, jeigu jose automatiškai asmens duomenis nuolat tvarko 10 arba daugiau įdarbintų asmenų.

Siekiant sudaryti galimybes pasiekti šį tikslą būtina užtikrinti tam tikrą duomenų valdytojo organizacijoje dirbančio pareigūno nepriklausomumo laipsnį, kaip tai aiškiai nurodyta direktyvoje. Tvirtos su įdarbinimu susijusios teisės, kurios padeda apsisaugoti nuo įvairių atsitiktinumų, pvz., nepagrįsto atleidimo iš darbo, taip pat būtinos siekiant užtikrinti veiksmingą šio pareigūno darbą.

Siekiant didinti atitiktį nacionalinei duomenų apsaugos teisei, vidaus asmens duomenų apsaugos pareigūnų sąvoka taip pat patikslinta kai kuriose ET rekomendacijose[171].

4.4.3. Elgesio kodeksai

Siekdamos didinti atitiktį, įmonės ir kitų sektorių dalyviai gali parengti išsamias taisykles, reglamentuojančias jų įprastą duomenų tvarkymo veiklą, ir taip kodifikuoti geriausią patirtį. Sektoriaus narių specialiosios žinios padės rasti praktinius sprendimus, kurių, tikėtina, bus paisoma. Todėl valstybės narės ir Europos Komisija raginamos skatinti rengti elgesio kodeksus, kuriais ketinama padėti tinkamai įgyvendinti

169 *Ibid.*, 18 straipsnio 2 dalies antra įtrauka.

170 *Ibid.*

171 Žr., pvz., Rekomendacijos dėl profiliavimo 8.3 straipsnį.

valstybių narių pagal direktyvą priimtas nacionalines nuostatas ir kuriuose būtų atsižvelgiama į įvairių sektorių specifiką[172].

Siekdamos užtikrinti šių elgesio kodeksų atitiktį pagal Duomenų apsaugos direktyvą priimtoms nacionalinėms nuostatoms, valstybės narės turi nustatyti kodeksų vertinimo tvarką. Paprastai būtų reikalaujama, kad šioje vertinimo procedūroje dalyvautų nacionalinė institucija, prekybos asociacijos ir kitos įstaigos, kurios atstovauja kitų kategorijų duomenų valdytojams[173].

Bendrijos elgesio kodeksų projektai ir galiojančių Bendrijos elgesio kodeksų pakeitimai arba papildymai gali būti teikiami vertinti 29 straipsnio duomenų apsaugos darbo grupei. Gavusi šios darbo grupės pritarimą, Europos Komisija gali užtikrinti tinkamą tokių elgesio kodeksų viešinimą[174].

Pavyzdys. Europos tiesioginės ir interaktyvios rinkodaros federacija (angl. FEDMA) parengė Europos praktikos kodeksą dėl asmens duomenų naudojimo tiesioginei rinkodarai. Kodeksas sėkmingai pateiktas 29 straipsnio duomenų apsaugos darbo grupei. 2010 m. kodeksas papildytas priedu dėl elektroninių rinkodaros ryšių[175].

172 Žr. Duomenų apsaugos direktyvos 27 straipsnio 1 dalį.

173 *Ibid.*, 27 straipsnio 2 dalis.

174 *Ibid.*, 27 straipsnio 3 dalis.

175 29 straipsnio duomenų apsaugos darbo grupė (2010 m.), 2010 m. liepos 13 d. *Nuomonė Nr. 4/2010 dėl Europos tiesioginės rinkodaros asociacijų federacijos (FEDMA) Europos elgesio kodekso dėl asmens duomenų naudojimo tiesioginei rinkodarai*, WP 174, Briuselis.

5

Duomenų subjekto teisės ir jų vykdymo užtikrinimas

ES	Aptariami klausimai	ET
Teisė susipažinti		
Duomenų apsaugos direktyvos 12 straipsnis. 2009 m. gegužės 7 d. ESTT sprendimas *College van burgemeester en wethouders van Rotterdam prieš M.E.E. Rijkeboer*, C-553/07.	**Teisė susipažinti su savo asmens duomenimis.**	Konvencijos Nr. 108 8 straipsnio b punktas.
	Teisė reikalauti, kad duomenys būtų ištaisyti, sunaikinti (ištrinti) arba užblokuoti.	Konvencijos Nr. 108 8 straipsnio c punktas. 2008 m. lapkričio 18 d. EŽTT sprendimas *Cemalettin Canli prieš Turkiją*, Nr. 22427/04. 2006 m. birželio 6 d. EŽTT sprendimas *Segerstedt-Wiberg ir kiti prieš Švediją*, Nr. 62332/00. 2010 m. balandžio 27 d. EŽTT sprendimas *Ciubotaru prieš Moldovą*, Nr. 27138/04.
Teisė nesutikti		
Duomenų apsaugos direktyvos 14 straipsnio 1 dalies a punktas.	**Teisė nesutikti atsižvelgiant į konkrečią duomenų subjekto padėtį.**	Rekomendacijos dėl profiliavimo 5.3 straipsnis.

Duomenų apsaugos direktyvos 14 straipsnio 1 dalies b punktas.	**Teisė nesutikti su tolesniu duomenų naudojimu rinkodaros tikslais.**	Rekomendacijos dėl tiesioginės rinkodaros 4.1 straipsnis.
Duomenų apsaugos direktyvos 15 straipsnis.	**Teisė nesutikti su automatiniais sprendimais.**	Rekomendacijos dėl profiliavimo 5.5 straipsnis.
Nepriklausoma priežiūra		
Chartijos 8 straipsnio 3 dalis. Duomenų apsaugos direktyvos 28 straipsnis. ES institucijų duomenų apsaugos reglamento V skyrius. Duomenų apsaugos reglamentas. 2010 m. kovo 9 d. ESTT sprendimas *Europos Komisija prieš Vokietijos Federacinę Respubliką*, C-518/07. 2012 m. spalio 16 d. ESTT sprendimas *Europos Komisija prieš Austrijos Respubliką*, C-614/10. 2012 m. birželio 8 d. ESTT sprendimas *Europos Komisija prieš Vengriją*, C-288/12, 2014 m. balandžio 8 d.	**Nacionalinės priežiūros institucijos.**	Konvencijos Nr. 108 papildomo protokolo 1 straipsnis.
Teisių gynimo būdai ir sankcijos		
Duomenų apsaugos direktyvos 12 straipsnis.	**Duomenų valdytojo prašymas.**	Konvencijos Nr. 108 8 straipsnio b punktas.
Duomenų apsaugos direktyvos 28 straipsnio 4 dalis. ES institucijų duomenų apsaugos reglamento 32 straipsnio 2 dalis.	**Priežiūros institucijai pateikti reikalavimai.**	Konvencijos Nr. 108 papildomo protokolo 1 straipsnio 2 dalies b punktas.
Chartijos 47 straipsnis.	**Teismai (apskritai).**	EŽTK 13 straipsnis.
Duomenų apsaugos direktyvos 28 straipsnio 3 dalis.	**Nacionaliniai teismai.**	Konvencijos Nr. 108 papildomo protokolo 1 straipsnio 4 dalis.
SESV 263 straipsnio 4 dalis. ES institucijų duomenų apsaugos reglamento 32 straipsnio 1 dalis. SESV 267 straipsnis.	**ESTT.**	
	EŽTT.	EŽTK 34 straipsnis.

Teisių gynimo būdai ir sankcijos		
Chartijos 47 straipsnis. Duomenų apsaugos direktyvos 22 ir 23 straipsniai. 1984 m. balandžio 10 d. ESTT sprendimas *Sabine von Colson ir Elisabeth Kamann prieš Land Nordrhein-Westfalen*, C-14/83. 1986 m. vasario 26 d. ESTT sprendimas *M. H. Marshall prieš Southampton ir South-West Hampshire Area Health Authority*, C-152/84.	**Dėl nacionalinės duomenų apsaugos teisės pažeidimų.**	EŽTK 13 straipsnis (tik ET valstybėms narėms). Konvencijos Nr. 108 10 straipsnis. 2008 m. kovo 2 d. EŽTT sprendimas *K. U. prieš Suomiją*, Nr. 2872/02. 2008 m. lapkričio 25 d. EŽTT sprendimas *Biriuk prieš Lietuvą*, Nr. 23373/03.
ES institucijų duomenų apsaugos reglamento 34 ir 49 straipsniai. 2010 m. birželio 29 d. ESTT sprendimas *Europos Komisija prieš The Bavarian Lager Co. Ltd*, C-28/08 P.	**Dėl ES institucijų ir įstaigų padarytų pažeidimų.**	

Teisės taisyklių apskritai, o ypač duomenų subjektų teisių, veiksmingumas labai priklauso nuo to, ar nustatyti tinkami jų vykdymo užtikrinimo mechanizmai. Pagal Europos duomenų apsaugos teisę duomenų subjektui nacionaliniu įstatymu turi būti suteikti įgaliojimai apsaugoti savo duomenis. Nacionaliniu įstatymu taip pat turi būti sukurtos nepriklausomos priežiūros institucijos, kurios padėtų duomenų subjektams įgyvendinti savo teises ir prižiūrėtų, kaip tvarkomi asmens duomenys. Be to, kadangi EŽTK ir Chartijoje garantuojama teisė pasinaudoti veiksmingomis teisių gynimo priemonėmis, būtina užtikrinti, kad kiekvienas asmuo galėtų pasinaudoti teisminėmis teisių gynimo priemonėmis.

5.1. Duomenų subjektų teisės

Pagrindiniai faktai

- Nacionalinėje teisėje kiekvienam asmeniui turi būti numatyta teisė prašyti, kad bet kuris duomenų valdytojas pateiktų informaciją apie tai, ar jis tvarko jo duomenis.
- Pagal nacionalinę teisę duomenų subjektai turi teisę:
  - susipažinti su savo asmens duomenimis, kuriuos tvarko bet kuris duomenų valdytojas;
  - prašyti, kad jų duomenis tvarkantis duomenų valdytojas ištaisytų (arba, kai tinkama, užblokuotų) duomenis, jeigu jie netikslūs;

- prašyti, kad duomenų valdytojas atitinkamai sunaikintų arba užblokuotų jų duomenis, jeigu duomenų valdytojas jų duomenis tvarko neteisėtai.

- Be to, duomenų subjektai turi teisę nesutikti, kad duomenų valdytojas:
  - priimtų automatizuotus sprendimus (kurie priimami asmens duomenis tvarkant tik automatiniais būdais);
  - tvarkytų jų duomenis, jeigu dėl to atsiranda neproporcingi rezultatai;
  - naudotų jų duomenis tiesioginės rinkodaros tikslais.

5.1.1. Prieigos teisė

Kalbant apie **ES teisę** pažymėtina, kad Duomenų apsaugos direktyvos 12 straipsnyje nustatyti teisės susipažinti elementai, įskaitant teisę gauti iš duomenų valdytojo „patvirtinimą, ar su juo susiję duomenys yra tvarkomi, ir informaciją bent jau apie tvarkymo tikslus, duomenų kategorijas, gavėjus, kuriems atskleidžiami duomenys, arba jų kategorijas“, taip pat, kad duomenų valdytojas „ištaisytų, ištrintų arba blokuotų duomenis, kurie tvarkomi nesilaikant šios direktyvos nuostatų, o ypač, kai tie duomenys yra neišsamūs ar netikslūs“.

ET teisėje nustatytos tokios pačios teisės ir jos turi būti numatytos vidaus teisėje (Konvencijos Nr. 108 8 straipsnis). Kai kuriose ET rekomendacijose vartojama sąvoka „susipažinti“, be to, aprašomi įvairūs teisės susipažinti aspektai, kuriuos vidaus teisėje įgyvendinti siūloma taip, kaip nurodyta pirmiau.

Pagal Konvencijos Nr. 108 9 straipsnį ir Duomenų apsaugos direktyvos 13 straipsnį duomenų valdytojų pareiga priimti sprendimą dėl duomenų subjekto prašymo susipažinti gali būti apribojama dėl viršesnių kitų asmenų teisinių interesų. Viršesni teisiniai interesai gali būti susiję su viešuoju interesu, pvz., nacionaliniu saugumu, visuomenės saugumu ir nusikalstamų veikų baudžiamuoju persekiojimu, taip pat privačiais interesais, kurie yra svarbesni už duomenų apsaugos interesus. Bet kokios išimtys arba apribojimai turi būti būtini demokratinėje visuomenėje ir proporcingi siekiamam tikslui. Tik išimtiniais atvejais, pvz., dėl ligos simptomų, duomenų subjekto apsaugos skaidrumas gali būti ribojamas; tai visų pirma susiję su kiekvieno duomenų subjekto teise susipažinti.

Kai duomenys tvarkomi tik mokslinių tyrimų arba statistiniais tikslais, Duomenų apsaugos direktyvoje numatyta galimybė teises susipažinti apriboti nacionalinėje teisėje; tačiau tokiu atveju taip pat turi būti nustatomos tinkamos teisinės apsaugos

priemonės. Visų pirma būtina užtikrinti, kad jokios priemonės arba sprendimai, susiję su kuriuo nors konkrečiu asmeniu, nebūtų priimami tvarkant tokius duomenis ir kad „nėra jokio pavojaus pažeisti duomenų subjekto privatumą“[176]. Panašios nuostatos numatytos Konvencijos Nr. 108 9 straipsnio 3 dalyje.

Teisė susipažinti su savo asmens duomenimis

Pagal ET teisę teisė susipažinti su savo asmens duomenimis aiškiai numatyta Konvencijos Nr. 108 8 straipsnyje. EŽTT ne kartą yra nusprendęs, kad esama teisės susipažinti su asmens duomenimis, kuriuos turi arba naudoja kiti asmenys, ir kad ši teisė atsiranda dėl poreikio gerbti privatų gyvenimą[177]. Vis dėlto byloje *Leander*[178] EŽTT padarė išvadą, kad teisė susipažinti su asmens duomenimis, kuriuos saugo valdžios institucijos, tam tikromis aplinkybėmis gali būti ribojama.

Pagal ES teisę teisė susipažinti su savo asmens duomenimis aiškiai numatyta Duomenų apsaugos direktyvos 12 straipsnyje ir kaip pagrindinė teisė – Chartijos 8 straipsnio 2 dalyje.

Direktyvos 12 straipsnio a punkte numatyta, kad valstybės narės turi užtikrinti kiekvieno duomenų subjekto teisę susipažinti su savo asmens duomenimis ir gauti informaciją. Visų pirma kiekvienas duomenų subjektas turi teisę gauti iš duomenų valdytojo patvirtinimą, kad su juo susiję duomenys yra tvarkomi, ir informaciją bent apie:

- tvarkymo tikslus;
- susijusių duomenų kategorijas;
- tvarkomus duomenis;
- gavėjus, kuriems atskleidžiami duomenys, arba jų kategorijas;
- bet kokią prieinamą informaciją, susijusią su tvarkomų duomenų šaltiniu;

176 Duomenų apsaugos direktyvos 13 straipsnio 2 dalis..

177 1989 m. liepos 7 d. EŽTT sprendimas *Gaskin prieš Jungtinę Karalystę*, Nr. 10454/83; 2003 m. vasario 13 d. EŽTT sprendimas *Odièvre prieš Prancūziją* (DK), Nr. 42326/98; 2009 m. balandžio 28 d. EŽTT sprendimas *K. H. ir kiti prieš Slovakiją*, Nr. 32881/04; 2012 m. rugsėjo 25 d. EŽTT sprendimas *Godelli prieš Italiją*, Nr. 33783/09.

178 1985 m. liepos 11 d. EŽTT sprendimas *Leander prieš Švediją*, Nr. 9248/81.

- automatinių sprendimų atveju – loginius metodus, taikomus automatiškai tvarkant duomenis.

Nacionalinėje teisėje gali būti nustatyta papildoma informacija, kurią turi pateikti duomenų valdytojas, pvz., teisinio pagrindo, kuriuo remiantis tvarkomi duomenys, nurodymas.

Pavyzdys. Susipažindamas su savo asmens duomenimis asmuo gali nustatyti, ar duomenys yra tikslūs. Todėl duomenų subjektą būtina informuoti apie tvarkomų duomenų kategorijas ir duomenų turinį. Taigi nepakanka, kad duomenų valdytojas paprasčiausiai informuotų duomenų subjektą, jog tvarko jo vardo ir pavardės, adreso, gimimo datos ir pomėgių duomenis. Duomenų valdytojas taip pat turi atskleisti, kad tvarko vardo ir pavardės, pvz., „N. N.“, adreso, pvz., „Schwarzenbergplatz 11, 1040 Viena, Austrija“, gimimo datos, pvz., „1974 m. spalio 10 d.“, ir pomėgių (kuriuos nurodė duomenų subjektas), pvz., „klasikinė muzika“, duomenis. Paskutinis elementas, be kita ko, apima informacijos apie duomenis šaltinį.

Duomenų subjektui informacija apie tvarkomus duomenis ir visus tokios informacijos šaltinius turi būti pateikiama aiškiai. Tai reiškia, kad duomenų valdytojui gali prireikti duomenų subjektui išsamiau paaiškinti, kokius duomenis jis tvarko. Pavyzdžiui, atsakyme į prašymą susipažinti su duomenimis paprastai nepakaks nurodyti techninius sutrumpinimus arba medicininius terminus, net jeigu saugomi tik tokie sutrumpinimai arba terminai.

Duomenų valdytojas, atsakydamas į prašymą leisti susipažinti su duomenimis, turi pateikti informaciją apie tvarkomų duomenų šaltinį, jeigu tokia informacija yra prieinama. Ši nuostata turi būti suprantama atsižvelgiant į sąžiningumo ir atskaitomybės principus. Duomenų valdytojas, siekdamas neatskleisti duomenų, negali sunaikinti informacijos apie duomenų šaltinį, jis taip pat negali nepaisyti įprastų šioje srityje taikomų standartų ir pripažįstamų poreikių. Duomenų valdytojas paprastai nevykdys pareigų, susijusių su teise susipažinti su duomenimis, jeigu jis dokumentuose nefiksuos tvarkomų duomenų šaltinio.

Atliekant automatinius vertinimus reikės paaiškinti vertinimo loginius metodus, įskaitant konkrečius kriterijus, kuriais vadovaujantis buvo vertinamas duomenų subjektas.

Direktyvoje aiškiai nenurodyta, ar teisė susipažinti su informacija susijusi su praeitimi, o jei susijusi, tai su kokiu praeities laikotarpiu. Šiuo atžvilgiu, kaip nurodyta ESTT praktikoje, teisė susipažinti su savo asmens duomenimis negali būti nepagrįstai ribojama nustatant terminus. Duomenų subjektams taip pat turi būti suteikiama pagrįsta galimybė gauti informaciją apie praeityje atliktas duomenų tvarkymo operacijas.

Pavyzdys. Byloje *Rijkeboer*[179] ESTT buvo prašoma nustatyti, ar pagal direktyvos 12 straipsnio a punktą asmens teisės gauti informaciją apie asmens duomenų gavėjus arba jų kategorijas ir duomenų turinį galiojimas gali būti apribojamas vienų metų terminu, kuris pradedamas skaičiuoti nuo prašymo susipažinti pateikimo dienos.

Siekdamas nustatyti, ar pagal direktyvos 12 straipsnio a punktą leidžiama nustatyti tokį terminą, Teismas pirmiausia nurodė, jog teisė susipažinti yra būtina, kad duomenų subjektas galėtų įgyvendinti teisę prašyti, kad duomenų valdytojas ištaisytų, sunaikintų arba užblokuotų jo duomenis (12 straipsnio b punktas) arba trečiosioms šalims, kurioms duomenys buvo atskleisti, pranešti, kad tokie duomenys buvo ištaisyti, sunaikinti arba užblokuoti (12 straipsnio c punktas). Teisė susipažinti taip pat yra būtina, kad duomenų subjektas galėtų įgyvendinti teisę nesutikti, kad jo asmens duomenys būtų tvarkomi (14 straipsnis), arba teisę pareikšti ieškinį tais atvejais, kai patiria nuostolių (22 ir 23 straipsniai).

Siekdamas užtikrinti praktinį pirmiau nurodytų nuostatų taikymą, Teismas nusprendė, kad „ši 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“.

Teisė reikalauti ištaisyti, sunaikinti ir užblokuoti duomenis

„Bet kuriam asmeniui turi būti sudarytos galimybės pasinaudoti teise gauti su juo susijusius tvarkomus duomenis, ypač norint patikrinti duomenų tikslumą ir tvarkymo teisėtumą.“[180] Vadovaujantis šiais principais, nacionalinėje teisėje duomenų subjektams turi būti nustatyta teisė reikalauti, kad duomenų valdytojas ištaisytų,

179 2009 m. gegužės 7 d. ESTT sprendimas *College van burgemeester en wethouders van Rotterdam prieš M. E. E. Rijkeboer*, C-553/07.

180 Duomenų apsaugos direktyvos 41 konstatuojamoji dalis.

sunaikintų arba užblokuotų duomenų subjektų duomenis, jei jie mano, kad tokių duomenų tvarkymas neatitinka direktyvos nuostatos, visų pirma todėl, kad duomenys yra netikslūs arba neišsamūs[181].

Pavyzdys. Byloje *Cemalettin Canli prieš Turkiją*[182] EŽTT nustatė, kad policija neteisingai rengė baudžiamosios bylos pranešimus ir pažeidė EŽTK 8 straipsnį.

Pareiškėjas du kartus dalyvavo baudžiamojoje byloje, kurioje buvo kaltinamas dalyvavęs neteisėtose organizacijose, tačiau niekada nebuvo nuteistas. Kai pareiškėjas buvo dar kartą suimtas ir apkaltintas kita nusikalstama veika, policija pateikė baudžiamajam teismui pranešimą, pavadintą „*Informacijos apie papildomus nusikaltimus forma*“, kuriame nurodyta, kad pareiškėjas buvo dviejų neteisėtų organizacijų narys. Pareiškėjo prašymas pakeisti pranešimą ir policijos įrašus nebuvo patenkintas. EŽTT nusprendė, kad pranešime policijos pateiktai informacijai buvo taikomas EŽTT 8 straipsnis, nes vieša informacija į sąvokos „privatus gyvenimas“ taikymo sritį galėjo patekti ir tais atvejais, kai ji buvo sistemiškai renkama ir saugoma institucijų rinkmenose. Be to, policijos pranešimas buvo neteisingas ir jis buvo parengtas ir pateiktas baudžiamajam teismui nesilaikant įstatymo nuostatų. Teismas nusprendė, kad 8 straipsnis buvo pažeistas.

Pavyzdys. Byloje *Segerstedt-Wiberg ir kiti prieš Švediją*[183] pareiškėjai buvo susiję su tam tikromis liberalų ir komunistų politinėmis partijomis. Pareiškėjams kilo įtarimų, kad informacija apie juos buvo įrašyta į slaptus policijos įrašus. EŽTT teigiamai įvertino tai, kad aptariami duomenys buvo saugojami remiantis teisiniu pagrindu ir buvo tvarkomi teisėtu tikslu. Dėl kai kurių pareiškėjų EŽTT nustatė, kad nuolat saugant duomenis buvo neproporcingai ribojamas jų privatus gyvenimas. Pavyzdžiui, valdžios institucijos saugojo apie Schmid informaciją, kad jis 1969 m. per demonstracijas tariamai dalyvavo smurtiniame pasipriešinime prieš policijos vykdomą kontrolę. EŽTT nustatė, kad naudojantis šia informacija nebuvo galima ginti kokio nors susijusio nacionalinio saugumo intereso, visų pirma atsižvelgiant į informacijos senumą. EŽTT nusprendė, kad keturių iš penkių pareiškėjų atžvilgiu EŽTK 8 straipsnis buvo pažeistas.

181 *Ibid.*, 12 straipsnio b punktas.

182 2008 m. lapkričio 18 d. EŽTT sprendimo *Cemalettin Canli prieš Turkiją*, Nr. 22427/04, 33, 42 ir 43 punktai; 2010 m. vasario 2 d. EŽTT sprendimas *Dalea prieš Prancūziją*, Nr. 964/07.

183 2006 m. birželio 6 d. EŽTT sprendimo *Segerstedt-Wiberg ir kiti prieš Švediją*, Nr. 62332/00, 89 ir 90 punktai; taip pat žr., pvz., 2013 m. balandžio 18 d. EŽTT sprendimą *M. K. prieš Prancūziją*, Nr. 19522/09.

Tam tikrais atvejais duomenų subjektui paprasčiausiai pakaks paprašyti ištaisyti vardą arba pavardę, pakeisti adresą arba telefono numerį. Tačiau jei tokie prašymai susiję su teisiniais klausimais, pvz., duomenų subjektų teisine tapatybe arba teisingu gyvenamosios vietos nurodymu teisiniams dokumentams įteikti, prašymų ištaisyti duomenis gali nepakakti ir duomenų valdytojui gali būti suteikiama teisė reikalauti, kad suinteresuotasis asmuo pateiktų tariamo duomenų netikslumo įrodymus. Dėl tokių reikalavimų duomenų subjektas negali patirti nepagrįstos įrodinėjimo naštos, kuri užkirstų kelią duomenų subjektui ištaisyti savo duomenis. EŽTT keliose bylose nustatė EŽTK 8 straipsnio pažeidimo atvejus, kai pareiškėjas negalėjo ginčyti slaptuose registruose laikomos informacijos slaptumo[184].

Pavyzdys. Byloje *Ciubotaru prieš Moldovą*[185] pareiškėjas negalėjo pakeisti oficialių etninės kilmės registracijos įrašų (iš moldavo į rumuną) tariamai dėl to, kad 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. Vis dėlto pareiškėjo prašymas buvo pagrįstas daugiau nei vien subjektyviu savo etninės kilmės supratimu; jis galėjo pateikti objektyviai patikrinamus ryšius su rumunų etnine grupe, pvz., kalba, vardas ir pavardė, priklausymo jausmas ir kt. Tačiau pagal vidaus teisę buvo reikalaujama, kad pareiškėjas pateiktų įrodymus, jog jo tėvai priklausė rumunų etninei grupei. Atsižvelgiant į istorines Moldovos aplinkybes, toks reikalavimas sukėlė neįveikiamą kliūtį registruojant etninę kilmę, kitokią nei ta, kurią jo tėvams suteikė sovietų valdžios institucijos. Kadangi pareiškėjo prašymas nebuvo nagrinėjamas atsižvelgiant į objektyviai patikrinamus įrodymus, valstybė nesilaikė teigiamo įsipareigojimo užtikrinti tinkamos pagarbos pareiškėjo privačiam gyvenimui. Teismas nusprendė, kad EŽTK 8 straipsnis buvo pažeistas.

Nagrinėjant civilinę bylą arba valdžios institucijai vykdant atitinkamas procedūras, per kurias siekiama nuspręsti, ar duomenys teisingi, duomenų subjektas gali prašyti jo duomenų rinkmenoje padaryti įrašą arba įrašyti pastabą, kad duomenų tikslumas yra ginčijamas, o oficialus sprendimas dar nepriimtas. Per šį laikotarpį duomenų valdytojas negali nurodyti, kad duomenys yra tikslūs arba galutiniai, visų pirma trečiųjų šalių atžvilgiu.

184 2000 m. gegužės 4 d. EŽTT sprendimas *Rotaru prieš Rumuniją*, Nr. 28341/95.

185 2010 m. balandžio 27 d. EŽTT sprendimo *Ciubotaru prieš Moldovą*, Nr. 27138/04, 51 ir 59 punktai.

Duomenų subjekto prašymas sunaikinti arba išbraukti duomenis dažnai būna grindžiamas tuo, kad duomenų tvarkymas nėra pagrįstas teisėtu pagrindu. Tokie prašymai dažnai pateikiami tais atvejais, kai sutikimas atšaukiamas arba kai tam tikri duomenys, atsižvelgiant į jų surinkimo tikslą, nebereikalingi. Su duomenų tvarkymo teisėtumu susijusi įrodinėjimo našta teks duomenų valdytojui, nes jis yra atsakingas už tvarkymo teisėtumą. Vadovaujantis atskaitomybės principu, duomenų valdytojas turi bet kuriuo metu gebėti įrodyti, kad duomenis tvarko remdamasis patikimu teisėtu pagrindu, priešingu atveju duomenys nebeturi būti tvarkomi.

Jeigu duomenų tvarkymas ginčijamas dėl to, kad duomenys tariamai neteisingi arba neteisėtai tvarkomi, duomenų subjektas, vadovaudamasis sąžiningo duomenų tvarkymo principu, gali reikalauti, kad ginčijami duomenys būtų užblokuoti. Tai reiškia, kad duomenys nesunaikinami, tačiau duomenų valdytojas duomenų blokavimo metu turi nenaudoti jų. Tai ypač reikalinga tais atvejais, kai nuolatinis netikslių arba neteisėtai laikomų duomenų naudojimas galėtų būti žalingas duomenų subjektui. Nacionalinėje teisėje turėtų būti išsamiau aprašomi pareigos užblokuoti duomenų naudojimą atsiradimo pagrindai ir tai, kaip ji turėtų būti vykdoma.

Be to, duomenų subjektai turi teisę reikalauti, kad duomenų subjektas praneštų trečiosioms šalims apie bet kokį duomenų užblokavimą, ištaisymą arba sunaikinimą, jeigu jos duomenis gavo prieš šias duomenų tvarkymo operacijas. Kadangi duomenų valdytojas turi pareigą dokumentuoti duomenų atskleidimo trečiosioms šalims atvejus, turėtų būti įmanoma nustatyti duomenų gavėjus ir prašyti ištrinti duomenis. Tačiau jei tuo metu duomenys buvo paskelbti, pvz., internete, bet kuriuo atveju duomenų nebūtų įmanoma ištrinti, nes duomenų gavėjų negalima nustatyti. Pagal Duomenų apsaugos direktyvą, siekiant ištaisyti, ištrinti arba užblokuoti duomenis, būtina susisiekti su duomenų gavėjais, „nebent tai padaryti būtų neįmanoma arba pernelyg sunku“[186].

5.1.2. Teisė nesutikti

Teisė nesutikti apima teisę nesutikti su automatiniais individualiais sprendimais, teisę nesutikti atsižvelgiant į konkrečią duomenų subjekto padėtį ir teisę nesutikti su tolesniu duomenų naudojimu tiesioginės rinkodaros tikslais.

186 Duomenų apsaugos direktyvos 12 straipsnio c punkto paskutinio sakinio pabaiga.

Teisė nesutikti su automatiniais individualiais sprendimais

Automatiniai sprendimai – tai sprendimai, kurie, naudojant asmens duomenis, priimami tik automatiniais būdais. Jeigu tokie sprendimai gali turėti didelį poveikį asmenų gyvenimui, nes, pvz., yra susiję su kreditingumu, darbo rezultatais, elgesiu arba patikimumu, siekiant užkirsti kelią neigiamoms pasekmėms, būtina užtikrinti specialią apsaugą. Duomenų apsaugos direktyvoje numatyta, kad priimant automatinius sprendimus neturėtų būti sprendžiami asmenims svarbūs klausimai, ir reikalaujama, kad asmeniui būtų suteikiama galimybė peržiūrėti automatinį sprendimą[187].

Pavyzdys. Svarbus praktinis automatinių sprendimų pavyzdys yra kreditingumo vertinimas. Siekiant greitai priimti sprendimą dėl būsimo kliento kreditingumo, iš kliento surenkami tam tikri duomenys, pvz., duomenys apie profesiją ir šeiminę padėtį, ir lyginami su atitinkama informacija kituose šaltiniuose, pvz., kredito informacijos sistemose. Šie duomenys automatiškai perduodami į vertinimo balų algoritmą, kuris apskaičiuoja bendrą potencialaus kliento kreditingumo vertę. Todėl įmonės darbuotojas gali greitai priimti sprendimą dėl to, ar duomenų subjektas yra tinkamas klientas, ar ne.

Vis dėlto pagal direktyvą valstybės narės numato, kad dėl asmens gali būti priimamas individualus sprendimas, kai, atsižvelgiant į tai, kad sprendimas buvo palankus duomenų subjektui, duomenų subjekto interesams pavojus nekyla arba jų apsauga užtikrinama tinkamomis priemonėmis[188]. Teisė nesutikti su automatiniais sprendimais taip pat numatyta **ET teisėje**, t. y. Rekomendacijoje dėl profiliavimo[189].

Teisė nesutikti atsižvelgiant į konkrečią duomenų subjekto padėtį

Duomenų subjektai neturi bendros teisės nesutikti, kad jų duomenys būtų tvarkomi[190]. Tačiau Duomenų apsaugos direktyvos 14 straipsnio a punkte duomenų subjektui suteikiama teisė pareikšti prieštaravimą remiantis įtikinamais teisėtais pagrindais, susijusiais su konkrečia savo padėtimi. Panaši teisė pripažįstama ET

187 *Ibid.*, 15 straipsnio 1 dalis.

188 *Ibid.*, 15 straipsnio 2 dalis.

189 Rekomendacijos dėl profiliavimo 5 straipsnio 5 dalis.

190 Taip pat žr. 1997 m. rugpjūčio 27 d. EŽTT sprendimą *M. S. prieš Švediją*, Nr. 20837/92, kuriame medicininiai duomenys buvo pateikti be sutikimo ir nesuteikus galimybės pasinaudoti teise nesutikti, arba 1987 m. kovo 26 d. EŽTT sprendimą *Leander prieš Švediją*, Nr. 9248/81, arba 2011 m. gegužės 10 d. EŽTT sprendimą *Mosley prieš Jungtinę Karalystę*, Nr. 48009/08.

Rekomendacijoje dėl profiliavimo[191]. Tokių nuostatų tikslas – rasti tinkamą duomenų subjektų duomenų apsaugos teisių ir kitų asmenų teisėtų interesų tvarkant duomenų subjekto duomenis pusiausvyrą.

Pavyzdys. Bankas septynerius metus saugo duomenis apie savo klientus, kurie vėluoja mokėti paskolos įmokas. Klientas, kurio duomenys saugomi šioje duomenų bazėje, prašo išduoti kitą paskolą. Išnagrinėjus duomenų bazėje esančius duomenis ir įvertinus kliento finansinę padėtį, jam atsisakoma išduoti paskolą. Tačiau klientas gali prieštarauti duomenų bazėje įrašytiems duomenims ir prašyti juos ištrinti, jei gali įrodyti, kad mokėjimą buvo vėluojama atlikti tik dėl klaidos, kuri buvo ištaisyta netrukus po to, kai klientas apie ją sužinojo.

Patenkinus prieštaravimą, duomenų valdytojas nebegali toliau tvarkyti duomenų. Tačiau iki duomenų subjekto prieštaravimo atliktos duomenų tvarkymo operacijos išlieka teisėtos.

Teisė nesutikti su tolesniu duomenų naudojimu tiesioginės rinkodaros tikslais

Duomenų apsaugos direktyvos 14 straipsnio b punkte numatyta konkreti teisė nesutikti su asmens duomenų naudojimu tiesioginės rinkodaros tikslais. Tokia teisė taip pat nustatyta ET Rekomendacijoje dėl tiesioginės rinkodaros[192]. Šios rūšies prieštaravimas turi būti pareikštas prieš leidžiant trečiosioms šalims tiesioginės rinkodaros tikslais susipažinti su duomenimis. Todėl duomenų subjektui turi būti suteikiama galimybė pareikšti nesutikimą prieš teikiant duomenis.

5.2. Nepriklausoma priežiūra

Pagrindiniai faktai

- Siekiant užtikrinti veiksmingą duomenų apsaugą, pagal nacionalinę teisę turi būti sukuriamos nepriklausomos priežiūros institucijos.

191 Rekomendacijos dėl profiliavimo 5 straipsnio 3 dalis.

192 ET Ministrų Komitetas (1985 m.), 1985 m. spalio 25 d. Rekomendacijos Nr. R (85) 20 valstybėms narėms dėl asmens duomenų, naudojamų tiesioginės rinkodaros tikslais, apsaugos 4 straipsnio 1 dalis.

- Nacionalinės priežiūros institucijos turi veikti visiškai nepriklausomai ir toks nepriklausomas statusas turi būti įtvirtintas įstatyme, kuriuo įsteigiama priežiūros institucija, ir atsispindėti jos konkrečioje organizacinėje struktūroje.
- Priežiūros institucijos, be kitų, vykdo šias užduotis:
  - stebi duomenų apsaugą ir skatina ją užtikrinti nacionaliniu lygmeniu;
  - konsultuoja duomenų subjektus ir duomenų valdytojus, taip pat vyriausybę ir visą visuomenę;
  - nagrinėja skundus ir padeda duomenų subjektams apginti tariamus duomenų apsaugos teisės pažeidimus;
  - prižiūri duomenų valdytojus ir duomenų tvarkytojus;
  - prireikus įsikiša ir:
    - įspėja duomenų valdytojus ir duomenų tvarkytojus, teikia jiems pastabą arba net skiria baudą,
    - liepia ištaisyti, užblokuoti arba ištrinti duomenis,
    - draudžia tvarkyti duomenis;
  - perduoda klausimą spręsti teismui.

Duomenų apsaugos direktyvoje reikalaujama nustatyti nepriklausomą priežiūrą kaip svarbią veiksmingos duomenų apsaugos mechanizmo sudedamąją dalį. Direktyvoje nustatyta duomenų apsaugos užtikrinimo priemonė, kuri iš pradžių nebuvo numatyta Konvencijoje Nr. 108 arba EBPO privatumo gairėse.

Paaiškėjus, kad nepriklausoma priežiūra yra būtina veiksmingai duomenų apsaugai užtikrinti, naujoje peržiūrėtų EBPO privatumo gairių nuostatoje, kuri buvo priimta 2013 m., šalys narės raginamos „nustatyti ir išlaikyti privatumą užtikrinančias institucijas, kurių valdymo struktūra, ištekliai ir techninės žinios padėtų veiksmingai joms įgyvendinti savo įgaliojimus ir priimti objektyvius, nešališkus ir nuoseklius sprendimus“[193].

Pagal ET teisę Konvencijos Nr. 108 papildomame protokole nustatyta pareiga sukurti priežiūros institucijas. Šio dokumento 1 straipsnyje įtvirtinta nepriklausomų priežiūros institucijų teisinė sistema, kurią susitariančiosios šalys turi įgyvendinti savo

193 2013 m. EBPO privatumo ir tarpvalstybinių asmens duomenų srautų apsaugai taikomų gairių 19 straipsnio c punktas.

vidaus teisėje. Joje šių institucijų užduotys ir įgaliojimai aprašomi panašiai kaip Duomenų apsaugos direktyvoje. Todėl iš esmės priežiūros institucijų veikimo principai pagal ES ir ET teisę yra vienodi.

Pagal ES teisę priežiūros institucijų kompetencija ir organizacinė struktūra pirmiausia buvo nustatyta Duomenų apsaugos direktyvos 28 straipsnio 1 dalyje. ES institucijų duomenų apsaugos reglamente[194] nustatyta, kad duomenų tvarkymą ES įstaigose ir institucijose prižiūri EDAPP. Šiame reglamente aprašant priežiūros institucijos funkcijas ir pareigas remiamasi patirtimi, įgyta paskelbus Duomenų apsaugos direktyvą.

Duomenų apsaugos institucijų nepriklausomumas garantuojamas SESV 16 straipsnio 2 dalyje ir Chartijos 8 straipsnio 3 dalyje. Iš pastarosios nuostatos matyti, kad nepriklausomos institucijos vykdoma kontrolė yra esminis pagrindinės teisės į duomenų apsaugą elementas. Be to, Duomenų apsaugos direktyvoje reikalaujama, kad valstybės narės sukurtų priežiūros institucijas, kurios, veikdamos visiškai nepriklausomai, stebėtų, kaip taikoma direktyva[195]. Nepriklausomumą garantuojančios konkrečios nuostatos turi būti numatytos ne tik įstatyme, kuriuo sukuriama priežiūros institucija, bet tokį nepriklausomumą turi padėti užtikrinti ir institucijos organizacinė struktūra.

2010 m. ESTT pirmą kartą nagrinėjo duomenų apsaugos priežiūros institucijų nepriklausomumo reikalavimo taikymo sritį[196]. Toliau nurodytame pavyzdyje pateikiama ESTT argumentacija.

Pavyzdys. Byloje *Komisija prieš Vokietiją*[197] Europos Komisija prašė ESTT pripažinti, kad Vokietija netinkamai perkėlė į nacionalinę teisę už duomenų apsaugą atsakingų priežiūros institucijų „visiško nepriklausomumo“ reikalavimą ir todėl neįgyvendino Duomenų apsaugos direktyvos 28 straipsnio 1 dalyje jai nustatytų pareigų. Komisijos manymu, problema buvo ta, kad Vokietija skirtingose

194 2000 m. gruodžio 18 d. Europos Parlamento ir Tarybos reglamento (EB) Nr. 45/2001 dėl asmenų apsaugos Bendrijos institucijoms ir įstaigoms tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo, OL L 8, 2001, 41–48 straipsniai.

195 Duomenų apsaugos direktyvos 28 straipsnio 1 dalies paskutinis sakinys; Konvencijos Nr. 108 papildomo protokolo 1 straipsnio 3 dalis.

196 Žr. FRA (2010 m.), 2010 m. metinės ataskaitos *„Pagrindinės teisės: 2010 m. iššūkiai ir pasiekimai“*, p. 59. FRA šį klausimą išsamiau aptarė savo 2010 m. gegužės mėn. paskelbtoje ataskaitoje *„Duomenų apsauga Europos Sąjungoje: nacionalinių duomenų apsaugos institucijų vaidmuo“*.

197 2010 m. kovo 9 d. ESTT sprendimo *Europos Komisija prieš Vokietijos Federacinę Respubliką*, C-518/07, 27 punktas.

federalinėse žemėse (vok. *Länder*) taikė valstybinę priežiūrą ne viešojo sektoriaus institucijoms, atsakingoms už asmens duomenų tvarkymo stebėseną.

Ieškinio esminis vertinimas, pasak Teismo, priklausė nuo šioje nuostatoje įtvirtinto nepriklausomumo reikalavimo taikymo srities ir nuostatos aiškinimo.

Teismas pabrėžė, kad direktyvos 28 straipsnio 1 dalyje vartojami žodžiai „visiškai nepriklausomai“ turi būti aiškinami remiantis faktine šios nuostatos formuluote ir Duomenų apsaugos direktyvos tikslais ir struktūra[198]. Teismas pabrėžė, kad priežiūros institucijos yra su asmens duomenų tvarkymu susijusių teisių, kurios užtikrinamos direktyvoje, „sergėtojos“, todėl jų įsteigimas laikomas „pagrindiniu asmenų apsaugos tvarkant asmens duomenis elementu“[199]. Teismas padarė išvadą, kad „vykdydamos savo funkcijas priežiūros institucijos turi veikti objektyviai ir nešališkai. Šiuo tikslu jų neturi veikti jokia valstybės ar *Länder* išorinė įtaka, įskaitant tiesioginę ar netiesioginę, o ne vien kontroliuojamų organizacijų įtaka“[200].

ESTT taip pat nusprendė, kad „visiško nepriklausomumo“ reikšmė turėtų būti aiškinama atsižvelgiant į EDAPP nepriklausomumą, kaip apibrėžta ES institucijų duomenų apsaugos reglamente. Kaip pažymėjo Teismas, šio reglamento 44 straipsnio 2 dalyje paaiškinama nepriklausomumo sąvoka, nurodant, kad EDAPP, vykdydamas pareigas, nei siekia iš kitų gauti nurodymų, nei juos vykdo. Todėl nepriklausomos duomenų apsaugos priežiūros institucijos valstybinė priežiūra yra draudžiama[201].

Atitinkamai ESTT nusprendė, kad Vokietijos duomenų apsaugos institucijos, kurios federaliniu lygiu atsako už viešajam sektoriui nepriklausančių įstaigų asmens duomenų tvarkymo priežiūrą, nebuvo pakankamai nepriklausomos, nes jų veiklą prižiūrėjo valstybė.

Pavyzdys. Byloje *Komisija prieš Austriją*[202] ESTT atkreipė dėmesį į panašias problemas, susijusias su tam tikrais Austrijos duomenų apsaugos institucijos (Duomenų apsaugos komisija, DSK) nariais ir darbuotojais. Teismas šioje byloje

198 *Ibid.*, 17 ir 29 punktai.

199 *Ibid.*, 23 punktas.

200 *Ibid.*, 25 punktas.

201 *Ibid.*, 27 punktas.

202 2012 m. spalio 16 d. ESTT sprendimo *Europos Komisija prieš Austrijos Respubliką*, C-614/10, 59 ir 63 punktai.

nusprendė, kad Austrijos teisės akte Austrijos duomenų apsaugos institucijai buvo draudžiama visiškai nepriklausomai vykdyti savo funkcijas, kaip nustatyta Duomenų apsaugos direktyvoje. Austrijos duomenų apsaugos institucijos nepriklausomumas nebuvo tinkamai užtikrinamas, nes Federalinė kanceliarija aprūpina Austrijos duomenų apsaugos instituciją savo darbuotojais, prižiūri jos veiklą ir turi teisę bet kuriuo metu gauti informaciją apie jos darbą.

Pavyzdys. Byloje *Europos Komisija prieš Vengriją*[203], ESTT nurodė, kad „reikalavimas [...] užtikrinti, kad kiekviena priežiūros institucija galėtų atlikti jai patikėtus uždavinius visiškai nepriklausomai reiškia valstybių narių pareigą sudaryti sąlygas tai institucijai veikti visą kadenciją“. Teismas taip pat konstatavo, kad „anksčiau laiko nutraukdama priežiūros institucijos asmens duomenų apsaugos priežiūros terminą, Vengrija neįvykdė savo įsipareigojimų pagal Direktyvos 95/46/EB [...].“

Priežiūros institucijos pagal nacionalinę teisę, be kita ko, turi ir šiuos įgaliojimus ir gebėjimus:[204]

- konsultuoti duomenų valdytojus ir duomenų subjektus visais duomenų apsaugos klausimais;
- tirti duomenų tvarkymo operacijas ir prireikus į jas įsikišti;
- įspėti duomenų valdytojus ir pateikti jiems pastabą;
- liepti ištaisyti, užblokuoti, ištrinti arba sunaikinti duomenis;
- laikinai arba visam laikui uždrausti tvarkyti duomenis;
- perduoti klausimą spręsti teismui.

Kad priežiūros institucija galėtų vykdyti savo funkcijas, jai būtina prieiga prie visų asmens duomenų ir informacijos, kurios reikia tyrimui atlikti, taip pat galimybė patekti į visas patalpas, kuriose duomenų valdytojas laiko susijusią informaciją.

203 2012 m. birželio 8 d. ESTT sprendimas *Europos Komisija prieš Vengriją*, C-288/12, p. 50 ir 67.

204 Duomenų apsaugos direktyvos 28 straipsnis; papildomai žr. Konvencijos Nr. 108 papildomo protokolo 1 straipsnį.

Kalbant apie vidaus jurisdikcijas pažymėtina, kad priežiūros institucijos taikomos procedūros ir priimamų išvadų teisinis pobūdis labai skiriasi. Tai gali būti tiek ombudsmeno tipo rekomendacijos, tiek nedelsiant vykdomi sprendimai. Todėl nagrinėjant jurisdikcijoje prieinamų teisių gynimo priemonių veiksmingumą kiekvieną teisių gynimo priemonę reikia vertinti atsižvelgiant į konkrečias aplinkybes.

5.3. Teisių gynimo priemonės ir sankcijos

Pagrindiniai faktai

- Pagal Konvenciją Nr. 108 ir Duomenų apsaugos direktyvą nacionalinėje teisėje turi būti numatytos tinkamos teisių gynimo priemonės ir sankcijos už teisės į duomenų apsaugą pažeidimus.
    - Pagal ES teisę teisė į veiksmingą teisių gynimo priemonę reiškia, kad nacionalinėje teisėje turi būti nustatytos teisminės duomenų apsaugos teisių gynimo priemonės, nepaisant galimybės kreiptis į priežiūros instituciją.
    - Nacionalinėje teisėje turi būti nustatytos veiksmingos, teisingos, proporcingos ir atgrasančios sankcijos.
- Prieš pareikšdamas ieškinį teisme asmuo pirmiausia turi kreiptis į duomenų valdytoją. Nacionalinėje teisėje nustatoma, ar prieš kreipiantis į teismą privaloma ginčą perduoti spręsti priežiūros institucijai.
- Duomenų subjektai tam tikromis aplinkybėmis dėl duomenų apsaugos pažeidimų gali kreiptis į EŽTT kaip kasacinę instanciją.
- Be to, duomenų subjektai gali kreiptis į ESTT, tačiau tik išimtiniais atvejais.

Duomenų apsaugos teisėje numatytas teises gali įgyvendinti tik tas asmuo, kurio teisėms gresia pavojus; tai asmuo, kuris yra duomenų subjektas arba bent jau teigia juo esantis. Tokiems asmenims įgyvendinant savo teises gali atstovauti asmenys, kurie atitinka nacionalinėje teisėje nustatytus būtinus reikalavimus. Nepilnamečiams atstovauja jų tėvai arba globėjai. Priežiūros institucijose asmeniui taip pat gali atstovauti asociacijos, kurių teisėtas tikslas – užtikrinti duomenų apsaugos teisių apsaugą.

5.3.1. Duomenų valdytojui teikiami prašymai

3.2 dalyje nurodytas teises visų pirma reikia įgyvendinti duomenų valdytojo atžvilgiu. Tiesioginis kreipimasis į priežiūros instituciją arba teismą nebūtų naudingas, nes

institucija galėtų tik patarti visų pirma kreiptis į duomenų valdytoją, o teismas nustatytų, kad ieškinys yra nepriimtinas. Nacionalinėje teisėje turi būti nustatyti oficialūs atitinkamo teisinio prašymo reikalavimai, visų pirma tai, ar toks prašymas turi būti pateikiamas raštu.

Subjektas, į kurį kreiptasi kaip į duomenų valdytoją, turi atsakyti į prašymą, net jeigu jis nėra duomenų valdytojas. Atsakymas duomenų subjektui bet kuriuo atveju turi būti pateikiamas per nacionaliniame įstatyme nustatytą terminą, net jeigu tokiame atsakyme reikia tik nurodyti, kad duomenys apie prašymą pateikusį asmenį nėra tvarkomi. Vadovaujantis Duomenų apsaugos direktyvos 12 straipsnio a punktu ir Konvencijos Nr. 108 8 straipsnio b punktu, šis prašymas turi būti nagrinėjamas „per daug nedelsiant“. Todėl nacionalinėje teisėje turėtų būti nustatytas gana trumpas, tačiau pakankamas terminas, per kurį duomenų valdytojas galėtų tinkamai išnagrinėti prašymą.

Prieš atsakydamas į prašymą subjektas, į kurį kreiptasi kaip į duomenų valdytoją, turi nustatyti prašymą pateikusio asmens tapatybę, kad išsiaiškintų, ar prašymą pateikė tikrai tas asmuo, ir taip išvengti rimto konfidencialumo pareigos pažeidimo. Jeigu tapatybės nustatymo tvarka nacionaliniame įstatyme nėra konkrečiai aptariama, ją nustato duomenų valdytojas. Tačiau vadovaujantis sąžiningo duomenų tvarkymo principu reikėtų, kad duomenų valdytojai nenustatytų pernelyg sudėtingų tapatybės nustatymo sąlygų (ir prašymo tapatumo nustatymo sąlygų, kaip aptarta 2.1.1 dalyje).

Nacionalinėje teisėje taip pat turi būti aptariama, ar prieš atsakydami į prašymus duomenų valdytojai gali reikalauti, kad prašymą pateikęs asmuo sumokėtų mokestį: direktyvos 12 straipsnio a punkte ir Konvencijos Nr. 108 8 straipsnio b punkte nustatyta, kad atsakymai į prašymus leisti susipažinti su duomenimis pateikiami „be pernelyg didelių išlaidų“. Daugumoje Europos valstybių galiojančiuose nacionaliniuose įstatymuose numatyta, kad su duomenų apsaugos teise susiję prašymai turi būti tenkinami nemokamai, jei tam nereikia itin didelių ir neįprastų pastangų; todėl nacionalinėje teisėje paprastai užtikrinama duomenų valdytojų apsauga nuo piktnaudžiavimo teise gauti atsakymą į prašymus.

Jeigu į asmenį, instituciją arba įstaigą kreiptasi kaip į duomenų valdytoją ir toks asmuo, institucija arba įstaiga nepaneigia, kad jis yra duomenų valdytojas, šis subjektas per nacionaliniame įstatyme nustatytą terminą turi:

- priimti prašymą ir prašymą pateikusį asmenį informuoti, kaip jo prašymas buvo nagrinėjamas, arba

- informuoti prašymą pateikusį asmenį apie priežastis, dėl kurių jo prašymas nebuvo nagrinėjamas.

5.3.2. Priežiūros institucijai pateikti reikalavimai

Kai asmuo, pateikęs duomenų valdytojui prašymą leisti susipažinti su duomenimis arba pareiškęs nesutikimą, kad duomenys būtų tvarkomi, laiku negauna jį tenkinančio atsakymo, jis gali kreiptis į duomenų apsaugos priežiūros instituciją ir prašyti suteikti pagalbą. Priežiūros institucijoje vykdomos procedūros metu reikėtų išsiaiškinti, ar asmuo, institucija arba įstaiga, į kurią kreipiasi prašymą pateikęs asmuo, iš tikrųjų turėjo pareigą atsakyti į prašymą ir ar atsakymas buvo teisingas ir išsamus. Priežiūros institucija turi informuoti susijusį asmenį apie reikalavimo nagrinėjimo procedūros rezultatus[205]. Nacionalinėje priežiūros institucijoje vykdomos procedūros rezultatų teisinis poveikis priklauso nuo nacionalinės teisės: ar institucijos sprendimus galima teisiškai vykdyti (tai reiškia, kad juos gali vykdyti oficiali institucija), ar būtina kreiptis į teismą, jei duomenų valdytojas nesilaiko priežiūros institucijos sprendimų (nuomonės, pastabos ir t. t.).

Jeigu SESV 16 straipsnyje garantuojamas duomenų apsaugos teises tariamai pažeidė ES institucijos arba įstaigos, duomenų subjektas gali pateikti skundą EDAPP[206], t. y. nepriklausomai duomenų apsaugos priežiūros institucijai, kurios teisės ir pareigos nustatytos ES institucijų duomenų apsaugos reglamente. Jei EDAPP per šešis mėnesius nepateikia atsakymo, skundas laikomas atmestu.

Turi būti numatyta galimybė nacionalinės priežiūros institucijos sprendimus skųsti teismams. Ši nuostata taikoma duomenų subjektui ir duomenų valdytojams, kurie kaip šalys dalyvavo priežiūros institucijos vykdomoje procedūroje.

Pavyzdys. Jungtinės Karalystės informacijos komisaras 2013 m. liepos 24 d. priėmė sprendimą, kuriame prašė, kad Harfordšyro policija nustotų naudoti transporto priemonių registracijos numerių sekimo sistemą, kuri, jo manymu, buvo

205 Duomenų apsaugos direktyvos 28 straipsnio 4 dalis.

206 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.

neteisėta. Kameromis užfiksuoti ir surinkti duomenys buvo saugomi vietos policijos duomenų bazėje ir centralizuotoje duomenų bazėje. Transporto priemonių registracijos numerių nuotraukos buvo saugomos dvejus metus, o automobilių – 90 dienų. Buvo nuspręsta, kad toks plataus masto kamerų ir kitų stebėjimo priemonių naudojimas nebuvo proporcingas problemai, kurią siekta spręsti tokiomis priemonėmis.

5.3.3. Ieškinys teismui

Duomenų apsaugos direktyvoje nustatyta, kad jei asmuo, kuris, vadovaudamasis duomenų apsaugos įstatymu pateikė prašymą duomenų valdytojui, nėra patenkintas duomenų valdytojo atsakymu, jam turi būti suteikiama teisė pateikti skundą nacionaliniam teismui[207].

Nacionalinėje teisėje turi būti reglamentuojama tai, ar prieš pareiškiant ieškinį teisme privaloma pirmiausia kreiptis į priežiūros instituciją. Vis dėlto dažniausiai savo duomenų apsaugos teises įgyvendinantiems asmenims būtų naudinga pirmiausia kreiptis į priežiūros instituciją, nes joje vykdoma prašymų suteikti pagalbą nagrinėjimo procedūra turėtų būti paprasta ir nemokama. Priežiūros institucijos sprendime (nuomonėje, pastaboje ir t. t.) užfiksuotos specialiosios žinios taip pat gali padėti duomenų subjektui ginti savo teises teismuose.

Pagal ET teisę duomenų apsaugos teisių pažeidimai, kuriuos tariamai nacionaliniu lygmeniu padarė EŽTK susitariančioji šalis, taigi ir EŽTK 8 straipsnio pažeidimai, EŽTT gali būti nagrinėjami išnaudojus visas prieinamas vidaus teisių gynimo priemones. Kreipiantis į EŽTT dėl EŽTK 8 straipsnio pažeidimo taip pat turi būti tenkinami kiti priimtinumo reikalavimai (EŽTK 34–37 straipsniai)[208].

Nors EŽTT teikiami prašymai gali būti nukreipti tik prieš susitariančiąsias šalis, juose taip pat gali būti netiesiogiai nurodomas privačių šalių veikimas arba neveikimas, jeigu susitariančioji šalis neįvykdė savo teigiamų įsipareigojimų pagal EŽTT ir savo nacionalinėje teisėje neužtikrino tinkamos apsaugos nuo duomenų apsaugos teisių pažeidimų.

207 Duomenų apsaugos direktyvos 22 straipsnis.

208 EŽTK 34–37 straipsniai, galima rasti adresu www.echr.coe.int/Pages/home.aspx?p=caselaw/analysis&c=#n1347458601286_pointer.

Pavyzdys. Byloje *K. U. prieš Suomiją*[209] nepilnametis pareiškėjas skundėsi, kad interneto pažinčių svetainėje apie jį pateiktas intymaus turinio skelbimas. Paslaugų teikėjas neatskleidė asmens, kuris paskelbė informaciją internete, tapatybės, nes turėjo laikytis Suomijos teisėje nustatytos konfidencialumo pareigos. Pareiškėjas teigė, kad Suomijos teisėje nebuvo numatyta tinkama apsauga nuo privataus asmens veiksmų internete skelbiant pareiškėją diskredituojančią informaciją. EŽTT nusprendė, kad valstybės ne tik turėjo pareigą susilaikyti nuo savavališko asmenų privataus gyvenimo apribojimo, bet joms taip pat turi būti nustatyti teigiami įpareigojimai, susiję su „priemonių, kurios padėtų apsaugoti pagarbą privačiam gyvenimui net ir 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 neužtikrino ir Teismas nusprendė, kad EŽTK 8 straipsnis buvo pažeistas.

Pavyzdys. Byloje *Köpke prieš Vokietiją*[210] pareiškėja buvo įtariama vagyste darbo vietoje, kuri buvo nustatyta peržiūrėjus slaptos vaizdo kameros įrašą. EŽTT padarė išvadą, kad „nebuvo jokių aplinkybių, rodančių, kad vidaus institucijos, veikdamos savo nuožiūra, nesugebėjo nustatyti tinkamos pareiškėjo teisės į privataus gyvenimo gerbimą pagal 8 straipsnį ir jos darbdavio interesų, susijusių su savo nuosavybės apsauga, ir viešojo intereso, susijusiu su tinkamu teisingumo vykdymu, pusiausvyros“. Todėl prašymas nebuvo priimtas nagrinėti.

EŽTT nustačius, kad susitariančioji šalis pažeidė kurią nors EŽTT saugomą teisę, susitariančioji šalis turi pareigą vykdyti EŽTT sprendimą. 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.

EŽTT nustačius EŽTK pažeidimą, EŽTK 41 straipsnyje nustatyta, kad EŽTT gali priteisti pareiškėjui teisingą atlyginimą, kurį sumoka susitariančioji šalis.

209 2009 m. kovo 2 d. EŽTT sprendimas *K. U. prieš Suomiją*, Nr. 2872/02.

210 2010 m. spalio 5 d. EŽTT sprendimas *Köpke prieš Vokietiją* (dec.) Nr. 420/07.

Pagal ES teisę[211] nacionalinių duomenų apsaugos įstatymų, kuriais įgyvendinama ES duomenų apsaugos teisė, pažeidimų aukos tam tikrais atvejais gali pareikšti ieškinį ESTT. Duomenų subjektas ieškinį dėl savo duomenų apsaugos teisių pažeidimo ESTT gali pareikšti dviem atvejais.

Pirmuoju atveju duomenų subjektas turėtų būti tiesioginė ES administracinio akto arba reglamentuojančio pobūdžio teisės akto, kuriuo pažeidžiama asmens teisė į duomenų apsaugą, auka. Vadovaujantis SESV 263 straipsnio ketvirta pastraipa,

> *„kiekvienas fizinis ar juridinis asmuo gali <...> pateikti ieškinį dėl jam skirtų aktų arba aktų, kurie yra tiesiogiai ir konkrečiai su juo susiję, ar dėl reglamentuojančio pobūdžio teisės aktų, tiesiogiai su juo susijusių ir dėl kurių nereikia patvirtinti įgyvendinančių priemonių“.*

Todėl ES organo atlikto neteisėto duomenų tvarkymo operacijų aukos gali tiesiogiai kreiptis į ESTT Bendrąjį Teismą, kuris turi kompetenciją priimti sprendimą ES institucijų duomenų apsaugos reglamento įgyvendinimo klausimais. Galimybę kreiptis tiesiogiai į ESTT taip pat turi asmenys, kurių teisinei padėčiai tiesioginį poveikį daro ES teisinė nuostata.

Antrasis atvejis susijęs su ESTT (Teisingumo Teismo) kompetencija priimti prejudicinius sprendimus pagal SESV 267 straipsnį.

Vidaus byloje dalyvaujantys duomenų subjektai gali prašyti nacionalinio teismo kreiptis į Teisingumo Teismą su prašymu išaiškinti ES sutartis ir ES institucijų, įstaigų, tarnybų arba agentūrų priimtų aktų galiojimą. 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.

Jeigu nacionaliniuose teismuose nagrinėjamos bylos šalis prašo perduoti prejudicinius klausimus ESTT, pareigą juos perduoti turi tik kasacinės instancijos nacionaliniai teismai.

211 ES, 2007 m., Lisabonos sutartis, iš dalies keičianti Europos Sąjungos sutartį ir Europos bendrijos steigimo sutartį, pasirašyta Lisabonoje, 2007 m. gruodžio 13 d., ES (2007), OL C 306, 2007. Taip pat žr. Europos Sąjungos sutarties suvestinę redakciją, OL C 326, 2012, ir SESV suvestinę redakciją, OL C 326, 2012.

Pavyzdys. Byloje *Kärntner Landesregierung ir kiti*[212] Austrijos Konstitucinis Teismas pateikė ESTT prejudicinius klausimus, susijusius su Direktyvos 2006/24/EB (*Duomenų saugojimo direktyva*) 3–9 straipsnių galiojimu atsižvelgiant į Chartijos 7, 9 ir 11 straipsnius ir su tuo, ar tam tikros Austrijos Federacinio įstatymo dėl telekomunikacijų, kuriuo į nacionalinę teisę perkeliama Duomenų saugojimo direktyva, nuostatos buvo suderinamos su tam tikromis Duomenų apsaugos direktyvos ir ES institucijų duomenų apsaugos reglamento nuostatomis.

M. Seitlinger (vienas iš Konstitucinio Teismo bylos pareiškėjų) nurodė, kad jis telefoną, internetą ir e. paštą naudoja darbo ir privataus gyvenimo reikmėms. Todėl informacija, kurią jis siunčia ir gauna, perduodama viešais telekomunikacijų tinklais. Pagal 2003 m. Austrijos telekomunikacijų įstatymą telekomunikacijų paslaugų teikėjas yra teisiškai įpareigotas rinkti ir saugoti su jo tinklo naudojimu susijusius duomenis. M. Seitlinger suprato, kad jo asmens duomenų rinkimas ir saugojimas jokiais būdais nebuvo reikalingas techniniais tikslais, kuriais informacija perduodama iš A tinklo į B tinklą. Tiesą sakant, toks nuotolinis duomenų rinkimas ir saugojimas net nebuvo reikalingas sąskaitų išrašymo tikslais. M. Seitlinger iš tikrųjų nesutiko, kad jo asmens duomenys būtų taip naudojami. Vienintelis visų šių papildomų duomenų rinkimo ir saugojimo pagrindas buvo 2003 m. Austrijos telekomunikacijų įstatymas.

Todėl M. Seitlinger pareiškė ieškinį Austrijos Konstituciniam Teismui, kuriame jis teigė, kad įstatyme jo telekomunikacijų paslaugų teikėjui nustatytos pareigos pažeidė jo pagrindines teises, nustatytas ES chartijos 8 straipsnyje.

ESTT sprendimą priima tik dėl prašyme priimti prejudicinį sprendimą nurodytų klausimų. Sprendimą pagrindinėje byloje vis tiek priima nacionalinis teismas.

Iš esmės Teisingumo Teismas turi atsakyti į jam pateiktus prejudicinius klausimus. Jis negali atsisakyti priimti prejudicinį sprendimą remdamasis tuo, kad jo atsakymas nebūtų susijęs su pagrindine byla ar pateikiamas laiku. Vis dėlto Teisingumo Teismas gali atsisakyti priimti prejudicinį sprendimą, jei neturi kompetencijos nagrinėti klausimo.

Galiausiai, jei SESV 16 straipsnyje garantuojamas duomenų apsaugos teises tariamai pažeidžia ES institucija arba įstaiga tvarkydama asmens duomenis, duomenų subjektas gali iškelti bylą ESTT Bendrajame Teisme (ES institucijų duomenų apsaugos

212 Sujungtos bylos C-293/12 ir C-594/12, *Digital Rights Ireland ir Seitlinger bei kiti*, 2014 m. balandžio 8 d.

reglamento 32 straipsnio 1 ir 4 dalys). Tą patį galima pasakyti apie EDAPP sprendimus, susijusius su tokiais pažeidimais (ES institucijų duomenų apsaugos reglamento 32 straipsnio 3 dalis).

Nors ESTT Bendrasis Teismas turi kompetenciją priimti sprendimus ES institucijų duomenų apsaugos reglamento įgyvendinimo klausimais, tačiau jeigu apginti teises siekia asmuo, kuris veikia kaip ES institucijos ar įstaigos darbuotojas, jis turi kreiptis į ES Tarnautojų teismą.

Pavyzdys. Byloje *Europos Komisija prieš The Bavarian Lager Co. Ltd*[213] paaiškinami teisių gynimo būdai, padedantys apsiginti nuo duomenų apsaugos srityje veikiančių ES institucijų ir įstaigų veiksmų arba sprendimų.

Bavarian Lager prašė Europos Komisijos leisti susipažinti su visu Komisijos surengto posėdžio protokolu, kuris tariamai buvo susijęs su įmonei svarbiais teisiniais klausimais. Komisija atmetė įmonės prašymą susipažinti su protokolu remdamasi svarbesniais duomenų apsaugos interesais[214]. *Bavarian Lager*, vadovaudamasi ES institucijų duomenų apsaugos reglamento 32 straipsniu, šį sprendimą apskundė ESTT; tiksliau tariant, Pirmosios instancijos teismui (Bendrojo Teismo pirmtakui). Savo sprendime *Bavarian Lager prieš Komisiją* (T-194/04) Pirmosios instancijos teismas panaikino Komisijos sprendimą atmesti prašymą leisti susipažinti su dokumentu. Europos Komisija apskundė šį sprendimą ESTT. Teisingumo Teismas (didžioji kolegija) priėmė sprendimą, kuriuo anuliavo Pirmosios instancijos teismo sprendimą, ir patvirtino, kad Europos Komisija pagrįstai atmetė prašymą leisti susipažinti su dokumentais.

5.3.4. Sankcijos

Kalbant apie **ET teisę** pažymėtina, jog Konvencijos Nr. 108 10 straipsnyje nustatyta, kad kiekviena šalis privalo nustatyti tinkamas sankcijas ir teisių gynimo priemones už vidaus teisės nuostatų, kurios įteisina Konvencijoje Nr. 108 nustatytus duomenų apsaugos principus, pažeidimą[215]**.** Pagal **ES teisę** Duomenų apsaugos direktyvos

213 2010 m. birželio 29 d. ESTT sprendimas *Europos Komisija prieš The Bavarian Lager Co. Ltd*, C-28/08 P.

214 Dėl argumentų analizės žr. EDAPP (2011 m.), *Galimybė visuomenei susipažinti su dokumentais, kuriuose pateikiami asmens duomenys, priėmus nutartį Bavarian Lager byloje,* galima rasti adresu www.secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/BackgroundP/11-03-24_Bavarian_Lager_EN.pdf.

215 2008 m. liepos 17 d. EŽTT sprendimas *I. prieš Suomiją*, Nr. 20511/03; 2008 m. gruodžio 2 d. EŽTT sprendimas *K. U. prieš Suomiją*, Nr. 2872/02.

24 straipsnyje nustatyta, jog valstybės narės „priima tinkamas priemones užtikrinti, kad šios direktyvos nuostatos būtų visiškai įgyvendintos, ir būtinai išdėsto sankcijas, kurios taikomos pažeidus <...> priimtas nuostatas“.

Abiejose priemonėse numatyta, kad valstybės narės, pasirinkdamos tinkamas sankcijas ir teisių gynimo priemones, naudojasi plačia diskrecijos teise. Nė vienoje teisinėje priemonėje nepateiktos konkrečios gairės dėl tinkamų sankcijų pobūdžio ar rūšies, taip pat nepateikiami sankcijų pavyzdžiai.

Tačiau,

> *„nors ES valstybės narės, nustatydamos tinkamiausias priemones iš ES teisės kildinamoms teisėms apsaugoti, naudojasi tam tikra diskrecijos teise, vadovaujantis ES sutarties 4 straipsnio 3 dalyje nustatytu lojalaus bendradarbiavimo principu, reikėtų paisyti minimalių veiksmingumo, lygiavertiškumo, proporcingumo ir atgrasymo principų“*[216].

ESTT ne kartą nurodė, kad nacionalinėje teisėje negalima visiškai laisvai nustatyti sankcijų.

Pavyzdys. Byloje *Von Colson ir Kamann prieš Land Nordrhein-Westfalen*[217] ESTT nurodė, kad visos valstybės narės, kurioms skirta direktyva, įpareigojamos savo nacionalinėse teisės sistemose nustatyti visas priemones, reikalingas jų visapusiškam veiksmingumui užtikrinti atsižvelgiant į tikslą, kurio siekiama šiomis priemonėmis. Teismas nusprendė, kad nors valstybės narės pačios gali pasirinkti būdus ir priemones, kuriomis būtų užtikrinamas direktyvos įgyvendinimas, ši laisvė nedaro poveikio joms nustatytam įpareigojimui. Veiksminga teisinė teisių gynimo priemonė visų pirma reiškia, kad asmuo gali naudotis atitinkama teise ir užtikrinti, kad ji būtų vykdoma visa apimtimi. Siekiant užtikrinti šią tikrą ir veiksmingą apsaugą, teisinės teisių gynimo priemonės turi būti susijusios su baudžiamosiomis ir (arba) kompensavimo procedūromis, kurias išnagrinėjus būtų skiriamos atgrasomojo pobūdžio sankcijos.

216 2012 m. spalio 1 d. *Europos Sąjungos pagrindinių teisių agentūros nuomonės Nr. 2/2012 dėl siūlomo duomenų apsaugos dokumentų rinkinio*, Viena, p. 27.

217 1984 m. balandžio 10 d. ESTT sprendimas C-14/83 *Sabine von Kolson ir Elisabeth Kamann prieš Land Nordrhein-Westfalen*.

Kalbant apie sankcijas už ES institucijų arba įstaigų padarytus ES teisės pažeidimus pažymėtina, kad, atsižvelgiant į specifinę ES institucijų duomenų apsaugos reglamento taikymo sritį, jame numatytos tik drausminio pobūdžio sankcijos. Pagal reglamento 49 straipsnį, „jeigu pareigūnas ar kitas Europos Bendrijų tarnautojas tyčia ar per aplaidumą nevykdo šiame reglamente nustatytų įsipareigojimų, <...> jam gali būti iškelta drausminė byla“.

6

Valstybės sienas kertančių duomenų srautai

ES	Aptariami klausimai	ET
Valstybės sienas kertančių duomenų srautai		
Duomenų apsaugos direktyvos 25 straipsnio 1 dalis. 2003 m. lapkričio 6 d. ESTT sprendimas *Bodil Lindqvist* C-101/01.	**Apibrėžtis.**	Konvencijos Nr. 108 papildomo protokolo 2 straipsnio 1 dalis.
Laisvas duomenų srautas		
Duomenų apsaugos direktyvos 1 straipsnio 2 dalis.	**Tarp ES valstybių narių.**	
	Duomenų srautas tarp Konvencijos Nr. 108 susitariančiųjų šalių.	Konvencijos Nr. 108 12 straipsnio 2 dalis.
Duomenų apsaugos direktyvos 25 straipsnis.	**Duomenų srautas į trečiąsias valstybes, kuriose užtikrinamas tinkamas duomenų apsaugos lygis.**	Konvencijos Nr. 108 papildomo protokolo 2 straipsnio 1 dalis.
Duomenų apsaugos direktyvos 26 straipsnio 1 dalis.	**Duomenų srautas į trečiąsias valstybes konkrečiais atvejais.**	Konvencijos Nr. 108 papildomo protokolo 2 straipsnio 2 dalies a punktas.

ES	Aptariami klausimai	ET
Apribotas duomenų srautas į trečiąsias valstybes		
Duomenų apsaugos direktyvos 26 straipsnio 2 dalis. Duomenų apsaugos direktyvos 26 straipsnio 4 dalis.	**Sutarties sąlygos.**	Konvencijos Nr. 108 papildomo protokolo 2 straipsnio 2 dalies b punktas. Sutarties sąlygų rengimo gairės.
Duomenų apsaugos direktyvos 26 straipsnio 2 dalis.	**Įmonei privalomos taisyklės.**	
Pavyzdžiai: ES ir JAV PNR susitarimas. ES ir JAV SWIFT susitarimas.	**Specialūs tarptautiniai susitarimai.**	

Duomenų apsaugos direktyvoje ne tik numatytas laisvas duomenų srautas tarp valstybių narių, bet ir pateikiamos nuostatos dėl asmens duomenų perdavimo į trečiąsias valstybes, esančias už ES ribų, reikalavimų. ET taip pat pripažino valstybės sienas kertančių duomenų srautų į trečiąsias valstybes svarbą ir 2001 m. priėmė Konvencijos Nr. 108 papildomą protokolą. Į šį protokolą perkeltos pagrindinės valstybės sienas kertančių duomenų srautus reguliuojančios nuostatos, kurios galioja konvencijos šalyse ir ES valstybėse narėse.

6.1. Valstybės sienas kertančių duomenų srautų pobūdis

Pagrindinis faktas

- Valstybės sienas kertančių duomenų srautas – tai asmens duomenų perdavimas duomenų gavėjui, kuris priklauso užsienio jurisdikcijai.

Konvencijos Nr. 108 papildomo protokolo 2 straipsnio 1 dalyje valstybės sienas kertančių duomenų srautas aprašomas kaip asmens duomenų perdavimas duomenų gavėjui, kuris priklauso užsienio jurisdikcijai. Duomenų apsaugos direktyvos 25 straipsnio 1 dalyje reglamentuojamas „asmens duomenų, kurie yra tvarkomi arba kuriuos juos perdavus ketinama tvarkyti, perdavimas į trečiąją šalį <...>“. Toks duomenų perdavimas yra leidžiamas tik vadovaujantis Konvencijos Nr. 108

papildomo protokolo 2 straipsnyje nustatytomis taisyklėmis, o ES valstybių narių atveju – taip pat Duomenų apsaugos direktyvos 25 ir 26 straipsniais.

Pavyzdys. Byloje *Bodil Lindqvist*[218] 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“ Direktyvos 95/46 3 straipsnio 1 dalies prasme“.

Paskui Teismas nurodė, kad direktyvoje taip pat nustatytos konkrečios taisyklės, kuriomis siekiama leisti valstybėms narėms stebėti asmens duomenų perdavimą į trečiąsias valstybes.

Tačiau, atsižvelgiant, pirma, į interneto technologijų pažangą direktyvos rengimo metu ir, antra, į tai, kad direktyvoje nėra interneto naudojimui taikomų kriterijų, „negalima preziumuoti, kad Bendrijos teisės aktų leidėjas į sąvoką „duomenų perdavimas į trečiąsias šalis“ ketino įtraukti <...> duomenų įrašymą į interneto puslapį, net jeigu jie dėl to tampa prieinami trečiųjų šalių asmenims, turintiems prieigai reikalingas priemones“.

Kita vertus, jei direktyva būtų „aiškinama taip, kad duomenys teikiami į trečiąsias šalis kiekvieną kartą, kai asmens duomenys įkraunami į interneto puslapį, šis perdavimas neišvengiamai būtų perdavimas į visas trečiąsias šalis, kur yra prieiti prie interneto reikalingos techninės priemonės. Taip (direktyvoje) numatyta speciali tvarka, kiek tai susiję su operacijomis internete, neišvengiamai taptų bendrąja tvarka. Kai tik <...> Komisija nustatytų, kad bent viena trečioji šalis neužtikrina tinkamos apsaugos, valstybės narės turėtų visiškai uždrausti pateikti asmens duomenis internete“.

Principas, kuriuo vadovaujantis daroma prielaida, kad vien (asmens) duomenų paskelbimas nėra laikomas valstybės sienas kertančių duomenų srautu, taikomas ir internetu prieinamiems viešiems registrams arba visuomenės informavimo priemonėms, pvz., (elektroniniams) laikraščiams ir televizijai. Tik konkretiems duomenų gavėjams skirtas pranešimas gali būti laikomas atitinkančiu valstybės sienas kertančių duomenų srauto koncepciją.

218 2003 m. lapkričio 6 d. ESTT sprendimo *Bodil Lindqvist*, C-101/01, 27, 68 ir 69 punktai.

6.2. Laisvas duomenų judėjimas tarp valstybių narių arba susitariančiųjų šalių

Pagrindinis faktas

- Asmens duomenų perdavimui į kitą Europos ekonominės erdvės valstybę narę arba Konvencijos Nr. 108 susitariančiąją šalį neturi būti taikomi jokie apribojimai.

Pagal Konvencijos Nr. 108 12 straipsnio 2 dalį **ET teisėje** turi būti užtikrinamas laisvas asmens duomenų judėjimas tarp konvencijos šalių. Vidaus teisėje negali būti nustatyti asmens duomenų perdavimo į susitariančiąsias šalis apribojimai, išskyrus atvejus, kai:

- to reikia atsižvelgiant į duomenų pobūdį[219] arba
- apribojimas yra būtinas siekiant išvengti vidaus teisės nuostatų, susijusių su valstybės sienas kertančių duomenų srautu į trečiąsias valstybes, netaikymo atvejais[220].

ES teisėje laisvo duomenų judėjimo tarp valstybių narių apribojimai, pagrįsti su duomenų apsauga susijusiomis priežastimis, yra draudžiami Duomenų apsaugos direktyvos 1 straipsnio 2 dalyje. Laisvo duomenų judėjimo taikymo sritis praplėsta Europos ekonominės erdvės (EEE) susitarimu[221], kuriuo į vidaus rinką įtraukiama Islandija, Lichtenšteinas ir Norvegija.

Pavyzdys. Jeigu keliose ES valstybėse narėse, įskaitant Slovėniją ir Prancūziją, įsikūrusios tarptautinės įmonių grupės filialas teikia asmens duomenis iš Slovėnijos į Prancūziją, toks duomenų teikimas negali būti ribojamas arba draudžiamas Slovėnijos nacionalinėje teisėje.

219 Konvencijos Nr. 108 12 straipsnio 3 dalies a punktas.

220 *Ibid.*, 12 straipsnio 3 dalies b punktas.

221 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.

Tačiau jeigu tas pats Slovėnijos filialas nori teikti tuos pačius asmens duomenis Jungtinėse Valstijose įsikūrusiai motininei bendrovei, Slovėnijos duomenų teikėjas privalo laikytis Slovėnijos teisėje nustatytos valstybės sienas kertančių duomenų srautui į trečiąsias valstybes, kuriose neužtikrinama tinkama duomenų apsauga, taikomos procedūros, išskyrus atvejus, kai motininė bendrovė laikosi „saugaus uosto privatumo“ principų, t. y. savanoriško tinkamos duomenų apsaugos užtikrinimo elgesio kodekso (žr. 6.3.1 dalį).

Tačiau valstybės sienas kertančių duomenų srautams į EEE valstybes nares siekiant duomenis teikti už vidaus rinkos ribų, pvz., tiriant nusikaltimus, Duomenų apsaugos direktyvos nuostatos netaikomos ir todėl nepatenka į laisvo duomenų judėjimo taikymo sritį. Kalbant apie ET teisę pažymėtina, kad į Konvencijos Nr. 108 ir jos papildomo protokolo taikymo sritį patenka visos sritys, tačiau susitariančiosios šalys gali numatyti išimtis. Konvencijos Nr. 108 susitariančiosiomis šalimis yra visos EEE valstybės narės.

6.3. Laisvas duomenų judėjimas į trečiąsias valstybes

Pagrindiniai faktai

- Asmens duomenų perdavimas į trečiąsias valstybes nacionaliniuose duomenų apsaugos įstatymuose nėra ribojamas, jeigu:
  - nustatyta, kad duomenų gavėjas užtikrina tinkamą duomenų apsaugą, arba
  - tai yra būtina atsižvelgiant į konkrečius duomenų subjekto interesus arba teisėtus svarbius kitų asmenų interesus, visų pirma viešąjį interesą.
- Tinkama duomenų apsauga trečiojoje valstybėje reiškia, kad šios valstybės nacionalinėje teisėje veiksmingai įgyvendinti pagrindiniai duomenų apsaugos principai.
- ES teisėje nustatyta, kad trečiojoje valstybėje užtikrinamą duomenų apsaugos tinkamumą vertina Europos Komisija. ET teisėje numatyta, kad duomenų apsaugos tinkamumo vertinimo procedūros nustatomos vidaus teisėje.

6.3.1. Laisvas duomenų judėjimas atsižvelgiant į tinkamą duomenų apsaugą

Pagal **ET teisę** laisvas duomenų judėjimas į valstybes, kurios nėra susitariančiosios šalys, leidžiamas, jeigu valstybė arba organizacija duomenų gavėja užtikrina tinkamą ketinamo atlikti duomenų perdavimo apsaugos lygį[222]. Vidaus teisėje nustatoma duomenų apsaugos lygio vertinimo užsienio valstybėje tvarka ir subjektai, kurie turėtų atlikti tokį vertinimą.

Pagal **ES teisę** laisvas duomenų judėjimas į trečiąsias valstybes, kuriose užtikrinama tinkama duomenų apsauga, numatytas Duomenų apsaugos direktyvos 25 straipsnio 1 dalyje. Būtent tinkamumo, o ne lygiavertiškumo reikalavimas sudaro sąlygas atsižvelgti į skirtingus duomenų apsaugos įgyvendinimo būdus. Pagal direktyvos 25 straipsnio 6 dalį Europos Komisija, priimdama išvadas dėl tinkamumo, turi kompetenciją įvertinti duomenų apsaugos lygį užsienio valstybėse, ir šiuo atveju dėl vertinimo ji konsultuojasi su 29 straipsnio duomenų apsaugos darbo grupe, kuri padėjo iš esmės išaiškinti direktyvos 25 ir 26 straipsnius[223].

Europos Komisijos išvada dėl tinkamumo turi privalomą galią. Jeigu Europos Komisija *Europos Sąjungos oficialiajame leidinyje* paskelbia išvadą dėl tinkamumo, susijusią su tam tikra valstybe, visos EEE valstybės narės ir jų institucijos turi vadovautis Europos Komisijos sprendimu ir tai reiškia, kad duomenų srautas į šią valstybę gali vykti nacionalinėms valdžios institucijoms neatliekant patikrinimo arba licencijavimo procedūrų[224].

Europos Komisija taip pat gali įvertinti valstybės teisinės sistemos dalis arba nustatyti konkrečius klausimus, kuriuos ji vertins. Pavyzdžiui, Europos Komisija priėmė išvadą dėl tinkamumo, susijusią tik su Kanados privatinės komercinės teisės aktais[225]. Taip pat priimta keletas išvadų dėl tinkamumo, susijusių su duomenų

222 Konvencijos Nr. 108 papildomo protokolo 2 straipsnio 1 dalis.

223 Žr., pvz., 29 straipsnio duomenų apsaugos darbo grupė (2003 m.), 2003 m. birželio 3 d. *Darbo dokumentas dėl asmens duomenų perdavimo trečiosioms valstybėms: ES duomenų apsaugos direktyvos 26 straipsnio 2 dalies taikymas įmonei privalomoms taisyklėms, susijusioms su tarptautiniu duomenų perdavimu,* WP 74, Briuselis; ir 29 straipsnio duomenų apsaugos darbo grupė (2005 m.), 2005 m. lapkričio 25 d. *Darbo dokumentas dėl 1995 m. spalio 24 d. Direktyvos 95/46/EB 26 straipsnio 1 dalies vienodo aiškinimo*, WP 114, Briuselis.

224 Nuolat atnaujinamą valstybių, dėl kurių priimta išvada dėl tinkamumo, sąrašą galima rasti Europos Komisijos Teisingumo generalinio direktorato pradžios tinklalapyje adresu http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm.

225 2001 m. gruodžio 20 d. Komisijos 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.

perdavimu, vadovaujantis ES ir užsienio valstybių susitarimais. Šiuose sprendimuose aptariama tik viena duomenų perdavimo rūšis, pvz., oro bendrovių užsienio pasienio kontrolės institucijoms teikiami keleivio duomenų įrašai, kai orlaivis iš ES skrenda į tam tikras užjūrio teritorijas (žr. 6.4.3 dalį). Pastaruoju metu ES ir trečiųjų valstybių konkrečiuose susitarimuose dėl duomenų perdavimo nereikalaujama priimti išvadų dėl tinkamumo ir daroma prielaida, kad pačiame susitarime yra nustatyta tinkama duomenų apsauga[226].

Vienas svarbiausių sprendimų dėl tinkamumo elementų nėra faktiškai susijęs su teisinių nuostatų rinkiniu[227]. Tiesą sakant, jis yra susijęs su elgesio kodeksu, vadinamaisiais „saugaus uosto privatumo" principais. Šiuos JAV verslo bendrovėms skirtus principus sukūrė ES ir Jungtinės Valstijos. Narystė „saugiame uoste" užtikrinama savanorišku įsipareigojimu JAV komercijos departamente ir šis įsipareigojimas įtraukiamas į šio departamento skelbiamą sąrašą. Vienas iš svarbių duomenų apsaugos tinkamumo elementų yra veiksmingas duomenų apsaugos įgyvendinimas, todėl „saugaus uosto" susitarime taip pat numatytas tam tikras valstybinės priežiūros lygis: prie „saugaus uosto" gali prisijungti tik tos įmonės, kurias prižiūri JAV federalinė prekybos komisija.

6.3.2. Laisvas duomenų judėjimas konkrečiais atvejais

Pagal ET teisę Konvencijos Nr. 108 papildomo protokolo 2 straipsnio 2 dalyje leidžiama asmens duomenis teikti į trečiąsias valstybes, kuriose neužtikrinama tinkama duomenų apsauga, jeigu duomenų teikimas numatytas vidaus teisėje ir yra būtinas:

- atsižvelgiant į konkrečius duomenų subjekto interesus arba
- atsižvelgiant į teisėtus svarbesnius kitų asmenų interesus, visų pirma viešąjį interesą.

226 Pavyzdžiui, Jungtinių Amerikos Valstijų ir Europos Sąjungos susitarimas dėl keleivio duomenų įrašų naudojimo ir perdavimo Jungtinių Valstijų Vidaus saugumo departamentui (OL L 215, 2012, p. 5–14) arba Europos Sąjungos ir Jungtinių Amerikos Valstijų susitarimas dėl finansinių mokėjimų pranešimų duomenų tvarkymo ir perdavimo iš Europos Sąjungos į Jungtines Valstijas terorizmo finansavimo sekimo programos tikslais (OL L 8, 2010, p. 11–16).

227 2000 m. liepos 26 d. Komisijos sprendimas 2000/520/EB dėl Europos Parlamento ir Tarybos direktyvos 95/46/EB dėl saugaus uosto privatumo principų teikiamos apsaugos pakankamumo ir su tuo susijusių JAV komercijos departamento pateiktų Dažnai užduodamų klausimų, OL L 215, 2000.

Pagal ES teisę Duomenų apsaugos direktyvos 26 straipsnio 1 dalyje įtvirtintos nuostatos, kurios yra panašios į Konvencijos Nr. 108 papildomo protokolo nuostatas.

Pagal direktyvą laisvas duomenų judėjimas į trečiąją valstybę gali būti pagrįstas duomenų subjekto interesais, jeigu:

- duomenų subjektas davė nedviprasmišką sutikimą teikti duomenis arba
- duomenų subjektas sudaro arba rengiasi sudaryti sutartį, kurioje aiškiai reikalaujamas duomenų teikimas duomenų gavėjui užsienyje, arba
- duomenų subjekto labui buvo sudaryta duomenų valdytojo ir trečiosios šalies sutartis, arba
- duomenis teikti būtina, kad būtų apsaugoti gyvybiniai duomenų subjekto interesai;
- duomenis reikia teikti iš viešųjų registrų; tai yra su svarbesniais interesais susijęs atvejis, kai plačiajai visuomenei turi būti sudaromos sąlygos susipažinti su viešuosiuose registruose laikoma informacija.

Kitų asmenų teisėtais interesais laisvas valstybės sienas kertančių duomenų judėjimas gali būti pagrįstas[228]:

- atsižvelgiant į svarbų viešąjį interesą, išskyrus su nacionaliniu arba visuomenės saugumu susijusius klausimus, kadangi Duomenų apsaugos direktyva jiems netaikoma, arba
- siekiant pateikti, vykdyti arba ginti teisinius reikalavimus.

Pirmiau nurodyti du atvejai turi būti suprantami kaip taisyklė, pagal kurią reikalaujama, kad nevaržomas duomenų teikimas į trečiąsias valstybes būtų vykdomas, jeigu valstybėje duomenų gavėjoje užtikrinamas tinkamas duomenų apsaugos lygis, taikomos išimtys. Išimtys visada turi būti aiškinamos siaurai. Šią nuostatą ne kartą pabrėžė 29 straipsnio duomenų apsaugos darbo grupė aiškindama Duomenų apsaugos direktyvos 26 straipsnio 1 dalį, visų pirma jeigu duomenų teikimo pagrindą

228 Duomenų apsaugos direktyvos 26 straipsnio 1 dalies d punktas.

sudaro sutikimas[229]. 29 straipsnio duomenų apsaugos darbo grupė priėjo prie išvados, kad bendrosios taisyklės, susijusios su sutikimo teisine svarba, taip pat taikomos direktyvos 26 straipsnio 1 daliai. Jeigu, pvz., darbo santykiuose neaišku, ar darbuotojų duotas sutikimas iš tikrųjų buvo duotas laisvai, tuomet duomenų teikimas negali būti grindžiamas direktyvos 26 straipsnio 1 dalies a punktu. Tokiais atvejais bus taikoma 26 straipsnio 2 dalis, kurioje reikalaujama, kad nacionalinės duomenų apsaugos institucijos išduotų licenciją duomenims teikti.

6.4. Duomenų judėjimo į trečiąsias valstybes ribojimai

Pagrindiniai faktai

- Prieš teikdamas duomenis į trečiąsias valstybes, kuriose neužtikrinamas tinkamas duomenų apsaugos lygis, duomenų valdytojas gali būti įpareigotas perduoti priežiūros institucijai nagrinėti planuojamo duomenų teikimo atvejį.
- Duomenis teikti norintis duomenų valdytojas per šią nagrinėjimo procedūrą privalo pateikti įrodymus dviem klausimais:
  - kad duomenų teikimas duomenų gavėjui yra pagrįstas teisiniu pagrindu ir
  - kad duomenų gavėjas yra nustatęs tinkamą duomenų apsaugą padedančias užtikrinti saugumo priemones.
- Priemonės, padedančios nustatyti, ar duomenų gavėjas užtikrina tinkamą duomenų apsaugą, gali apimti:
  - duomenis teikiančio duomenų valdytojo ir užsienio duomenų gavėjo nustatytas sutarties sąlygas arba
  - įmonei privalomas taisykles, kurios paprastai taikomos duomenų teikimui tarptautinių įmonių grupėje.
- Duomenų teikimo užsienio institucijoms tvarka taip pat gali būti reglamentuojama konkrečia tarptautine sutartimi.

Duomenų apsaugos direktyvoje ir Konvencijos Nr. 108 papildomame protokole numatyta, kad vidaus teisėje galima nustatyti valstybės sienas kertančių duomenų

229 Visų pirma žr. 29 straipsnio duomenų apsaugos darbo grupė (2005 m.), 2005 m. lapkričio 25 d. *Darbo dokumentas dėl 1995 m. spalio 24 d. Direktyvos 95/46/EB 26 straipsnio 1 dalies vienodo aiškinimo*, WP 114, Briuselis.

srautų į trečiąsias valstybes, kuriose neužtikrinamas tinkamas duomenų apsaugos lygis, režimą, jeigu duomenų valdytojas nustatė konkrečias taisykles, užtikrinančias, kad duomenų gavėjas turėtų tinkamas duomenų apsaugos priemones, ir jeigu duomenų valdytojas gali tai įrodyti kompetentingai institucijai. Šis reikalavimas aiškiai minimas tik Konvencijos Nr. 108 papildomame protokole; tačiau laikomasi nuomonės, kad tai yra įprasta procedūra pagal Duomenų apsaugos direktyvą.

6.4.1. Sutarties sąlygos

ET teisėje ar **ES teisėje** minimos duomenis teikiančio duomenų valdytojo ir trečiosios valstybės gavėjos sutarties sąlygos, kuriomis galima pasinaudoti kaip priemone pakankamam duomenų gavėjo duomenų apsaugos lygiui užtikrinti.

ES lygmeniu Europos Komisija, padedama 29 straipsnio duomenų apsaugos darbo grupės, parengė standartines sutarties sąlygas, kurios Komisijos sprendimu buvo oficialiai patvirtintos kaip tinkamos duomenų apsaugos įrodymas[230]. Kadangi Komisijos sprendimai valstybėms narėms yra privalomi visa apimtimi, nacionalinės institucijos, atsakingos už valstybės sienas kertančių duomenų srautųpriežiūrą, vykdydamos savo procedūras privalo paisyti šių standartinių sutarties sąlygų[231]. 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.

Dėl to, kad ES teisinėje sistemoje yra standartinės sutarties sąlygos, nedraudžiama duomenų valdytojams suformuluoti kitas *ad hoc* sutarties sąlygas. Tačiau tokiomis sąlygomis turėtų būti užtikrinamas toks pat apsaugos lygis, kuris numatytas standartinėse sutarties sąlygose. Svarbiausi standartinių sutarties sąlygų požymiai yra šie:

- trečiosios šalies labui nustatyta sąlyga, kuri sudaro sąlygas duomenų subjektams įgyvendinti sutartyje nustatytas teises, net jeigu ji nėra sutarties šalis;

- duomenų gavėjas arba importuotojas sutinka, kad jam ginčo atveju būtų taikoma duomenis teikiančio duomenų valdytojo nacionalinės priežiūros institucijos ir (arba) teismų procedūra.

230 Duomenų apsaugos direktyvos 26 straipsnio 4 dalis.

231 SESV 288 straipsnis.

Šiuo metu duomenų valdytojų tarpusavio duomenų teikimui taikomi du standartinių sąlygų rinkiniai, kurių vieną gali pasirinkti duomenis teikiantis duomenų valdytojas[232]. Kai duomenų valdytojas duomenis teikia duomenų tvarkytojui, galima pasinaudoti tik vienu standartiniu sutarčių sąlygų rinkiniu[233].

Kalbant apie **ET teisę** pažymėtina, kad Konvencijos Nr. 108 konsultacinis komitetas parengė sutarties sąlygų rengimo gaires[234].

6.4.2. Įmonei privalomos taisyklės

Rengiant daugiašales įmonei privalomas taisykles (angl. BCR) labai dažnai vienu metu dalyvauja keletas Europos duomenų apsaugos institucijų[235]. Kad BCR būtų patvirtintos, jų projektas, įskaitant standartines paraiškos formas, turi būti nusiųstas vadovaujančiajai institucijai[236]. Vadovaujančiąją instituciją galima nustatyti remiantis standartine paraiškos forma. Tuomet ši institucija informuoja visų EEE valstybių narių, kuriose įsisteigę grupės filialai, priežiūros institucijas, kurių dalyvavimas vertinant BCR vis dėlto yra savanoriškas. Nors tai nėra privaloma, visos susijusios duomenų apsaugos institucijos turėtų įtraukti vertinimo rezultatą į savo oficialias licencijavimo procedūras.

6.4.3. Specialūs tarptautiniai susitarimai

ES sudarė specialius susitarimus dėl dviejų rūšių duomenų perdavimo.

---

232 I rinkinys pateikiamas 2001 m. birželio 15 d. Komisijos sprendimo 2001/497/EB dėl sutarčių, susijusių su asmens duomenų perdavimu trečiosioms šalims, tipinių punktų, atsižvelgiant į Direktyvą 95/46/EB, OL L 181, 2001, priede; II rinkinys pateikiamas 2004 m. gruodžio 27 d. Komisijos sprendimo 2004/915/EB, iš dalies keičiančio Sprendimą 2001/497/EB dėl sutarčių, susijusių su asmens duomenų perdavimu trečiosioms šalims, tipinių punktų, OL L 385, 2004, priede.

233 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.

234 ET Konvencijos Nr. 108 konsultacinis komitetas (2002 m.), *Gairės dėl sutarties sąlygų, reglamentuojančių duomenų apsaugą teikiant duomenis į trečiąsias valstybes, kurios neprivalo užtikrinti tinkamo duomenų apsaugos lygio, rengimo*.

235 Tinkamų įmonei privalomų taisyklių turinį ir struktūrą paaiškina 29 straipsnio duomenų apsaugos darbo grupė (2008 m.), 2008 m. birželio 24 d. *Darbo dokumentas, kuriuo nustatoma įmonei privalomų taisyklių struktūra*, WP 154, Briuselis; ir 29 straipsnio duomenų apsaugos darbo grupė (2008 m.), 2008 m. birželio 24 d. *Darbo dokumentas, kuriuo nustatoma elementų ir principų, kurie turi būti numatyti įmonei privalomose taisyklėse, lentelė*, WP 153, Briuselis.

236 29 straipsnio duomenų apsaugos darbo grupė (2007 m.), 2007 m. sausio 10 d. *Rekomendacija Nr. 1/2007 dėl įmonėms privalomų taisyklių, taikomų asmens duomenų perdavimui duomenų tvarkymo veiklai, patvirtinimo paraiškos formą*, WP 133, Briuselis.

Keleivio duomenų įrašai

Keleivio duomenų įrašų (angl. PNR) duomenis rezervacijos metu renka oro vežėjai ir šiuos duomenis sudaro vardai ir pavardės, adresai, informacija apie kredito korteles ir oro keleivių vietų numerius. Pagal JAV teisę oro vežėjas turi pareigą leisti prieš keleiviui išvykstant su šiais duomenimis susipažinti Vidaus saugumo departamentui. Ši taisyklė taikoma skrydžiams į Jungtines Valstijas ir iš jų.

Siekiant užtikrinti tinkamą PNR duomenų apsaugą ir sutinkamai su Direktyvos 95/46/EB nuostatomis 2004 metais buvo priimtas „PNR paketas“[237]. Paketas, apėmė duomenų tvarkymo, kurį atlieka JAV Vidaus saugumo departamentas JAV (VSD), tinkamumą.

ESTT panaikinus PNR paketą[238] ES ir Jungtinės Amerikos Valstijos pasirašė du atskirus susitarimus turinčius dvejopą tikslą: pirma, numatyti teisinį pagrindą atskleisti PNR duomenis užsienio institucijoms ir antra, duomenis gaunančioje valstybėje užtikrinti tinkamą duomenų apsaugą.

Pirmas ES valstybių ir Jungtinių Valstijų susitarimas dėl dalijimosi duomenimis ir jų valdymo pasirašytas 2012 m., turėjo keletą trūkumų ir tais pačiais metais buvo pakeistas nauju susitarimu, kuriuo užtikrinamas didesnis teisinis tikrumas[239]. Naujajame susitarime numatyta svarbių patobulinimų. Jame apribojami ir paaiškinami tikslai, kuriais galima naudoti informaciją, pvz., sunkūs tarptautiniai nusikaltimai ir terorizmas ir nustatomas laikotarpis, kurį duomenys gali būti saugomi: po šešių mėnesių, duomenys turi būti nuasmeninti ir užmaskuoti. Jeigu duomenys netinkamai naudojami, kiekvienas turi teisę pagal JAV teisę pasinaudoti administracinėmis ir teisminėmis savo teisių gynimo priemonėmis. Taip pat turi teisę susipažinti su savo

237 2004 m. gegužės 17 d. Tarybos sprendimas 2004/496/EB dėl susitarimo tarp Europos Bendrijų ir Jungtinių Amerikos Valstijų susitarimo dėl oro vežėjų atliekamo PNR duomenų tvarkymo ir perdavimo Jungtinių Valstijų Vidaus saugumo departamentui, Muitinės ir sienos apsaugos biuro, OL 2004 L 183, p. 83 ir 2004 gegužės 14 d. Komisijos sprendimas 2004/535/EB dėl oro vežėjų keleivio duomenų įraše teikiamų asmens duomenų Jungtinių Valstijų Muitinės ir sienos apsaugos biurui, OL 2004 L 235, p. 11-22.

238 2006 gegužės 30 d. ESTT sujungtos bylos C-317/04 ir C-318/04 *Europos Parlamentas prieš Europos Sąjungos Tarybą*, 57, 58 ir 59 paragrafai, kuriuose Teisingumo Teismas nusprendė, kad tiek sprendimas dėęl tinkamo apsaugos lygio tiek ir susitarimas dėl duomenų tvarkymo, yra direktyvos taikymo srities išimtys.

239 2012 m. balandžio 26 d. Tarybos sprendimas 2012/472/ES dėl Jungtinių Amerikos Valstijų ir Europos Sąjungos susitarimo dėl keleivio duomenų įrašų naudojimo ir perdavimo Jungtinių Valstijų vidaus saugumo departamentui sudarymo, OL L 215/4, 2012. Susitarimo tekstas pridedamas prie šio sprendimo, OL L 215, 215, p. 5–14.

PNR duomenimis ir prašyti, kad Vidaus saugumo departamentas juos ištaisytų, įskaitant galimybę juos ištrinti, jeigu informacija nėra tiksli.

Susitarimas, kuris įsigaliojo 2012 m. birželio 1 d., galioja septynerius metus, t. y. iki 2019 m.

2011 m. Europos Sąjungos Taryba patvirtino atnaujintą ES ir Australijos sudarytą susitarimą dėl PNR duomenų tvarkymo ir perdavimo[240]. ES ir Australijos susitarimas dėl PNR duomenų yra kitas ES darbotvarkės klausimas, susijęs su pasaulinėmis PNR gairėmis[241], ES PNR schemos sukūrimu[242] ir derybomis su trečiosiomis valstybėmis dėl susitarimo[243].

Finansinių pranešimų duomenys

Belgijoje įsikūrusi Pasaulinė tarpbankinių finansinių telekomunikacijų organizacija (angl. SWIFT), kuri yra daugumos Europos bankų atliekamų pasaulinių pinigų pervedimo operacijų duomenų tvarkytoja, valdžiusi „veidrodini" centrą Jungtinėse Valstijose ir jai buvo pateiktas prašymas terorizmo tyrimo tikslais atskleisti duomenis JAV iždo departamentui[244].

240 2011 m. gruodžio 13 d. Tarybos sprendimas 2012/381/ES dėl Europos Sąjungos ir Australijos susitarimo dėl oro vežėjų atliekamo keleivio duomenų įrašo (PNR) duomenų tvarkymo ir perdavimo Australijos muitinės ir sienos apsaugos tarnybai sudarymo, OL L 186/3, 2012. Susitarimo tekstas, kuris pakeitė 2008 m. susitarimą, pridedamas prieš šio sprendimo, OL L 186, 2012, p. 4–16.

241 Visų pirma žr. 2010 m. rugsėjo 21 d. Komisijos komunikatą dėl keleivio duomenų įrašo (PNR) duomenų perdavimo trečiosioms šalims bendros koncepcijos, KOM(2010) 492 galutinis, Briuselis. Taip pat žr. 29 straipsnio duomenų apsaugos darbo grupė (2010), Nuomonė Nr. 7/2010 dėl Europos Komisijos komunikato dėl keleivio duomenų įrašo (PNR) duomenų perdavimo trečiosioms šalims bendros koncepcijos. WP 178, Briuselis, 2010 m. lapkričio12 d.

242 2011 m. vasario 2 d. Europos Parlamento ir Tarybos pasiūlymas dėl direktyvos dėl keleivio duomenų įrašo duomenų naudojimo teroristinių nusikaltimų ir sunkių nusikaltimų prevencijos, nustatymo, tyrimo ir patraukimo už juos baudžiamojon atsakomybėn tikslais, KOM(2011) 32 galutinis, Briuselis. 2011 m. balandžio mėn. Europos Parlamentas paprašė Europos Sąjungos pagrindinių teisių agentūros pateikti nuomonę dėl šio pasiūlymo ir jo atitikties Europos Sąjungos pagrindinių teisių chartijai. Žr. FRA (2011 m.), 2011 m. birželio 14 d. *Nuomonė Nr. 1/2011 dėl keleivio duomenų įrašo*, Viena.

243 ES derasi dėl naujo PNR susitarimo su Kanada, kuris pakeis šiuo metu galiojantį 2006 m. susitarimą.

244 Šiuo atžvilgiu žr. 29 straipsnio duomenų apsaugos darbo grupė (2011 m.), 2011 m. birželio 13 d. *Nuomonė Nr. 14/2011 dėl duomenų apsaugos klausimų, susijusių su pinigų plovimu ir teroristų finansavimu*, WP 186, Briuselis; 29 straipsnio duomenų apsaugos darbo grupė (2006 m.), 2006 m. lapkričio 22 d. *Nuomonė Nr. 10/2006 dėl Pasaulinės tarpbankinių finansinių telekomunikacijų organizacijos (SWIFT) atliekamo asmens duomenų tvarkymo*, WP 128, Briuselis; 2008 m. gruodžio 9 d. Belgijos privatumo apsaugos komisijos (pranc. *Commission de la protection de la vie privée*) sprendimą *„Kontrolės ir rekomendacijų procedūra, kuri pradėta atsižvelgiant į įmonę „SWIFT scrl""*.

ES lygmeniu nebuvo jokio tinkamo teisinio pagrindo atskleisti šiuos iš esmės europinius duomenis, su kuriais Jungtinės Valstijos galėjo susipažinti tik dėl to, kad SWIFT duomenų tvarkymo centrai buvo įkurti Jungtinėse Valstijose.

2010 m. buvo sudarytas specialus ES ir Jungtinių Valstijų susitarimas (vadinamasis SWIFT susitarimas), kuriuo siekiama numatyti būtiną teisinį pagrindą ir užtikrinti tinkamą duomenų apsaugą[245].

Pagal šį susitarimą SWIFT saugomi finansiniai duomenys JAV iždo departamentui vis dar teikiami teroristinių nusikaltimų arba terorizmo finansavimo prevencijos, tyrimo, nustatymo ar patraukimo baudžiamojon atsakomybėn už juos tikslais. JAV iždo departamentas gali prašyti SWIFT pateikti finansinius duomenis, jeigu prašyme:

- kuo aiškiau nurodomi finansiniai duomenys;
- aiškiai pagrindžiamas tokių duomenų būtinumas;
- pateikiamas kuo siauresnis aprašymas, kad būtų pateiktas kuo mažesnis prašomų duomenų kiekis;
- neprašoma pateikti kokių nors duomenų, susijusių su bendra mokėjimų eurais erdve (angl. SEPA).

Europolas privalo gauti kiekvieno JAV iždo departamento prašymo kopiją ir patikrinti, ar laikomasi SWIFT susitarimo principų[246]. Europolui patvirtinus, kad šių principų laikomasi, SWIFT privalo pateikti finansinius duomenis tiesiogiai JAV iždo departamentui. 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. Paprastai iš SWIFT gauti finansiniai duomenys ištrinami ne vėliau kaip per penkerius metus nuo jų gavimo. Finansiniai duomenys, kurie yra svarbūs tiriant konkrečius nusikaltimus arba vykdant jų baudžiamąjį persekiojimą,

245 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.

246 Europolo jungtinė priežiūros institucija šioje srityje atliko Europolo veiklos auditus, su kurių rezultatais galima susipažinti adresu: http://europoljsb.consilium.europa.eu/reports/inspection-report.aspx?lang=en.

gali būti saugomi tiek, kiek jie yra būtini šiems tyrimams arba baudžiamiesiems persekiojimams vykdyti.

JAV iždo departamentas gali teikti su SWIFT pateiktais duomenimis susijusią informaciją konkrečioms teisėsaugos, viešo saugumo arba kovos su terorizmu institucijoms, esančioms Jungtinėse Valstijose arba už jų ribų, tik teroristinių nusikaltimų tyrimo, nustatymo, prevencijos ir patraukimo baudžiamojon atsakomybėn 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 užkirsti kelią staigiam ir dideliam pavojui visuomenės saugumui.

Nepriklausomi prižiūrėtojai, įskaitant Europos Komisijos paskirtą asmenį, stebi, kaip laikomasi SWIFT susitarimo principų.

Duomenų subjektai turi teisę gauti kompetentingos ES duomenų apsaugos institucijos patvirtinimą, kad jų asmens duomenų apsaugos teisės nėra pažeidžiamos. Duomenų subjektai taip pat turi teisę reikalauti, kad jų duomenys, kuriuos JAV iždo departamentas surinko ir saugojo pagal SWIFT susitarimą, būtų ištaisyti, sunaikinti arba užblokuoti. Tačiau duomenų subjektų teisėms susipažinti su duomenimis gali būti taikomi tam tikri teisiniai apribojimai. Atsisakius leisti susipažinti su duomenimis, duomenų subjektas turi būti informuojamas raštu apie tokį atsisakymą ir teisę ginti savo teises Jungtinėse Valstijose administracinėmis ir teisminėmis gynimo priemonėmis.

SWIFT susitarimas galioja penkerius metus, t. y. 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.

7

Duomenų apsauga policijos ir baudžiamosios teisenos srityje

ES	Aptariami klausimai	ET
	Bendro pobūdžio.	Konvencija Nr. 108.
	Policija.	Rekomendacija dėl policijos.
		2009 m. gruodžio 17 d. EŽTT sprendimas *B. B. prieš Prancūziją*, Nr. 5335/06.
		2008 m. gruodžio 4 d. EŽTT sprendimas *S. ir Marper prieš Jungtinę Karalystę*, Nr. 30562/04 ir 30566/04.
		2005 m. gegužės 31 d. EŽTT sprendimas *Vetter prieš Prancūziją*, Nr. 59842/00.
	Elektroniniai nusikaltimai.	Konvencija dėl elektroninių nusikaltimų.
Duomenų apsauga policijos ir teisminių institucijų tarpvalstybinio bendradarbiavimo srityje		
Duomenų apsaugos pagrindų sprendimas.	**Bendro pobūdžio.**	Konvencija Nr. 108. Rekomendacija dėl policijos.
Priumo sprendimas.	**Specialių duomenų apsauga: pirštų atspaudai, DNR, duomenys apie chuliganizmą ir t. t.**	Konvencija Nr. 108. Rekomendacija dėl policijos.
Europolo sprendimas. Eurojusto sprendimas. FRONTEX reglamentas.	**Duomenų apsauga specialiose agentūrose.**	Konvencija Nr. 108. Rekomendacija dėl policijos duomenų.

ES	Aptariami klausimai	ET
Šengeno II sprendimas. VIS reglamentas. Eurodac reglamentas. CIS sprendimas.	**Duomenų apsauga specialiose bendrose informacinėse sistemose**	Konvencija Nr. 108. Rekomendacija dėl policijos. 2010 m. vasario 2 d. EŽTT sprendimas *Dalea prieš Prancūziją*, Nr. 964/07.

Siekdamos nustatyti asmens interesų, susijusių su duomenų apsauga, ir visuomenės interesų, susijusių su duomenų rinkimu siekiant kovoti su nusikalstamumu ir užtikrinti nacionalinį ir visuomenės saugumą, pusiausvyrą ET ir ES nustatė specialias teisines priemones.

7.1. Duomenų apsauga sprendžiant policijos ir baudžiamosios teisenos klausimus pagal ET teisę

Pagrindiniai faktai

- Konvencijoje Nr. 108 ir ET rekomendacijoje dėl policijos aptariama duomenų apsauga visose policijos veiklos srityse.
- Konvencija dėl elektroninių nusikaltimų (*Budapešto konvencija*) yra teisiškai privaloma tarptautinė priemonė, kurioje reglamentuojami nusikaltimai elektroniniuose tinkluose naudojant elektronines priemones.

Europos lygmeniu Konvencija Nr. 108 apima visas asmens duomenų tvarkymo sritis ir šios konvencijos nuostatomis siekiama reglamentuoti asmens duomenų tvarkymą apskritai. Todėl Konvencija Nr. 108 taikoma duomenų apsaugai policijos ir baudžiamosios teisenos srityje, tačiau susitariančiosios šalys gali riboti jos taikymo sritį.

Policijos ir baudžiamosios teisenos institucijos, vykdydamos savo užduotis, dažnai turi tvarkyti asmens duomenis ir toks tvarkymas gali sukelti svarbias pasekmes susijusiems asmenims. ET 1987 m. priimtoje Rekomendacijoje dėl policijos duomenų susitariančiosioms šalims pateikiamos gairės, kaip jos turėtų praktiškai įgyvendinti Konvencijos Nr. 108 principus asmens duomenis tvarkant policijos institucijoms[247].

247 ET Ministrų Komitetas (1987 m.), 1987 m. rugsėjo 17 d. Rekomendacija Nr. R (87) 15 valstybėms narėms dėl asmens duomenų naudojimo policijos sektoriuje.

7.1.1. Rekomendacija dėl policijos

EŽTT ne kartą yra nusprendęs, kad policijos arba nacionalinių saugumo institucijų laikomi ir saugomi asmens duomenys reiškia EŽTK 8 straipsnio 1 dalies apribojimą. EŽTT priėmė nemažai sprendimų, kuriuose nagrinėjo tokių apribojimų pagrįstumą[248].

Pavyzdys. Byloje *B. B. prieš Prancūziją*[249] EŽTT nusprendė, kad asmens, nuteisto už seksualinį nusikaltimą, įtraukimas į nacionalinę teismų duomenų bazę pateko į EŽTK 8 straipsnio taikymo sritį. Tačiau, atsižvelgiant į tai, kad buvo įgyvendintos pakankamos duomenų apsaugos priemonės, pvz., duomenų subjekto teisė prašyti ištrinti duomenis, ribota duomenų saugojimo trukmė ir ribotos galimybės susipažinti su tokiais duomenimis, nuspręsta, kad buvo nustatyta tinkama privataus ir viešojo intereso pusiausvyra. Teismas nusprendė, kad EŽTK 8 straipsnis nebuvo pažeistas.

Pavyzdys. Byloje *S. ir Marper prieš Jungtinę Karalystę*[250] abiem pareiškėjams pareikšti kaltinimai dėl nusikaltimų, tačiau jie nebuvo nuteisti. Vis dėlto policija laikė ir saugojo jų pirštų atspaudus, DNR profilius ir ląstelių mėginius. Neribotos trukmės biometrinių duomenų saugojimas tais atvejais, kai asmuo buvo įtariamas padaręs nusikaltimą, nepaisant to, kad įtariamasis vėliau buvo išteisintas arba kaltinimai jam buvo atmesti, buvo numatytas įstatyme. EŽTT nusprendė, kad visa apimantis ir nediferencijuojamas asmens duomenų saugojimas, kurio terminas nebuvo nustatytas, kai išteisinti asmenys turėjo tik ribotas galimybes prašyti ištrinti duomenis, reiškė neproporcingą pareiškėjo teisės į privataus gyvenimo gerbimą ribojimą. Teismas nusprendė, kad EŽTK 8 straipsnis buvo pažeistas.

Nemažai kitų EŽTT sprendimų nagrinėjamas teisės į duomenų apsaugą apribojimo pagrįstumas taikant stebėjimo priemones.

Pavyzdys. Byloje *Allan prieš Jungtinę Karalystę*[251] institucijos slapta įrašinėjo kalinio ir jo draugo pokalbius kalinių lankymo salėje ir kalinio ir kito nuteistojo

248 Žr., pvz., 1987 m. kovo 26 d. EŽTT sprendimą *Leander prieš Švediją*, Nr. 9248/81; 2012 m. lapkričio 13 d. EŽTT sprendimą *M. M. prieš Jungtinę Karalystę*, Nr. 24029/07; 2013 m. balandžio 18 d. EŽTT sprendimą *M. K. prieš Prancūziją*, Nr. 19522/09.

249 2009 m. gruodžio 17 d. EŽTT sprendimas *B. B. prieš Prancūziją*, Nr. 5335/06.

250 2008 m. gruodžio 4 d. EŽTT sprendimo *S. ir Marper prieš Jungtinę Karalystę*, Nr. 30562/04 ir 30566/04, 119 ir 125 punktai.

251 2002 m. lapkričio 5 d. EŽTT sprendimas *Allan prieš Jungtinę Karalystę*, Nr. 48539/99.

pokalbius kalėjimo kameroje. EŽTT nusprendė, kad garso ir vaizdo įrašymo įrangos naudojimas pareiškėjo kalėjimo kameroje, kalinių lankymo salėje ir pokalbių su kartu kalinčiu nuteistuoju įrašinėjimas reiškė pareiškėjo teisės į privatų gyvenimą apribojimą. Kadangi įstatymuose tuo metu nebuvo nustatyta policijos slaptos įrašymo įrangos naudojimo tvarka, minėtas apribojimas neatitiko įstatymo. Teismas nusprendė, kad EŽTT 8 straipsnis buvo pažeistas.

Pavyzdys. Byloje *Klass ir kiti prieš Vokietiją*[252] pareiškėjai teigė, kad keli Vokietijos teisės aktai, kuriais buvo leidžiama slapta stebėti laiškus, pašto korespondenciją ir telekomunikacijas, pažeidė EŽTK 8 straipsnį, visų pirma todėl, kad susijęs asmuo nebuvo informuotas apie stebėjimo priemones ir negalėjo kreiptis į teismus po to, kai tokias priemones nustota naudoti. EŽTT nusprendė, kad stebėjimo grėsmė neabejotinai ribojo pašto ir telekomunikacijų paslaugų naudotojų susirašinėjimo laisvę. Tačiau EŽTT padarė išvadą, kad buvo nustatytos tinkamos apsaugos priemonės nuo piktnaudžiavimo. Vokietijos teisės aktai buvo pagrįsti atsižvelgiant į tai, kad tokios priemonės buvo būtinos demokratinėje visuomenėje atsižvelgiant į nacionalinio saugumo interesus ir siekiant užkirsti kelią neramumams arba nusikaltimams. Teismas nusprendė, kad EŽTK 8 straipsnis nebuvo pažeistas.

Kadangi policijos institucijų atliekamas duomenų tvarkymas gali turėti didelį poveikį susijusiems asmenims, šioje srityje ypač reikalingos išsamios duomenų apsaugos taisyklės, susijusios su duomenų bazių sukūrimu šioje srityje. ET rekomendacija dėl policijos siekta išspręsti šį klausimą pateikiant tokias gaires: kaip turėtų būti renkami duomenys policijos darbe; kaip turėtų būti laikomi duomenys šioje srityje; kam turėtų būti leidžiama susipažinti su rinkmenomis, įskaitant duomenų perdavimo užsienio policijos institucijoms sąlygas; kaip duomenų subjektai galėtų pasinaudoti savo duomenų apsaugos teisėmis ir kaip turėtų būti įgyvendinama nepriklausomų institucijų kontrolė. Taip pat aptariama pareiga užtikrinti tinkamą duomenų saugumą.

Rekomendacijoje nenumatyta, kad policijos institucijos gali rinkti bet kokius duomenis, jų nediferencijuodamos. Joje policijos institucijų renkami asmens duomenys ribojami atsižvelgiant į tai, kokie duomenys yra būtini siekiant užkirsti kelią realiam pavojui arba užkardyti konkretų nusikaltimą. Bet kokie papildomi duomenys turi būti renkami remiantis nacionalinės teisės aktuose nustatytais pagrindais. Turi būti tvarkomi tik tokie ypatingi duomenys, kurie yra neišvengiamai būtini atsižvelgiant į konkretų tyrimą.

252 1978 m. rugsėjo 6 d. EŽTT sprendimas *Klass ir kiti prieš Vokietiją*, Nr. 5029/71.

Kai asmens duomenys renkami be duomenų subjekto žinios, duomenų subjektas turi būti informuojamas apie duomenų rinkimą iš karto, kai toks atskleidimas nebetrukdo atlikti tyrimo. Domenų rinkimas techninėmis stebėjimo priemonėmis arba kitais automatiniais būdais taip pat turi būti pagrįstas konkrečiomis teisinėmis nuostatomis.

Pavyzdys. Byloje *Vetter prieš Prancūziją*[253] anoniminiai liudytojai apkaltino pareiškėją žmogžudyste. Kadangi pareiškėjas nuolat lankėsi draugo namuose, policija, gavusi bylą nagrinėjančio teisėjo leidimą, juose įrengė pasiklausymo įrangą. Remiantis įrašytais pokalbiais pareiškėjas buvo areštuotas ir apkaltintas žmogžudyste. Jis teigė, kad pokalbių įrašų įrodymai yra nepriimtini, nes tokia galimybė nenumatyta įstatyme. EŽTT iš esmės nagrinėjo klausimą, ar pasiklausymo įranga „atitiko įstatymą". Blakių įrengimas privačiose patalpose akivaizdžiai neatitiko Baudžiamojo proceso kodekso 100 ir kitų straipsnių, nes šios nuostatos buvo susijusios su telefoninių pokalbių klausymusi. Šio kodekso 81 straipsnyje nebuvo pakankamai aiškiai nurodyta institucijų diskrecija, susijusi su privačių pokalbių klausymosi sankcionavimu, taikymo sritimi arba būdais. Todėl pareiškėjas negalėjo pasinaudoti minimalia apsauga, teisę į kurią demokratinės visuomenės piliečiai turėjo pagal įstatymą. Teismas nusprendė, kad EŽTK 8 straipsnis buvo pažeistas.

Rekomendacijoje prieinama prie išvados, kad saugant asmens duomenis reikėtų aiškiai atskirti administracinius duomenis ir policijos duomenis, skirtingų rūšių duomenų subjektus, pvz., įtariamuosius, nuteistuosius, aukas ir liudytojus, ir duomenis, kurie laikomi patvirtintais faktais ir įtarimais arba spėlionėmis pagrįstais faktais.

Policijos duomenys turėtų turėti griežtai ribotą tikslą. Tai sukelia pasekmes policijos duomenis teikiant trečiosioms šalims: tokių duomenų perdavimas arba siuntimas policijos sektoriuje turėtų būti reglamentuojamas atsižvelgiant į tai, ar dalijimasis informacija yra pagrįstas teisėtu interesu. Tokių duomenų perdavimas arba siuntimas už policijos sektoriaus ribų turėtų būti leidžiamas tik tais atvejais, kai yra aiški teisinė pareiga arba leidimas. Tarptautinį duomenų perdavimą arba siuntimą turėtų atlikti tik užsienio policijos institucijos ir jis turėtų būti pagrįstas konkrečiomis teisinėmis nuostatomis, pvz., tarptautiniais susitarimais, išskyrus atvejus, kai duomenis teikti būtina siekiant užkirsti kelią dideliam ir neišvengiamam pavojui.

253 2005 m. gegužės 31 d. EŽTT sprendimas *Vetter prieš Prancūziją*, Nr. 59842/00.

Siekiant užtikrinti atitiktį vidaus duomenų apsaugos teisei, policijos tvarkomų duomenų priežiūrą turi atlikti nepriklausoma priežiūros institucija. Duomenų subjektams turi būti suteikiamos visos Konvencijoje Nr. 108 numatytos teisės susipažinti. Tais atvejais, kai, siekiant užtikrinti veiksmingus policijos tyrimus, duomenų subjektų teisės susipažinti buvo apribotos vadovaujantis Konvencijos Nr. 108 9 straipsniu, duomenų subjektas pagal nacionalinį įstatymą turi turėti teisę pateikti skundą nacionalinei duomenų apsaugos priežiūros institucijai arba kitai nepriklausomai įstaigai.

7.1.2. 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 nustatė tarptautinę teisinę priemonę, t. y. Konvenciją dėl elektroninių nusikaltimų (taip pat vadinama Budapešto konvencija), kad spręstų nusikaltimų prieš elektroninius tinklus ir nusikaltimų naudojant elektroninius tinklus problemą[254]. Prie šios konvencijos taip pat gali prisijungti ne ET valstybės narės ir iki 2013 m. prie konvencijos prisijungė keturios ET nepriklausančios valstybės (Australija, Dominikos Respublika, Japonija ir Jungtinės Valstijos), o 12 kitų ne ET valstybių narių pasirašė konvenciją arba buvo pakviestos prie jos prisijungti.

Konvencija dėl elektroninių nusikaltimų išlieka didžiausią įtaką turinčia tarptautine sutartimi, kurioje reglamentuojami interneto arba kitų informacijos tinklų teisės pažeidimai. Konvencijos šalys įpareigojamos atnaujinti ir suderinti savo baudžiamuosius įstatymus, susijusius su įsibrovimais ir kitais saugumo pažeidimais, įskaitant autorių teisių pažeidimus, sukčiavimą naudojant kompiuterius, vaikų pornografiją ir kitą neteisėtą elektroninę veiklą. Konvencijoje taip pat numatyti procesiniai įgaliojimai, susiję su kompiuterinių tinklų apžiūra ir ryšių perėmimu kovos su elektroniniais nusikaltimais tikslais. Galiausiai joje sudaromos sąlygos veiksmingam tarptautiniam bendradarbiavimui. Konvencijos papildomame protokole aptariami baudžiamosios atsakomybės už rasinę ir ksenofobinę propagandą kompiuteriniuose tinkluose numatymo klausimai.

Nors konvencija nėra duomenų apsaugą padedanti didinti priemonė, joje numatoma baudžiamoji atsakomybė už veikas, kuriomis gali būti pažeista duomenų subjektų

254 Europos Tarybos Ministrų Komitetas (2001 m.), 2001 m. lapkričio 23 d. Konvencija dėl elektroninių nusikaltimų, ET SS Nr. 185, Budapeštas; įsigaliojo 2004 m. liepos 1 d.

teisė į savo duomenų apsaugą. Joje konvenciją įgyvendinančios susitariančiosios šalys įpareigojamos taip pat numatyti tinkamą žmogaus teisių ir laisvių apsaugą, įskaitant EŽTK garantuojamas teises, pvz., teisę į duomenų apsaugą[255].

7.2. ES duomenų apsaugos teisė policijos ir baudžiamosiose bylose

Pagrindiniai faktai

- ES lygmeniu duomenų apsauga policijos ir baudžiamosios teisenos sektoriuje reglamentuojama tik tiek, kiek ji susijusi su policijos ir teisminių institucijų tarpvalstybiniu bendradarbiavimu.
- Specialaus duomenų apsaugos režimo laikosi Europos policijos biuras (Europolas) ir ES teisminio bendradarbiavimo padalinys (Eurojustas), t. y. ES įstaigos, kurios padeda užtikrinti tarpvalstybinį teisėsaugos institucijų bendradarbiavimą ir jį remia.
- Specialūs duomenų apsaugos režimai taip pat taikomi ES lygmeniu sukurtoms bendroms informacinėms sistemoms, kurios padeda kompetentingoms policijos ir teisminėms institucijoms keistis informacija tarpvalstybiniu lygmeniu. Svarbūs pavyzdžiai: Šengenas II, Vizų informacinė sistema (VIS) ir sistema EURODAC (centralizuota sistema, kurioje saugomi trečiųjų valstybių piliečių, prašančių prieglobsčio vienoje iš ES valstybių narių, pirštų atspaudai).

Duomenų apsaugos direktyvoje neaptariama policijos ir baudžiamosios teisenos sritis. 7.2.1 dalyje aprašomos svarbiausios šioje srityje galiojančios teisinės priemonės.

7.2.1. Duomenų apsaugos pamatinis sprendimas

Tarybos pamatinio sprendimo 2008/977/TVR dėl asmens duomenų, tvarkomų vykdant policijos ir teisminį bendradarbiavimą baudžiamosiose bylose, apsaugos (*Duomenų apsaugos pamatinis sprendimas*)[256] tikslas – užtikrinti fizinių asmenų asmens duomenų apsaugą, kai jų asmens duomenys tvarkomi nusikalstamos veikos prevencijos, tyrimo, nustatymo ar patraukimo už šią veiką baudžiamojon atsakomybėn arba bausmių vykdymo tikslais. Kompetentingos institucijos dirba policijos ir baudžiamosios teisenos srityje valstybių narių arba ES vardu. Šios institucijos yra ES

255 *Ibid.*, 15 straipsnio 1 dalis.

256 Europos Sąjungos Taryba (2008 m.), 2008 m. lapkričio 27 d. Tarybos pamatinis sprendimas 2008/977/TVR dėl asmens duomenų, tvarkomų vykdant policijos ir teisminį bendradarbiavimą baudžiamosiose bylose, apsaugos (*Duomenų apsaugos pamatinis sprendimas*), OL L 350, 2008.

agentūros arba įstaigos, taip pat valstybių narių institucijos[257]. Pamatinio sprendimo taikymo sritis apribojama tiek, kiek to reikia duomenų apsaugai šioms institucijoms bendradarbiaujant tarpvalstybiniu mastu užtikrinti, ir neapima nacionalinio saugumo klausimų.

Duomenų apsaugos pamatinis sprendimas iš esmės yra pagrįstas Konvencijoje Nr. 108 ir Duomenų apsaugos direktyvoje nustatytais principais ir pateiktomis apibrėžtimis.

Duomenis turi naudoti tik kompetentinga institucija ir tik šių duomenų perdavimo arba atskleidimo tikslu. Duomenis gaunanti valstybė narė turi paisyti visų duomenis teikiančios valstybės narės teisėje numatytų keitimuisi duomenimis taikomų apribojimų. Vis dėlto duomenis gaunančiai valstybei tam tikromis sąlygomis leidžiama duomenis naudoti kitu tikslu. Kompetentingos institucijos aiškiai įpareigojamos registruoti ir dokumentuoti duomenų perdavimo atvejus siekiant padėti paaiškinti skunduose ginčijamas pareigas. Tolesnis duomenų, gautų bendradarbiaujant tarpvalstybiniu lygmeniu, perdavimas trečiosioms šalims turi būti atliekamas gavus valstybės narės, kuri pirmoji perdavė duomenis, sutikimą, tačiau skubiais atvejais galima taikyti išimtis.

Kompetentingos institucijos turi imtis būtinų saugumo priemonių, kad užtikrintų asmens duomenų apsaugą nuo bet kokios neteisėtos jų tvarkymo formos.

Kiekviena valstybė narė turi užtikrinti, kad viena arba daugiau nepriklausomų nacionalinių priežiūros institucijų būtų įpareigotos teikti konsultacijas pagal Duomenų apsaugos pamatinį sprendimą priimtų nuostatų taikymo klausimais ir stebėti, kaip taikomos šios nuostatos. Jos taip pat nagrinėja kiekvieno asmens ieškinius dėl jo teisių ir laisvių apsaugos kompetentingoms institucijoms tvarkant asmens duomenis.

Duomenų subjektas turi teisę gauti informaciją apie tvarkomus jo asmens duomenis, taip pat turi teises susipažinti su duomenimis ir reikalauti, kad duomenys būtų ištaisyti, sunaikinti arba užblokuoti. Jeigu atsisakoma šias teises vykdyti remiantis būtinais pagrindais, duomenų subjektui turi būti suteikiama teisė pateikti skundą kompetentingai nacionalinei priežiūros institucijai ir (arba) teismui. Jeigu asmuo dėl nacionalinio įstatymo, kuriuo įgyvendinamas Duomenų apsaugos pamatinis sprendimas, pažeidimų patiria nuostolių, jis turi teisę gauti kompensaciją iš duomenų

257 *Ibid.*, 2 straipsnio h punktas.

valdytojo[258]. Paprastai duomenų subjektams turi būti leidžiama teisminėmis teisių gynimo priemonėmis pasinaudoti kiekvienu atveju, kai pažeidžiamos jų teisės, nustatytos nacionaliniame įstatyme, kuriuo įgyvendinamas Duomenų apsaugos pamatinis sprendimas[259].

Europos Komisija pateikė pasiūlymą dėl reformos, kurią sudaro Bendrasis duomenų apsaugos reglamentas[260] ir Bendroji duomenų apsaugos direktyva[261]. Ši nauja direktyva pakeis dabartinį Duomenų apsaugos pamatinį sprendimą ir pagal ją policijos ir teisminio bendradarbiavimo baudžiamosiose bylose srityje bus taikomi bendrieji principai ir taisyklės.

7.2.2. Policijos ir teisėsaugos institucijų tarpvalstybinio bendradarbiavimo srityje galiojančios konkretesnės duomenų apsaugos teisinės priemonės

Be Duomenų apsaugos pamatinio sprendimo, keitimąsi valstybių narių turima informacija konkrečiose srityse reglamentuoja įvairios teisinės priemonės, pvz., Tarybos pamatinis sprendimas 2009/315/TVR dėl valstybių narių keitimosi informacija iš nuosprendžių registro organizavimo ir turinio ir Tarybos sprendimas dėl valstybių narių finansinės žvalgybos padalinių bendradarbiavimo susitarimų dėl keitimosi informacija[262].

258 *Ibid.*, 19 straipsnis.

259 *Ibid.*, 20 straipsnis.

260 Europos Komisija (2012 m.), 2012 m. sausio 25 d. *Pasiūlymas dėl Europos Parlamento ir Tarybos reglamento dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (Bendrasis duomenų apsaugos reglamentas)*, KOM(2012) 11 galutinis, Briuselis.

261 Europos Komisija (2012 m.), 2012 m. sausio 25 d. *Pasiūlymas dėl Europos Parlamento ir Tarybos direktyvos dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, nustatymo ar traukimo baudžiamojon atsakomybėn už jas arba baudžiamųjų sankcijų vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo (Bendroji duomenų apsaugos direktyva)*, KOM(2012) 10 galutinis, Briuselis.

262 Europos Sąjungos Taryba (2009 m.), 2009 m. vasario 26 d. Tarybos 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 L 271, 2000.

Svarbu paminėti, kad kompetentingoms institucijoms bendradarbiaujant tarpvalstybiniu mastu[263] vis dažniau keičiamasi imigracijos duomenimis. Ši teisės sritis nepriklauso policijos ir baudžiamosios teisenos byloms, tačiau daugeliu aspektų yra susijusi su policijos ir teisminių institucijų darbu. Tą patį galima pasakyti apie į ES importuojamų arba iš ES eksportuojamų prekių duomenis. ES panaikinus vidaus sienos kontrolės postus padidėjo sukčiavimo rizika, todėl būtina, kad valstybės narės aktyviau bendradarbiautų, visų pirma skatindamos tarpvalstybinį keitimąsi informacija, kad veiksmingiau nustatytų nacionalinės ir ES muitinės teisės pažeidimus ir vykdytų šių pažeidimų baudžiamąjį persekiojimą.

Priumo sprendimas

Svarbus institucionalizuoto tarpvalstybinio bendradarbiavimo keičiantis nacionaliniais duomenimis pavyzdys yra Tarybos sprendimas 2008/615/TVR dėl tarpvalstybinio bendradarbiavimo gerinimo, visų pirma kovos su terorizmu ir tarpvalstybiniu nusikalstamumu srityje (*Priumo sprendimas*), kuriuo į ES teisę 2008 m. įtraukta Priumo sutartis[264]. Priumo sutartis – 2005 m. Austrijos, Belgijos, Prancūzijos, Vokietijos, Liuksemburgo, Nyderlandų ir Ispanijos pasirašytas tarptautinis policijos bendradarbiavimo susitarimas[265].

Priumo sprendimo tikslas – padėti valstybėms narėms pagerinti dalijimąsi informacija siekiant vykdyti nusikaltimų prevenciją ir kovoti su jais trijose srityse: terorizmo, tarpvalstybinio nusikalstamumo ir nelegalios migracijos. Šiuo tikslu sprendime įtvirtinamos nuostatos, susijusios su:

- automatine prieiga prie DNR profilių, pirštų atspaudų duomenų ir tam tikrų nacionalinių transporto priemonių registracijos duomenų;

- duomenų teikimu atsižvelgiant į pagrindinius įvykius, kurie turi tarpvalstybinį aspektą;

263 Europos Komisija (2012 m.), 2012 m. gruodžio 7 d. Komisijos komunikatas Europos Parlamentui ir Tarybai „Bendradarbiavimo teisėsaugos srityje stiprinimas ES. Europos keitimosi informacija modelis (EKIM)“, KOM(2012) 735 galutinis, Briuselis.

264 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.

265 Belgijos Karalystės, Vokietijos Federacinės Respublikos, Ispanijos Karalystės, Prancūzijos Respublikos, Liuksemburgo Didžiosios Hercogystės, Nyderlandų Karalystės ir Austrijos Respublikos konvencija dėl tarpvalstybinio bendradarbiavimo gerinimo, visų pirma kovos su terorizmu, tarpvalstybiniu nusikalstamumu ir neteisėta migracija; galima rasti adresu http://register.consilium.europa.eu/pdf/en/05/st10/st10900.en05.pdf.

- informacijos teikimu siekiant vykdyti teroristinių nusikaltimų prevenciją;
- kitomis priemonėmis, padedančiomis gerinti tarpvalstybinį policijos bendradarbiavimą.

Duomenų bazėms, kuriomis galima pasinaudoti remiantis Priumo sprendimu, išimtinai taikoma nacionalinė teisė, tačiau sprendimu papildomai reglamentuojamas keitimasis duomenimis ir visai neseniai – Duomenų apsaugos pagrindų sprendimu. Už tokių duomenų srautų priežiūrą atsakingos kompetentingos įstaigos yra nacionalinės duomenų apsaugos priežiūros institucijos.

7.2.3. Europolo ir Eurojusto užtikrinama duomenų apsauga

Europolas

ES teisėsaugos institucijos Europolo būstinė yra Hagoje ir jis turi nacionalinius Europolo padalinius kiekvienoje valstybėje narėje. Europolas įsteigtas 1998 m.; dabartinis jo, kaip ES institucijos, statusas nustatytas Tarybos sprendimu dėl Europos policijos biuro įsteigimo (*Europolo sprendimas*)[266]. Europolo tikslas – padėti vykdyti organizuoto nusikalstamumo, terorizmo ir kitų formų sunkių nusikaltimų, nurodytų Europolo sprendimo priede, kurie daro poveikį dviem arba daugiau valstybių narių, prevenciją ir juos tirti.

Kad pasiektų savo tikslus, Europolas sukūrė Europolo informacinę sistemą, t. y. valstybėms narėms skirtą duomenų bazę, kuria naudodamiesi nacionaliniai Europolo padaliniai keičiasi kriminaline operatyvine informacija ir informacija. Europolo informacinė sistema gali būti naudojama siekiant sudaryti sąlygas susipažinti su duomenimis, susijusiais su asmenimis, kurie įtariami padarę Europolo kompetencijai priklausančią nusikalstamą veiką arba nuteisti už tokią veiką, arba asmenimis, dėl kurių kyla pagrįstų įtarimų, kad jie padarys tokias veikas. Europolas ir nacionaliniai Europolo padaliniai duomenis gali įrašyti tiesiogiai į Europolo informacinę sistemą ir

266 Europos Sąjungos Taryba (2009 m.), 2009 m. balandžio 6 d. Tarybos sprendimas dėl Europos policijos biuro (Europolo) įsteigimo, OL L 121, 2009. Taip pat žr. Komisijos pasiūlymą dėl reglamento, kuriuo sukuriamas teisinis pagrindas naujam Europolui, kuris pakeistų Europolą, įsteigtą 2009 m. balandžio 6 d. Tarybos sprendimu 2009/371/TVR dėl Europos policijos biuro (Europolo) įsteigimo, ir Europos policijos koledžą, įsteigtą Tarybos sprendimu 2005/681/TVR, įsteigiančiu Europos policijos koledžą (CEPOL), KOM(2013) 173 galutinis.

gauti duomenis iš šios sistemos. Duomenis keisti, taisyti arba ištrinti gali tik juos įrašiusi šalis.

Siekdamas atlikti savo užduotis Europolas prireikus gali saugoti, keisti ir naudoti su nusikalstamomis veikomis susijusius duomenis analizei skirtose darbo bylose. Analizei skirtos darbo bylos sukuriamos siekiant surinkti, tvarkyti arba naudoti duomenis ir padėti atlikti konkretų baudžiamąjį tyrimą, kurį Europolas vykdo kartu su ES valstybėmis narėmis.

Atsižvelgdamas į naujausius pokyčius, 2013 m. sausio 1 d. Europole sukurtas Europos elektroninių nusikaltimų centras[267]. 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, pvz., sukčiavimas internete;
- kurie sukelia didelę žalą aukai, pvz., vaikų seksualinis išnaudojimas internetu;
- kurie daro poveikį ES ypatingos svarbos infrastruktūrai ir informacinėms sistemoms.

Europolo veiklą reglamentuojantis duomenų apsaugos režimas yra patobulintas. Europolo sprendimo 27 straipsnyje nurodyta, kad taikomi Konvencijoje Nr. 108 ir Rekomendacijoje dėl policijos duomenų numatyti principai, susiję su automatiniu ir neautomatiniu duomenų tvarkymu. Duomenų perdavimas tarp Europolo ir valstybių narių taip pat turi būti vykdomas laikantis Duomenų apsaugos pamatiniame sprendime nustatytų taisyklių.

Siekdama užtikrinti atitiktį taikytinai duomenų apsaugos teisei ir visų pirma, kad tvarkant asmens duomenis nebūtų pažeidžiamos asmenų teisės, nepriklausoma Europolo jungtinė priežiūros institucija (angl. JSB) peržiūri ir stebi Europolo veiklą[268]. Kiekvienas asmuo turi teisę susipažinti su visais savo asmens duomenimis, kuriuos

267 Taip pat žr. EDAPP (2012 m.), 2012 m. birželio 29 d. *Europos duomenų apsaugos priežiūros pareigūno nuomonė dėl Europos Komisijos komunikato Tarybai ir Europos Parlamentui dėl Europos kovos su elektroniniu nusikalstamumu centro kūrimo*, Briuselis.

268 Europolo sprendimo 34 straipsnis.

gali turėti Europolas, įskaitant teisę prašyti šiuos asmens duomenis patikrinti, ištaisyti arba sunaikinti. Jeigu asmens netenkina Europolo sprendimas dėl šių teisių vykdymo, jis gali pateikti skundą JSB Apeliaciniam komitetui.

Jeigu dėl teisinių arba faktinių klaidų, susijusių su Europolo saugomais arba tvarkomais duomenimis, atsirado žala, nukentėjusioji šalis gali siekti apginti savo teises tik valstybės narės, kurioje atsitiko žalą sukėlęs įvykis, kompetentingame teisme[269]. Europolas išmokės kompensaciją valstybei narei, jeigu žala atsirado dėl to, kad Europolas nesilaikė savo teisinių įsipareigojimų.

Eurojustas

Eurojustas kaip ES įstaiga įsteigtas 2002 m. su būstine Hagoje ir jis remia teisminį bendradarbiavimą vykdant tyrimus ir baudžiamuosius persekiojimus, susijusius su sunkiais nusikaltimais, kurie daro poveikį ne mažiau kaip dviem valstybėms narėms[270]. Eurojustas turi kompetenciją:

- 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 paskiria vieną teisėją arba prokurorą, kuriam taikoma nacionalinė teisė ir suteikiama būtina kompetencija atlikti užduotis, kurios yra reikalingos teisminiam bendradarbiavimui skatinti ir gerinti. Be to, nacionaliniai nariai kartu veikia kaip kolegija, kuri vykdo specialias Eurojusto užduotis.

Eurojustas gali tvarkyti asmens duomenis tiek, kiek to reikia Eurojusto tikslams pasiekti. Tačiau šie duomenys apribojami konkrečia informacija, susijusia su asmenimis, kurie įtariami padarę arba dalyvavę darant Eurojusto kompetencijai

269 *Ibid.*, 52 straipsnis.

270 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/TVR dėl Eurojusto stiprinimo ir iš dalies keičiantis Sprendimą 2002/187/TVR, įkuriantį Eurojustą siekiant sustiprinti kovą su sunkiais nusikaltimais, OL L 138, 2009 (*Eurojusto sprendimai*).

priklausančią nusikalstamą veiką arba buvo nuteisti už tokią veiką. Eurojustas taip pat gali tvarkyti tam tikrą informaciją, susijusią su Eurojusto kompetencijai priklausančios nusikalstamos veikos liudytojais arba aukomis[271]. Išimtinėmis aplinkybėmis Eurojustas gali ribotą laikotarpį tvarkyti įvairesnius asmens duomenis, susijusius su veikos aplinkybėmis, jeigu tokie duomenys tiesiogiai susiję su vykdomu tyrimu. Atsižvelgdamas į savo kompetencijos ribas, Eurojustas gali bendradarbiauti su kitomis ES institucijomis, įstaigomis ir agentūromis ir keistis su jomis asmens duomenimis. Eurojustas taip pat gali bendradarbiauti ir keistis asmens duomenimis su trečiosiomis valstybėmis ir organizacijomis.

Duomenų apsaugos srityje Eurojustas turi užtikrinti tokį apsaugos lygį, kuris būtų lygiavertis Europos Tarybos konvencijoje Nr. 108 ir jos vėlesniuose pakeitimuose įtvirtintiems principams. Tais atvejais, kai keičiamasi duomenimis, būtina laikytis konkrečių taisyklių ir apribojimų, kurie buvo nustatyti bendradarbiavimo arba darbo tvarkos susitarimuose, priimtuose pagal Eurojusto tarybos sprendimus ir Eurojusto duomenų apsaugos taisyklėse[272].

Eurojuste įsteigta nepriklausoma jungtinė priežiūros institucija (angl. JSB), kuriai pavesta užduotis stebėti, kaip Eurojustas tvarko asmens duomenis. Asmenys gali pateikti skundus JSB, jei jų netenkina Eurojusto atsakymas į prašymą susipažinti su asmens duomenimis, ištaisyti, užblokuoti arba sunaikinti asmens duomenis. Jei Eurojustas asmens duomenis tvarko neteisėtai, jis už bet kokią duomenų subjektui padarytą žalą atsako pagal valstybės narės, kurioje yra jo būstinė, t. y. Nyderlandų, nacionalinę teisę.

7.2.4. Duomenų apsauga ES bendrose informacinėse sistemose

Ne tik yra keičiamasi duomenimis tarp valstybių narių ir įsteigtos specialios ES institucijos, kovojančios su tarpvalstybiniu nusikalstamumu, bet ir buvo sukurtos kelios ES bendros informacinės sistemos, kuriomis naudodamosi kompetentingos nacionalinės ir ES institucijos gali tarpusavyje keistis duomenimis siekdamos konkrečių teisėsaugos tikslų, įskaitant imigracijos ir muitinės teisę. Kai kurios šios sistemos buvo sukurtos remiantis daugiašaliais susitarimais, kuriuos vėliau papildė ES teisinės

271 Tarybos sprendimo 2002/187/TVR, iš dalies pakeisto Tarybos sprendimu 2003/659/TVR ir Tarybos sprendimu 2009/426/TVR, konsoliduotos redakcijos 15 straipsnio 2 dalis.

272 2005 m. kovo 19 d. Asmens duomenų tvarkymo ir apsaugos Eurojuste darbo tvarkos taisyklės, OL C 68/01, 2005, p. 1.

priemonės ir sistemos, pvz., Šengeno informacinė sistema, Vizų informacinė sistema, sistema EURODAC, EUROSUR arba Muitinės informacinė sistema.

Europos didelės apimties IT sistemų agentūra (angl. eu-LISA)[273], kuri buvo įsteigta 2012 m., yra atsakinga už ilgalaikį antrosios kartos Šengeno informacinės sistemos (SIS II), Vizų informacinės sistemos (VIS) ir sistemos EURODAC 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 buvusiųjų Europos Bendrijų valstybių narių sudarė Beniliukso ekonominės sąjungos, Vokietijos ir Prancūzijos susitarimą dėl laipsniško patikrinimų kertant bendras sienas panaikinimo (*Šengeno susitarimas*), kuriuo siekta sukurti laisvo asmenų judėjimo erdvę, kuri Šengeno teritorijoje nebūtų varžoma sienos kontrolės[274]. Siekiant įveikti visuomenės saugumui dėl atvirų sienų galintį kilti pavojų, Šengeno išorės sienose nustatyta griežtesnė sienų kontrolė, taip pat užmegzti glaudūs policijos ir teisėsaugos institucijų bendradarbiavimo santykiai.

Prie Šengeno susitarimo prisijungus kitoms valstybėms, Šengeno sistema Amsterdamo sutartimi galiausiai buvo integruota į ES teisinę sistemą[275]. Šis sprendimas įgyvendintas 1999 m. Naujausia Šengeno informacinės sistemos versija – SIS II – pradėjo veikti 2013 m. balandžio 9 d. Dabar ji veikia visose ES valstybėse narėse, įskaitant Islandiją, Lichtenšteiną, Norvegiją ir Šveicariją[276]. Europolas ir Eurojustas taip pat turi prieigą prie SIS II.

273 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.

274 Susitarimas tarp Beniliukso ekonominės sąjungos valstybių, Vokietijos Federacinės Respublikos ir Prancūzijos Respublikos vyriausybių dėl laipsniško jų bendrų sienų kontrolės panaikinimo, OL L 239, 2000.

275 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.

276 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.

SIS II sudaro centrinė sistema (C-SIS), kiekvienos valstybės narės nacionalinė sistema (N-SIS) ir ryšių perdavimo tarp centrinės sistemos ir nacionalinių sistemų infrastruktūra. C-SIS sudaro tam tikri valstybių narių įrašyti duomenys apie asmenis ir objektus. C-SIS naudoja visoje Šengeno erdvėje veikiančios nacionalinės sienų kontrolės tarnybos, policija, muitinės, vizas išduodančios 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. N-SIS naudojamasi ir joje bus pateiktas įspėjimas tais atvejais, kai:

- asmuo neturi teisės atvykti į Šengeno teritoriją arba apsistoti joje; arba
- asmens arba objekto ieško teisminės arba teisėsaugos institucijos; arba
- paskelbta dingusio asmens paieška; arba
- paskelbta apie pavogtas arba prarastas prekes, pvz., banknotus, automobilius, krovinines transporto priemones, šaunamuosius ginklus ir tapatybės dokumentus.

Įspėjimo atveju nacionalinėse Šengeno informacinėse sistemose turi būti pradėti tolesni veiksmai.

SI II numatytos naujos funkcijos, pvz., galimybė įrašyti biometrinius duomenis, kaip antai pirštų atspaudus ir nuotraukas; arba naujos įspėjimų kategorijos, pvz., pavogti laivai, orlaiviai, konteineriai arba mokėjimo priemonės; ir patobulinti įspėjimai apie asmenis ir objektus; Europos arešto orderiai (EAO) dėl asmenų arešto, perdavimo arba ekstradicijos.

Tarybos sprendimu 2007/533/TVR dėl antrosios kartos Šengeno informacinės sistemos sukūrimo, veikimo ir naudojimo (Šengeno II sprendimas) į jį įtraukiama Konvencija Nr. 108: „Taikant šį sprendimą asmens duomenys saugomi pagal Europos Tarybos konvenciją Nr. 108.“[277] Kai nacionalinės policijos institucijos asmens duomenis naudoja taikydamos Šengeno II sprendimą, nacionalinėje teisėje turi būti įgyvendintos Konvencijos Nr. 108 ir Rekomendacijos dėl policijos duomenų nuostatos.

277 Europos Sąjungos Taryba (2007 m.), 2007 m. birželio 12 d. Tarybos sprendimo 2007/533/TVR dėl antrosios kartos Šengeno informacinės sistemos (SIS II) sukūrimo, veikimo ir naudojimo, OL L 205, 2007, 57 straipsnis.

Kiekvienos valstybės narės kompetentinga nacionalinė priežiūros institucija prižiūri vidaus N-SIS. Visų pirma ji turi patikrinti valstybės narės į C-SIS per N-SIS įrašomų duomenų kokybę. Nacionalinė priežiūros institucija turi užtikrinti, kad vidaus N-SIS atliekamos duomenų tvarkymo operacijos būtų audituojamos ne rečiau kaip kas ketverius metus. Nacionalinės priežiūros institucijos ir EDAPP bendradarbiauja ir užtikrina koordinuotą SIS priežiūrą, o EDAPP yra atsakingas už C-SIS priežiūrą. Siekiant užtikrinti skaidrumą, kas dvejus metus Europos Parlamentui, Tarybai ir „eu-LISA“ siunčiama bendra veiklos ataskaita.

Asmenys teise susipažinti su SIS II gali pasinaudoti bet kurioje valstybėje narėje, nes kiekviena N-SIS yra tiksli C-SIS kopija.

Pavyzdys. Byloje *Dalea prieš Prancūziją*[278] pareiškėjui atsisakyta išduoti Prancūzijos vizą, nes Prancūzijos institucijos Šengeno informacinėje sistemoje įrašė, kad jam turėtų būti atsisakoma išduoti leidimą atvykti į šalį. 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 privataus gyvenimo gerbimą apribojimas buvo proporcingas. Todėl pareiškėjo skundas pagal 8 straipsnį buvo paskelbtas nepriimtinu.

Vizų informacinė sistema

Vizų informacinė sistema (VIS), kurią taip pat valdo „eu-LISA“, sukurta siekiant paremti ES vizų politikos įgyvendinimą[279]. VIS sudaro sąlygas Šengeno valstybėms keistis vizų duomenimis šiuo tikslu naudojant sistemą, kuri sujungia ne ES valstybėse įsikūrusių Šengeno valstybių konsulatus ir visų Šengeno valstybių išorės sienų

278 2010 m. vasario 2 d. EŽTT sprendimas *Dalea prieš Prancūziją* (spr.), Nr. 964/07.

279 Europos Sąjungos Taryba (2004 m.), 2004 m. birželio 8 d. Tarybos sprendimas dėl Vizų informacinės sistemos (VIS) sukūrimo, OL L 2013, 2004; 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; 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.

perėjimo punktus. VIS tvarkomi duomenys, susiję su prašymais dėl trumpalaikių vizų apsilankymo Šengeno erdvėje arba jos kirtimo tikslais. VIS sudaro sąlygas pasienio institucijoms, pasinaudojant biometriniais duomenimis, patikrinti, ar vizą pateikiantis asmuo yra teisėtas jos turėtojas, ir nustatyti asmenis, neturinčius dokumentų arba turinčius suklastotus dokumentus.

Pagal Europos Parlamento ir Tarybos reglamentą (EB) Nr. 767/2008 dėl Vizų informacinės sistemos (VIS) ir apsikeitimo duomenimis apie trumpalaikes vizas tarp valstybių narių (*VIS reglamentas*), į VIS gali būti registruojami tik duomenys apie vizos prašantį asmenį, jo vizas, nuotraukos, pirštų atspaudai, nuorodos į kitus prašymus ir jį lydinčių asmenų prašymų išduoti vizas dokumentai[280]. Prieiga prie VIS siekiant įrašyti, pakeisti arba ištrinti duomenis suteikiama tik valstybių narių vizas išduodančioms institucijoms, o galimybė susipažinti su duomenimis suteikiama vizas išduodančioms institucijoms ir institucijoms, kurios yra kompetentingos atlikti patikrinimus išorės sienų perėjimo punktuose, imigracijos patikrinimus ir kurioms priskirta kompetencija prieglobsčio srityje. Tam tikromis sąlygomis nacionalinės kompetentingos policijos institucijos ir Europolas gali prašyti leisti susipažinti su į VIS įrašytais duomenimis nusikalstamų ir teroristinių veikų prevencijos, atskleidimo ir tyrimo tikslais[281].

Sistema EURODAC

Sistemos EURODAC pavadinimas reiškia daktilogramas arba pirštų atspaudus. Tai centralizuota sistema, kurioje pateikiami trečiųjų valstybių piliečių, teikiančių prašymus dėl prieglobsčio vienoje iš ES valstybių narių, pirštų atspaudų duomenys[282]. Sistema veikia nuo 2003 m. sausio mėn., o jos tikslas – padėti nustatyti, kuri valstybė narė turėtų būti atsakinga už konkretaus prieglobsčio prašymo nagrinėjimą pagal Tarybos reglamentą (EB) Nr. 343/2003, nustatantį valstybės narės, atsakingos už trečiosios šalies piliečio vienoje iš valstybių narių pateikto prieglobsčio prašymo

280 2008 m. liepos 9 d. Europos Parlamento ir tarybos reglamento (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.

281 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.

282 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*).

nagrinėjimą, nustatymo kriterijus ir mechanizmus (*Dublino II reglamentas*)[283]. Sistemos EURODAC asmens duomenys gali būti naudojami tik siekiant palengvinti Dublino II reglamento taikymą; už asmens duomenų naudojimą kitais tikslais taikomos sankcijos.

Sistemą EURODAC sudaro „eu-LISA" valdomas centrinis padalinys, kuris skirtas pirštų atspaudams saugoti ir lyginti, ir elektroninių duomenų perdavimo tarp valstybių narių ir centrinės duomenų bazės sistema. Valstybės narės paima ir perduoda kiekvieno ne jaunesnio nei 14 metų ne ES piliečio arba asmens be pilietybės, kurie šios valstybės narės teritorijoje prašo prieglobsčio arba yra sulaikyti dėl neteisėto jų išorės sienų perėjimo, pirštų atspaudus. Valstybės narės taip pat gali paimti ir perduoti tų ne ES piliečių arba asmenų be pilietybės pirštų atspaudus, kurie, kaip nustatyta, yra be leidimo apsistoję valstybės narės teritorijoje.

Sistemos EURODAC duomenų bazėje saugomi tik pseudoniminiai pirštų atspaudų duomenys. Nustačius atitikimą, pseudonimas kartu su pirmosios pirštų atspaudų duomenis perdavusios valstybės narės pavadinimu atskleidžiami antrajai valstybei narei. Tuomet ši antroji valstybė narė kreipiasi į pirmąją valstybę narę, nes pagal Dublino II reglamentą pirmoji valstybė narė atsako už prieglobsčio prašymo nagrinėjimą.

Su prieglobsčio prašančiais asmenimis susiję duomenys sistemoje EURODAC saugomi 10 metų nuo pirštų atspaudų paėmimo datos, išskyrus atvejus, kai duomenų subjektui suteikiama ES valstybės narės pilietybė. Šiuo atveju duomenys turi būti nedelsiant ištrinti. Duomenys, susiję su užsienio piliečiais, kurie, kaip nustatyta, neteisėtai perėjo išorės sieną, saugomi dvejus metus. Šie duomenys turi būti nedelsiant ištrinti, jeigu duomenų subjektas gauna leidimą gyventi, išvyksta iš ES teritorijos arba jam suteikiama valstybės narės pilietybė.

Sistemoje EURODAC, be visų ES valstybių narių, taip pat tarptautinių susitarimų pagrindu dalyvauja Islandija, Norvegija, Lichtenšteinas ir Šveicarija.

283 2003 m. vasario 18 d. Tarybos reglamentas (EB) Nr. 343/2003, nustatantis valstybės narės, atsakingos už trečiosios šalies piliečio vienoje iš valstybių narių pateikto prieglobsčio prašymo nagrinėjimą, nustatymo kriterijus ir mechanizmus (*Dublino II reglamentas*), OL L 50, 2003.

EUROSUR

Europos sienų stebėjimo sistema (EUROSUR)[284] sukurta siekiant gerinti Šengeno išorės sienų kontrolę atskleidžiant ir užkardant neteisėtą imigraciją ir tarpvalstybinius nusikaltimus ir su jais kovojant. Ši sistema padeda gerinti keitimąsi informacija ir nacionalinių koordinavimo centrų ir FRONTEX (ES agentūros, atsakingos už naujos integruoto sienų valdymo koncepcijos kūrimą ir taikymą) bendradarbiavimą[285]. EUROSUR bendri tikslai:

- mažinti neteisėtų migrantų, kurie į ES patenka nepastebėti, skaičių;
- sumažinti neteisėtų migrantų mirčių skaičių daugiau gyvybių išgelbstint jūroje;
- padėti vykdyti tarpvalstybinio nusikalstamumo prevenciją ir taip padidinti ES bendrą saugumą[286].

EUROSUR pradėjo veikti 2013 m. gruodžio 2 d. visose valstybėse narėse, kurios turi išorės sienas, o kitose valstybėse narėse pradės veikti nuo 2014 m. gruodžio 1 d. Reglamentas bus taikomas valstybių narių sausumos, jūros išorės sienų ir oro sienų stebėjimui.

284 2013 m. spalio 22 d. Europos Parlamento Tarybos reglamentas (ES) Nr. 1052/2013, kuriuo sukuriama Europos sienų stebėjimo sistema (EUROSUR), OL L 295, 2013.

285 2011 m. spalio 25 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 1168/2011, kuriuo iš dalies keičiamas Reglamentas (EB) Nr. 2007/2004, įsteigiantis Europos operatyvaus bendradarbiavimo prie Europos Sąjungos valstybių narių išorės sienų valdymo agentūrą (FRONTEX *reglamentas*), OL L 394, 2011.

286 Taip pat žr. Europos Komisija (2008 m.), 2008 m. vasario 13 d. Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui – Europos sienų stebėjimo sistemos (EUROSUR) sukūrimo nagrinėjimas, KOM(2008) 68 galutinis, Briuselis; Europos Komisija (2011 m.), 2011 m. gruodžio 12 d. Komisijos tarnybų darbinio dokumento „Poveikio vertinimas, pridedamas prie pasiūlymo dėl Europos Parlamento ir Tarybos reglamento, kuriuo sukuriama Europos sienų stebėjimo sistema (EUROSUR)“, SEC(2011) 1536 galutinis, Briuselis, p. 18.

Muitinės informacinė sistema

Kita svarbi ES lygmeniu sukurta bendra informacinė sistema yra Muitinės informacinė sistema (MIS)[287]. 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 laikoma informacija apima asmens duomenis, įskaitant nuorodas į prekes, transporto rūšis, įmones, asmenis, prekes ir sulaikytus, areštuotus arba konfiskuotus pinigus. Šią informaciją galima naudoti tik stebint ir vykdant konkrečius tyrimus arba teikiant apie juos ataskaitas, arba atliekant strategines analizes, susijusias su muitinės nuostatų pažeidimu.

Prieiga prie CIS suteikiama nacionalinėms muitinės, mokesčių, žemės ūkio, visuomenės sveikatos ir policijos institucijoms, taip pat Europolui ir Eurojustui.

Tvarkant asmens duomenis būtina laikytis konkrečių Reglamente Nr. 515/97 ir MIS konvencijoje[288] nustatytų taisyklių, taip pat Duomenų apsaugos direktyvos, ES institucijų duomenų apsaugos reglamento, Konvencijos Nr. 108 ir Rekomendacijos dėl policijos duomenų nuostatų. EDAPP yra atsakingas už CIS atitikties Reglamentui (EB) Nr. 45/2001 priežiūrą ir, ne rečiau kaip kartą per metus, surengia posėdžius su visų nacionalinių duomenų apsaugos priežiūros institucijų, atsakingų už klausimų susijusių su CIS priežiūrą.

287 Europos Sąjungos Taryba (1995 m.), 1995 m. liepos 26 d. Tarybos aktas dėl Konvencijos dėl informacinių technologijų naudojimo muitinės tikslais parengimo, OL C 316, 1995, iš dalies pakeistas Europos Sąjungos Tarybos (2009 m.), 1997 m. kovo 13 d. Reglamentas 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 informacinių technologijų naudojimo muitinės tikslais (*MIS sprendimas*), OL L 323, 2009.

288 *Ibid.*

8

Kiti konkretūs Europos duomenų apsaugos įstatymai

ES	Aptariami klausimai	ET
Duomenų apsaugos direktyva. E. privatumo direktyva.	**Elektroniniai ryšiai.**	Konvencija Nr. 108. Rekomendacija dėl telekomunikacijų paslaugų.
Duomenų apsaugos direktyvos 8 straipsnio 2 dalies b punktas.	**Darbo santykiai.**	Konvencija Nr. 108. Rekomendacija dėl užimtumo.
		2007 m. balandžio 3 d. EŽTT sprendimas *Copland prieš Jungtinę Karalystę*, Nr. 62617/00.
Duomenų apsaugos direktyvos 8 straipsnio 3 dalis.	**Medicininiai duomenys.**	Konvencija Nr. 108. Rekomendacija dėl medicininių duomenų.
		1997 m. vasario 25 d. EŽTT sprendimas *Z. prieš Suomiją*, Nr. 22009/93.
Klinikinių tyrimų direktyva.	**Klinikiniai tyrimai.**	
Duomenų apsaugos direktyvos 6 straipsnio 1 dalies b ir e punktai, 13 straipsnio 2 dalis.	**Statistika**	Konvencija Nr. 108.8 Rekomendacija dėl statistinių duomenų.
Reglamentas (EB) Nr. 223/2009 dėl Europos statistikos. 2008 m. gruodžio 16 d. ESTT sprendimas *Huber prieš Vokietiją*, C-524/06.	**Oficiali statistika.**	Konvencija Nr. 108. Rekomendacija dėl statistinių duomenų.

ES	Aptariami klausimai	ET
Direktyva 2004/39/EB 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.**	Konvencija Nr. 108. Rekomendacija Nr. R (90) 19 dėl asmens duomenų, naudojamų apmokėjimui arba kitoms su tuo susijusioms operacijoms, apsaugos. 2012 m. gruodžio 6 d. EŽTT sprendimas *Michaud prieš Prancūziją*, Nr. 12323/11.

Kai kurie klausimai reglamentuojami Europos lygmeniu priimtuose specialiuose teisinėse priemonėse, kuriose išsamiau aptariama Konvencijos Nr. 108 arba Duomenų apsaugos direktyvos bendrųjų taisyklių taikymo konkrečioms situacijoms tvarka.

8.1. Elektroniniai ryšiai

Pagrindiniai faktai

- 1995 m. ET priimtoje rekomendacijoje pateikiamos konkrečios duomenų apsaugos taisyklės, galiojančios telekomunikacijų, ypač telefono ryšio paslaugų, srityje.
- Asmens duomenų, susijusių su ryšių paslaugų teikimu ES, tvarkymas reglamentuojamas E. privatumo direktyvoje.
- Elektroninių ryšių konfidencialumas susijęs ne tik su ryšio turiniu, bet ir su srauto duomenimis, pvz., informacija apie tai, kas su kuo, kada ir kaip ilgai bendravo, ir vietos nustatymo duomenimis, pvz., vieta, iš kurios buvo skambinta.

Dėl ryšių tinklų padidėjo nepagrįsto kišimosi į asmeninę naudotojų sferą pavojus, nes šie tinklai suteikia papildomas technines galimybes klausytis pokalbių tokiuose tinkluose ir juos stebėti. Todėl prieita prie išvados, kad, siekiant sumažinti šį ryšių paslaugų naudotojams kylantį pavojų, būtina priimti konkrečius duomenų apsaugos reglamentus.

1995 m. ET priėmė rekomendaciją dėl duomenų apsaugos telekomunikacijų, visų pirma telefono ryšio paslaugų, srityje[289]. Pagal šią rekomendaciją asmens duomenų rinkimas ir tvarkymas teikiant telekomunikacijų paslaugas turėtų būti susijęs tik su naudotojo prijungimu prie tinklo, konkrečios telekomunikacijų paslaugos teikimu, sąskaitų išrašymu, patikrinimu, optimalaus techninio veikimo užtikrinimu ir tinklo ir paslaugos tobulinimu.

Ypatingas dėmesys taip pat atkreiptas į telekomunikacijų tinklų naudojimą siunčiant tiesioginės rinkodaros pranešimus. Paprastai tiesioginės rinkodaros pranešimai negali būti skirti abonentui, kuris aiškiai atsisakė gauti reklamos pranešimus. Automatinė skambučių įranga, kurią naudojant perduodami iš anksto įrašyti reklamos pranešimai, gali būti naudojama tik tuo atveju, jeigu abonentas davė aiškų sutikimą. Vidaus teisėje turi būti nustatytos išsamios šios srities taisyklės.

ES teisinėje sistemoje po pirmojo bandymo 1997 m., 2002 m. buvo priimta, o 2009 m. iš dalies pakeista Direktyva dėl privatumo ir elektroninių ryšių (*E. privatumo direktyva*), kurios tikslas – papildyti ir sukonkretinti Duomenų apsaugos direktyvos nuostatas, susijusias su telekomunikacijų sektoriumi[290]. E. privatumo direktyva taikoma tik ryšių paslaugoms, kurios teikiamos naudojant viešus elektroninius tinklus.

E. privatumo direktyvoje išskiriamos trys pagrindinės duomenų, gaunamų teikiant ryšių paslaugas, kategorijos:

- duomenys, kurie sudaro ryšio metu siunčiamų pranešimų turinį; šie duomenys yra visiškai konfidencialūs;

- ryšiui užmegzti ir palaikyti reikalingi duomenys, vadinamieji srauto duomenys, pvz., informacija apie ryšio partnerius, ryšio laiką ir trukmę;

289 ET Ministrų Komitetas (1995 m.), 1995 m. vasario 7 d. Ministrų Komiteto rekomendacija Nr. R (95) 4 valstybėms narėms dėl asmens duomenų apsaugos telekomunikacijų paslaugų, visų pirma telefono ryšio paslaugų, srityje.

290 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.

- srauto duomenyse yra konkrečių su ryšio prietaisu susijusių duomenų, vadinamųjų vietos nustatymo duomenų; šie duomenys kartu atskleidžia ryšio prietaisų *naudotojų* buvimo vietą ir yra ypač svarbūs atsižvelgiant į mobiliojo ryšio prietaisų naudotojus.

Paslaugų teikėjas srauto duomenis gali naudoti tik išrašydamas sąskaitas ir užtikrindamas techninius paslaugos teikimo aspektus. Tačiau duomenų subjekto sutikimu šie duomenys gali būti atskleisti kitiems duomenų valdytojams, siūlantiems pridėtinės vertės paslaugas, pvz., informacijos, susijusios su naudotojui artimiausia metro stotele arba vaistine, arba naudotojo buvimo vietos oro prognoze, teikimas.

Kitokia prieiga prie duomenų apie pranešimus elektroniniuose tinkluose, pvz., prieiga siekiant tirti nusikaltimus, pagal E. privatumo direktyvos 15 straipsnį turi atitikti pagrįsto teisės į duomenų apsaugą reikalavimus, kaip nustatyta EŽTK 8 straipsnio 2 dalyje ir patvirtinta Chartijos 8 ir 2 straipsniuose.

2009 m. atlikti E. privatumo direktyvos pakeitimai[291], kuriais:

- 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 įpareigotos užtikrinti teismines teisių gynimo priemones, susijusias su nepageidaujamų pranešimų draudimo pažeidimais[292];

- draudžiama be kompiuterio naudotojo sutikimo nustatyti slapukus, t. y. naudoti programinę įrangą, kuria stebimi ir įrašomi kompiuterio naudotojo veiksmai.

291 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.

292 Žr. iš dalies pakeistos direktyvos 13 straipnį.

Nacionalinėje teisėje, siekiant užtikrinti pakankamą apsaugą, reikėtų išsamiau reglamentuoti sutikimo davimo ir gavimo būdą[293].

Kai duomenų saugumo pažeidimas padaromas dėl neteisėtos prieigos prie duomenų, jų praradimo arba sunaikinimo, kompetentinga priežiūros institucija turi būti apie tai nedelsiant informuojama. Abonentai turi būti informuojami, kai jie dėl duomenų saugumo pažeidimo gali patirti žalos[294].

Duomenų saugojimo direktyva[295] (netekusioje galios 2014 m. balandžio 8 d.) įpareigojimą ryšių paslaugų teikėjus leisti susipažinti su srauto duomenimis, visų pirma kovos su sunkiais nusikaltimais tikslais, ne mažiau kaip 6 ir ne ilgiau kaip 24 mėnesius, nepaisant to, ar paslaugų teikėjui šių duomenų vis dar reikėjo sąskaitų išrašymo tikslais arba siekiant užtikrinti techninius paslaugų teikimo aspektus.

ES valstybės narės paskiria nepriklausomas valdžios institucijas, kurios atsako už saugomų duomenų saugumo stebėseną.

Akivaizdu, kad saugant telekomunikacijų duomenis ribojama teisė į duomenų apsaugą[296]. Šio apribojimo pagrįstumas ginčijamas keliose ES valstybių narių teismo bylose[297].

Pavyzdys: *Digital Rights Ireland ir Seitlinger bei kiti*[298], ESTT paskelbė Duomenų saugojimo direktyvą negaliojančia. Teismo teigimu, „plataus masto ir ypač rimtas direktyvos įsikišimas į nagrinėjamas pagrindines teises yra nepakankamai

293 Žr. *ibid.*, 5 straipsnis; taip pat žr. 29 straipsnio duomenų apsaugos darbo grupė (2012 m.), 2012 m. birželio 7 d. *Nuomonė 04/2012 dėl slapukams taikomos reikalavimo gauti sutikimą išimties*, WP 194, Briuselis.

294 Taip pat žr. 29 straipsnio duomenų apsaugos darbo grupė (2011 m.), 2011 m. balandžio 5 d. *Darbo dokumentas 01/2011 dėl dabartinės ES asmens duomenų saugumo pažeidimų sistemos ir rekomendacijų dėl būsimų politikos pokyčių*, WP 184, Briuselis.

295 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.

296 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.*

297 Vokietija, Federalinis Konstitucinis Teismas (vok. *Bundesverfassungsgericht*), 1 BvR 256/08, 2010 m. kovo 2 d.; Rumunija, Federalinis Konstitucinis Teismas (rum. *Curtea Constituțională a României*), Nr. 1258, 2009 m. spalio 8 d.; Čekija, Konstitucinis Teismas (ček. *Ústavní soud České republiky*), 94/2011 Coll., 2011 m. kovo 22 d.

298 2014 balandžio 8 d. ESTT sujungtos bylos C-293/12 ir C-594/12, *Digital Rights Ireland ir Seitlinger bei kiti*, 65 paragrafas.

apribotas siekiant užtikrinti, kad toks įsikišimas būtų apribotas tik tuo, kas yra griežtai būtina“.

Elektroninių ryšių srityje labai svarbus yra valdžios institucijų nustatytų apribojimų klausimas. Stebėjimo priemonės arba pranešimų perėmimas, pvz., pasiklausymo ar perėmimo prietaisai, leidžiamas tik tuo atveju, jeigu tai numatyta įstatyme ir jeigu tai yra būtina priemonė demokratinėje visuomenėje atsižvelgiant į interesus, susijusius su valstybės saugumo apsauga, visuomenės sauga, valstybės piniginiais interesais arba nusikalstamų veikų užkardymu arba su duomenų subjektų arba kitų asmenų teisių ir laisvių apsauga.

Pavyzdys. Byloje *Malone prieš Jungtinę Karalystę*[299] pareiškėjui pateikti kaltinimai dėl įvairių nusikaltimų, susijusių su nesąžiningu disponavimu vogtomis prekėmis. Nagrinėjant bylą paaiškėjo, kad, remiantis Vidaus reikalų departamento valstybės sekretoriaus išduotu orderiu, pareiškėjo pokalbių telefonu buvo slapta klausomasi. Nors būdas, kuriuo buvo slapta klausomasi pareiškėjo pokalbių, pagal vidaus teisę buvo teisėtas, EŽTT nustatė, kad negaliojo jokios teisinės taisyklės dėl valdžios institucijų diskrecijos teisės šioje srityje taikymo ir naudojimosi ja ir kad dėl to, remiantis galiojančia praktika, nustatytas apribojimas „neatitiko įstatymo“. Teismas nusprendė, kad EŽTK 8 straipsnis buvo pažeistas.

8.2. Užimtumo duomenys

Pagrindiniai faktai

- ET rekomendacijoje dėl užimtumo duomenų nustatytos konkrečios duomenų apsaugos taisyklės darbo santykių srityje.
- Duomenų apsaugos direktyvoje darbo santykiai aiškiai nurodomi tik ypatingų duomenų tvarkymo atveju.
- Sutikimo, kuris turi būti duotas aiškiai, galiojimas, kaip teisinis duomenų apie darbuotojus tvarkymo pagrindas, gali būti abejotinas atsižvelgiant į nelygias darbdavio ir darbuotojo jėgas. Aplinkybės, kuriomis duotas sutikimas, turi būti atidžiai vertinamos.

Konkrečios ES teisinės sistemos, reglamentuojančios duomenų tvarkymą užimtumo srityje, nėra. Duomenų apsaugos direktyvoje užimtumo santykiai yra aiškiai nurodyti šios direktyvos 8 straipsnio 2 dalyje, susijusioje su ypatingų duomenų

299 1985 m. balandžio 26 d. EŽTT sprendimas *Malone prieš Jungtinę Karalystę*, Nr. 8691/79.

tvarkymu. Kalbant apie ET teisę pažymėtina, kad 1989 m. buvo priimta Rekomendacija dėl užimtumo duomenų ir ji šiuo metu atnaujinama[300].

29 straipsnio duomenų apsaugos darbo grupės darbo dokumente galima rasti dažniausiai užimtumo srityje pasitaikančių duomenų apsaugos problemų apžvalgą[301]. Darbo grupė išanalizavo sutikimo, kaip teisinio pagrindo tvarkyti užimtumo duomenis, svarbą[302]. Darbo grupė nustatė, kad dėl ekonominio disbalanso tarp sutikimą prašančio duoti darbdavio ir sutikimą duodančio darbuotojo dažnai kyla abejonių, ar sutikimas buvo duotas laisvai. Todėl vertinant sutikimo užimtumo srityje galiojimą reikėtų atidžiai atsižvelgti į aplinkybes, kuriomis prašoma sutikimo.

Pastaruoju metu įprastoje darbo aplinkoje susiduriama su bendra duomenų apsaugos problema, susijusia su teisėta darbuotojų susirašinėjimo darbo vietoje stebėjimo apimtimi. Dažnai teigiama, kad šią problemą galima lengvai išspręsti draudžiant darbe naudoti asmeninę ryšių įrangą. Tačiau toks bendras draudimas galėtų būti neproporcingas ir nerealus. Toliau nurodytas EŽTT sprendimas aptariamomis aplinkybėmis ypač tinkamas.

Pavyzdys. Byloje *Copland prieš JK*[303] siekiant išsiaiškinti, ar kolegijos darbuotoja pernelyg dažnai asmeninėms reikmėms nesinaudoja kolegijos įranga, buvo slapta stebima, kaip ji naudojasi kolegijos telefonu, el. paštu ir internetu. EŽTT nustatė, kad telefono skambučiams iš įmonės patalpų buvo taikomos privataus gyvenimo ir susirašinėjimo sąvokos. Todėl tokie skambučiai ir el. laiškai iš darbo vietos, taip pat informacija, gauta stebint asmeninį interneto naudojimą, buvo apsaugoti pagal EŽTK 8 straipsnį. Pareiškėjos byloje negaliojo jokios nuostatos, reglamentuojančios aplinkybes, kuriomis darbdaviai galėtų stebėti, kaip darbuotojai naudojasi telefonu, el. paštu ir internetu. Todėl apribojimas neatitiko įstatymo. Teismas nusprendė, kad EŽTK 8 straipsnis buvo pažeistas.

300 Europos Tarybos Ministrų Komitetas (1989 m.), 1989 m. sausio 18 d. Rekomendacija Nr. R (89) 2 valstybėms narėms dėl asmens duomenų, naudojamų įdarbinimo tikslais, apsaugos. Taip pat žr. 2011 m. rugsėjo 9 d. Konvencijos Nr. 108 konsultacinio komiteto atliktą Rekomendacijos Nr. R (89) 2 valstybėms narėms dėl asmens duomenų, naudojamų įdarbinimo tikslais, apsaugos tyrimą, kuriame pateikiami pasiūlymai persvarstyti minėtą rekomendaciją.

301 29 straipsnio duomenų apsaugos darbo grupė (2001 m.), 2001 m. rugsėjo 13 d. *Nuomonė 8/2001 dėl asmens duomenų tvarkymo užimtumo srityje*, WP 48, Briuselis.

302 29 straipsnio duomenų apsaugos darbo grupė (2005 m.), 2005 m. lapkričio 25 d. *Darbo dokumentas dėl 1995 m. spalio 24 d. Direktyvos 95/46/EB 26 straipsnio 1 dalies vienodo aiškinimo*, WP 114, Briuselis.

303 2007 m. balandžio 3 d. EŽTT sprendimas *Copland prieš Jungtinę Karalystę*, Nr. 62617/00.

Pagal ET rekomendaciją dėl užimtumo įdarbinimo tikslais renkami duomenys turėtų būti gaunami tiesiogiai iš darbuotojo.

Įdarbinimo tikslais surinkti asmens duomenys turi būti susiję tik su ta informacija, kurios reikia kandidatų tinkamumui ir jų karjeros galimybėms įvertinti.

Rekomendacijoje taip pat konkrečiai užsimenama apie kritinius duomenis, susijusius su atskirų darbuotojų darbu arba potencialu. Kritiniai 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 siekiant jiems sudaryti sąlygas atstovauti darbuotojų interesams.

Įdarbinimo tikslais surinkti ypatingi asmens duomenys gali būti tvarkomi tik konkrečiais atvejais ir atsižvelgiant į vidaus teisėje nustatytas apsaugos priemones. Darbdaviai gali prašyti darbuotojų arba darbo pareiškėjų nurodyti savo sveikatos būklę arba atlikti jų medicininę apžiūrą tik jeigu to reikia siekiant nustatyti, ar jie tinka dirbti siūlomą darbą, įgyvendinti profilaktinės medicinos reikalavimus arba nustatyti sąlygas socialinėms išmokoms mokėti. Asmens sveikatos duomenų negalima rinkti iš kitų nei darbuotojas šaltinių, išskyrus atvejus, kai buvo gautas aiškus informuoto asmens sutikimas, arba kai tokia galimybė numatyta nacionalinėje teisėje.

Pagal Rekomendaciją dėl užimtumo darbuotojai turėtų būti informuojami apie jų asmens duomenų tvarkymo tikslą, saugomų asmens duomenų rūšį, subjektus, kuriems reguliariai teikiami duomenys, ir tokio duomenų teikimo tikslą ir teisinį pagrindą. Darbdaviai taip pat turėtų iš anksto informuoti savo darbuotojus apie automatinių darbuotojų asmens duomenų tvarkymo arba darbuotojų judėjimo ar produktyvumo stebėjimo sistemų numatymą ir įdiegimą.

Darbuotojams turi būti suteikiama teisė susipažinti su savo užimtumo duomenimis, taip pat teisė reikalauti, kad duomenys būtų ištaisyti arba sunaikinti. Tvarkant kritinius duomenis darbuotojai turi teisę ginčyti kritiniais duomenimis pagrįstą sprendimą. Vis dėlto šios teisės laikinai gali būti ribojamos siekiant atlikti vidaus tyrimus. Jei atsisakoma darbuotojui leisti susipažinti su asmeniniais užimtumo duomenimis, juos ištaisyti arba sunaikinti, nacionalinėje teisėje turi būti numatytos tinkamos tokio atsisakymo ginčijimo procedūros.

8.3. Medicininiai duomenys

Pagrindinis faktas

- Medicininiai duomenys yra ypatingi duomenys, todėl jiems taikoma speciali apsauga.

Su duomenų subjekto sveikatos būkle susiję asmens duomenys pagal Duomenų apsaugos direktyvos 8 straipsnio 1 dalį ir Konvencijos Nr. 108 6 straipsnį laikomi ypatingais duomenimis. Todėl medicininiams duomenims taikomas griežtesnis duomenų tvarkymo režimas, palyginti su neypatingais duomenimis.

Pavyzdys. Byloje *Z. prieš Suomiją*[304] pareiškėjos buvęs vyras, kuris buvo užsikrėtęs ŽIV, padarė įvairius seksualinius nusikaltimus. Vėliau jis buvo nuteistas už žmogžudystę remiantis tuo, kad sąmoningai kėsinosi užkrėsti savo aukas ŽIV. Nacionalinis teismas nusprendė, kad visas teismo sprendimas ir visi bylos dokumentai turi išlikti konfidencialūs 10 metų, nepaisant pareiškėjos prašymo išlaikyti konfidencialumą ilgesnį laiką. Apeliacinis teismas atsisakė patenkinti šiuos prašymus ir jo sprendime buvo nurodyti pareiškėjos ir jos buvusio vyro vardai ir pavardės. EŽTT nusprendė, kad apribojimas nebuvo būtinas demokratinėje visuomenėje, nes medicininių duomenų apsauga buvo ypač svarbi naudojantis teise į privatų ir šeimos gyvenimą, visų pirma atsižvelgiant į ŽIV infekciją dėl daugumoje valstybių su šia liga susijusių stereotipų. Todėl Teismas padarė išvadą, kad, leidus su pareiškėjos tapatybe ir sveikatos būkle, kaip aprašyta apeliacinio teismo sprendime, susipažinti tik po 10 metų nuo teismo sprendimo priėmimo, būtų pažeistas EŽTK 8 straipsnis.

Pagal Duomenų apsaugos direktyvos 8 straipsnio 3 dalį medicininius duomenis tvarkyti leidžiama tais atvejais, kai duomenis reikia tvarkyti teikiant profilaktines medicinos, medicininės diagnostikos, priežiūros ar gydymo paslaugas arba valdant sveikatos priežiūros paslaugas. Vis dėlto duomenis tvarkyti leidžiama tik sveikatos priežiūros specialistui, kuris privalo laikytis profesinės paslapties pareigos, arba kitam asmeniui, kuriam taikoma tokia pati pareiga[305].

304 1997 m. vasario 25 d. EŽTT sprendimo *Z. prieš Suomiją*, Nr. 22009/93, 94 ir 112 punktai; taip pat žr. 1997 m. rugpjūčio 27 d. EŽTT sprendimą *M. S. prieš Švediją*, Nr. 20837/92; 2006 m. spalio 10 d. EŽTT sprendimą *L. L. prieš Prancūziją*, Nr. 7508/02; 2008 m. liepos 17 d. EŽTT sprendimą *I. prieš Suomiją*, Nr. 20511/03; 2009 m. balandžio 28 d. EŽTT sprendimą *K. H. ir kiti prieš Slovakiją*, Nr. 32881/04; 2009 m. birželio 2 d. EŽTT sprendimą *Szuluk prieš Jungtinę Karalystę*, Nr. 36936/05.

305 Taip pat žr. 2008 m. lapkričio 25 d. EŽTT sprendimą *Biriuk prieš Lietuvą*, Nr. 23373/03.

1997 m. ET Rekomendacijoje dėl medicininių duomenų numatyta išsamesnė Konvencijos Nr. 108 principų taikymo medicinos srityje tvarka[306]. Siūlomos taisyklės atitinka Duomenų apsaugos direktyvos taisykles, susijusias su teisėtais medicininių duomenų tvarkymo tikslais, būtinais įsipareigojimais saugoti profesinę paslaptį, kurių turi laikytis sveikatos duomenis naudojantys asmenys, ir duomenų subjektų teisėmis į skaidrius duomenis ir teisė susipažinti su duomenimis ir reikalauti, kad jie būtų ištaisyti ir ištrinti. Be to, medicininiai duomenys, kuriuos teisėtai tvarko sveikatos priežiūros specialistai, negali būti teikiami teisėsaugos institucijoms, išskyrus atvejus, kai numatomos „pakankamos apsaugos priemonės, padedančios užkirsti kelią su privačiu gyvenimu, kuris garantuojamas pagal EŽTK 8 straipsnį, nesuderinamam duomenų atskleidimui“[307].

Be to, Rekomendacijoje dėl medicininių duomenų yra pateikiamos konkrečios nuostatos dėl negimusių vaikų ir riboto veiksnumo asmenų medicininių duomenų ir genetinių duomenų tvarkymo. Neabejotinai pripažįstama, kad moksliniai tyrimai yra tinkama priežastis saugoti duomenis ilgiau nei reikia, nors paprastai tokiu atveju duomenis reikalaujama anonimizuoti. Rekomendacijos dėl medicininių duomenų 12 straipsnyje pateikiamos išsamios taisyklės, taikytinos tais atvejais, kai tyrėjams reikalingi asmens duomenys, o anoniminių duomenų nepakanka.

Pseudonimizacija gali būti tinkama priemonė moksliniams poreikiams patenkinti ir kartu apsaugoti susijusio paciento interesus. Pseudonimizacijos sąvoka duomenų apsaugos srityje išsamiau aptariama 2.1.3 dalyje.

Nacionaliniu ir Europos lygmenimis vyko intensyvios diskusijos dėl iniciatyvų, susijusių su pacientų medicininio gydymo duomenų saugojimu elektroninėje sveikatos istorijoje[308]. Konkretus elektroninių sveikatos istorijų sistemų aspektas yra susijęs su jų tarpvalstybiniu prieinamumu, tai yra ypatingos svarbos ES klausimas tarpvalstybinės sveikatos priežiūros srityje[309].

Kita aptariama sritis, susijusi su naujomis nuostatomis, yra klinikiniai tyrimai, kitaip tariant, naujų pacientams skirtų vaistų bandymai dokumentuojamų mokslinių tyrimų

306 ET Ministrų Komitetas (1997 m.), Rekomendacija Nr. R (97) 5 valstybėms narėms dėl medicininių duomenų apsaugos, 1997 m. vasario 13 d.

307 2013 m. birželio 6 d. EŽTT sprendimo Nr. 1585/09, *Avilkina ir kiti prieš Rusiją*, 53 punktas (negalutinis).

308 29 straipsnio duomenų apsaugos darbo grupė (2007 m.), *Darbinis dokumentas dėl asmens sveikatos duomenų tvarkymo elektroninėse sveikatos istorijose (ESI)*, WP 131, Briuselis, 2007 m. vasario 15 d.

309 2011 m. kovo 9 d. Europos Parlamento ir Tarybos direktyva 2011/24/ES dėl pacientų teisių į tarpvalstybines sveikatos priežiūros paslaugas įgyvendinimo, OL L 88, 2011.

srityje; be to, šis klausimas yra susijęs su rimtomis duomenų apsaugos pasekmėmis. Klinikiniai žmonėms skirtų vaistų bandymai reglamentuojami 2001 m. balandžio 4 d. Europos Parlamento ir Tarybos direktyvoje 2001/20/EB dėl valstybių narių įstatymų ir kitų teisės aktų, susijusių su geros klinikinės praktikos įgyvendinimu atliekant žmonėms skirtų vaistų klinikinius tyrimus, suderinimo (*Klinikinių tyrimų direktyva*)[310]. 2012 m. gruodžio mėn. Europos Komisija pasiūlė Klinikinių tyrimų direktyvą pakeičiantį reglamentą, kurio tikslas – suvienodinti klinikinių tyrimų procedūras ir padaryti jas veiksmingesnes[311].

ES lygmeniu esama daug kitų teisėkūros ir kitokių iniciatyvų, susijusių su sveikatos sektoriaus asmens duomenimis[312].

8.4. Duomenų tvarkymas statistiniais tikslais

Pagrindiniai faktai

- Statistiniais tikslais surinkti duomenys negali būti naudojami jokiu kitu tikslu.
- Teisėtai bet kuriuo tikslu surinkti duomenys toliau gali būti naudojami statistiniais tikslais, jeigu nacionalinėje teisėje yra nustatytos tinkamos apsaugos priemonės, kurių turi paisyti duomenų naudotojai. Šiuo tikslu prieš teikiant duomenis trečiosioms šalims reikėtų numatyti duomenų anonimizavimą arba pseudonimizavimą.

Duomenų apsaugos direktyvoje duomenų tvarkymas statistiniais tikslais nurodomas kaip viena galimų duomenų apsaugos principų išimčių. Pagal Direktyvos 6 straipsnio 1 dalies b punktą nacionalinėje teisėje tikslo ribojimo principu siekiant toliau naudoti duomenis statistiniais tikslais galima remtis, tačiau nacionaliniame įstatyme taip pat turi būti nustatytos visos būtinos apsaugos priemonės. Direktyvos 13 straipsnio 2 dalyje leidžiama nacionaliniame įstatyme riboti teises susipažinti su duomenimis, jeigu duomenys tvarkomi tik statistiniais tikslais; be to, nacionalinėje teisėje turi būti

310 2001 m. balandžio 4 d. Europos Parlamento ir Tarybos direktyva 2001/20/EB dėl valstybių narių įstatymų ir kitų teisės aktų, susijusių su geros klinikinės praktikos įgyvendinimu atliekant žmonėms skirtų vaistų klinikinius tyrimus, suderinimo, OL L 121, 2001.

311 Europos Komisija (2012 m.), *Pasiūlymas Europos Parlamento ir Tarybos reglamentas dėl žmonėms skirtų vaistų klinikinių tyrimų, kuriuo panaikinama Direktyva 2001/20/EB*, KOM(2012) 369 galutinis, Briuselis, 2012 m. liepos 17 d.

312 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.

numatytos tinkamos apsaugos priemonės. Šiomis aplinkybėmis Duomenų apsaugos direktyvoje nustatytas konkretus reikalavimas, kad jokie statistinio mokslinio tyrimo metu gauti arba sukurti duomenys negali būti naudojami konkretiems sprendimams, susijusiems su duomenų subjektais, priimti.

Nors bet kokiu tikslu duomenų valdytojo surinkti duomenys šio duomenų valdytojo gali būti pakartotinai naudojami statistiniais tikslais, – vadinamoji antrinė statistika, – duomenys prieš juos teikiant trečiajai šaliai statistiniais tikslais turėtų būti, priklausomai nuo situacijos, anonimizuojami arba pseudonimizuojami, išskyrus atvejus, kai duomenų subjektas su tuo sutiko arba tai konkrečiai numatyta nacionaliniame įstatyme. Ši išvada daroma atsižvelgiant į tinkamų apsaugos priemonių reikalavimą, numatytą Duomenų apsaugos direktyvos 6 straipsnio 1 dalies b punkte.

Dažniausiai duomenys statistiniais tikslais naudojami rengiant oficialią statistiką ir tai daro pagal ES įstatymus dėl oficialios statistikos įsteigti nacionaliniai ir ES statistikos biurai. Remiantis šiais įstatymais piliečiai ir įmonės paprastai įpareigojami atskleisti duomenis statistikos institucijoms. Statistikos biuruose dirbantys pareigūnai turi laikytis konkrečių profesinės paslapties įsipareigojimų, kurių laikymasis atidžiai stebimas, nes tai yra labai svarbu siekiant užtikrinti didelį piliečių pasitikėjimą, kuris yra būtinas, jei bus leista su duomenimis susipažinti statistikos institucijoms.

Reglamente (EB) Nr. 223/2009 dėl Europos statistikos (*Europos statistikos reglamentas*) pateikiamos esminės taisyklės dėl duomenų apsaugos oficialios statistikos srityje ir todėl jos gali būti svarbios atsižvelgiant į nacionalines oficialios statistikos nuostatas[313]. Reglamente įtvirtintas principas, kad oficialios statistikos operacijos turi būti atliekamos remiantis konkrečiu teisiniu pagrindu[314].

Pavyzdys. Byloje *Huber prieš Vokietiją*[315] ESTT nustatė, kad institucijos atliekamas duomenų rinkimas ir saugojimas statistiniais tikslais pats savaime nebuvo pakankamas pagrindas teisėtai tvarkyti duomenis. Asmens duomenų tvarkymą

313 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.

314 Šis principas turi būti išsamiau aptartas Eurostato praktikos kodekse, kuriame pagal Europos statistikos reglamento 11 straipsnį pateikiamos etinės gairės dėl oficialios statistikos, įskaitant tikslų asmens duomenų naudojimą, rengimo; galima rasti adresu http://epp.eurostat.ec.europa.eu/portal/page/portal/about_eurostat/introduction.

315 2008 m. gruodžio 16 d. ESTT sprendimas *Huber prieš Vokietiją*, C-524/06; žr. visų pirma 68 punktą.

reglamentuojančiame įstatyme taip pat buvo numatytas būtinumo reikalavimas, kuris nebuvo tenkinamas nagrinėjamoje byloje.

ET kontekste Rekomendacija dėl statistinių duomenų, priimta 1997 m., apima statistinių duomenų rinkimą viešajame ir privačiajame sektoriuose[316]. Šioje rekomendacijoje nustatyti principai, kurie sutampa su pagrindinėmis jau aprašytomis Duomenų apsaugos direktyvos taisyklėmis. Išsamesnės taisyklės pateikiamos dėl toliau aptariamų klausimų.

Duomenų valdytojo statistiniais tikslais surinkti duomenys negali būti naudojami kuriuo nors kitu tikslu, o duomenys, kurie buvo surinkti ne statistiniais tikslais, gali būti toliau naudojami statistiniais tikslais. Rekomendacijoje dėl statistinių duomenų netgi leidžiama teikti duomenis trečiosioms šalims, jeigu jie teikiami tik statistiniais tikslais. Tokiais atvejais šalys turėtų susitarime aprašyti teisėto tolesnio duomenų naudojimo statistiniais tikslais apimtį. Kadangi toks susitarimas negali pakeisti duomenų subjekto sutikimo, turi būti daroma prielaida, kad nacionalinėje teisėje yra nustatytos papildomos apsaugos priemonės, kuriomis kuo labiau sumažinamas netinkamo asmens duomenų naudojimo pavojus, pvz., pareiga anonimizuoti arba pseudonimizuoti teikiamus duomenis.

Statistinius mokslinius tyrimus atliekantiems specialistams nacionalinėje teisėje (kaip ir oficialios statistikos atveju) turėtų būti nustatyti konkretūs įpareigojimai išsaugoti profesinę paslaptį. Šių pareigų taip pat turėtų laikytis apklausas atliekantys asmenys, jei jų įdarbinimo tikslas – rinkti duomenis iš duomenų subjektų arba kitų asmenų.

Jeigu statistinė apklausa, kurioje naudojami asmens duomenys, nėra reglamentuojama įstatymu, duomenų subjektai, kad toks naudojimas būtų teisėtas, turėtų duoti sutikimą naudoti jų duomenis arba jiems bent jau turėtų būti suteikiama galimybė nesutikti dėl to. Jeigu asmens duomenis statistiniais tikslais surenka apklausas atliekantys asmenys, jie turi būti aiškiai informuojami, ar pagal nacionalinę teisę privaloma atskleisti duomenis. Ypatingi duomenys niekada neturėtų būti renkami taip, kuris būtų galima nustatyti asmens tapatybę, išskyrus atvejus, kai tai aiškiai leidžiama pagal nacionalinį įstatymą.

316 Europos Tarybos Ministrų Komitetas (1997 m.), Rekomendacija Nr. R (97) 18 valstybėms narėms dėl asmens duomenų, renkamų ir tvarkomų statistiniais tikslais, apsaugos, 1997 m. rugsėjo 30 d.

Kai statistinės apklausos negalima atlikti su anoniminiais duomenimis ir asmens duomenys iš tikrųjų yra būtini, šiuo tikslu surinkti duomenys turėtų būti anonimizuojami iš karto, kai tai tampa įmanoma. Statistinės apklausos rezultatai bent jau negali sudaryti sąlygų nustatyti kurių nors duomenų subjektų tapatybes, išskyrus atvejus, kai akivaizdu, kad tai nekelia jokio pavojaus.

Užbaigus statistinę analizę, naudoti asmens duomenys turėtų būti ištrinami arba anonimizuojami. Šiuo atveju Rekomendacijoje dėl statistinių duomenų siūloma tapatybę padedančius nustatyti duomenis saugoti atskirai nuo kitų asmens duomenų. Tai, pavyzdžiui, reiškia, kad duomenys turėtų būti pseudonimizuojami, o iššifravimo raktas arba sinonimų kodų sąrašas turėtų būti saugomi atskirai nuo pseudoniminių duomenų.

8.5. Finansiniai duomenys

Pagrindiniai faktai

- Nors finansiniai duomenys nėra ypatingi duomenys, kaip apibrėžta Konvencijoje Nr. 108 arba Duomenų apsaugos direktyvoje, juos tvarkant turi būti taikomos ypatingos apsaugos priemonės, užtikrinančios duomenų tikslumą ir saugumą.
- Elektroninio mokėjimo sistemose turi būti integruota duomenų apsauga, t. y. pritaikytoji duomenų apsauga.
- Šioje srityje ypatingos duomenų apsaugos problemos kyla dėl poreikio taikyti tinkamus tapatumo nustatymo mechanizmus.

Pavyzdys. *Michaud prieš Prancūziją*[317] pareiškėjas (Prancūzijos advokatas) ginčijo Prancūzijos įstatyme nustatytą pareigą pranešti apie savo klientų įtartiną veiklą, susijusią su galimu pinigų plovimu. EŽTT atkreipė dėmesį į tai, kad reikalavimas, kad advokatai teiktų administracinėms institucijoms su kitu asmeniu susijusią informaciją, kurią advokatai sužinojo bendraudami su savo klientais, reiškė advokatų teisės į susirašinėjimą ir pagarbą privačiam gyvenimui pagal EŽTK 8 straipsnį apribojimą, nes ši sąvoka apėmė profesinę arba verslo veiklą. Tačiau apribojimas atitiko įstatymą ir juo buvo siekiama teisėto tikslo, t. y.

317 2012 m. gruodžio 6 d. EŽTT sprendimas *Michaud prieš Prancūziją*, Nr. 12323/11; taip pat žr. 1992 m. gruodžio 16 d. EŽTT sprendimo *Niemietz prieš Vokietiją*, Nr. 13710/88, 29 punktą, ir 1997 m. birželio 25 d. EŽTT sprendimo *Halford prieš Jungtinę Karalystę*, Nr. 20605/92, 42 punktą.

užkirsti kelią neramumams ir nusikaltimams. Kadangi advokatai turėjo laikytis pareigos pranešti apie įtartiną veiklą tik labai specifinėmis aplinkybėmis, EŽTT nustatė, kad ši pareiga buvo tinkama, ir nusprendė, kad 8 straipsnis nebuvo pažeistas.

Bendrosios duomenų apsaugos teisinės sistemos, kuri įtvirtinta Konvencijoje Nr. 108, taikymas mokėjimų srityje išsamiau reglamentuojamas 1990 m. ET rekomendacijoje Nr. (90) 19[318]. Šioje rekomendacijoje paaiškinama teisėto su mokėjimais (visų pirma atliekamais naudojant mokėjimo korteles) susijusių duomenų rinkimo ir naudojimo taikymo sritis. Joje taip pat siūloma vidaus teisės aktų leidėjams nustatyti išsamias taisykles dėl trečiosioms šalims teikiamų mokėjimo duomenų ribų, duomenų saugojimo terminų, skaidrumo, duomenų saugumo ir valstybės sienas kertančių duomenų srautų ir galiausiai dėl priežiūros ir teisių gynimo priemonių. Siūlomi sprendimai yra susiję su vėliau Duomenų apsaugos direktyva įtvirtintoje ES bendra duomenų apsaugos sistemoje numatytomis priemonėmis.

Šiuo metu kuriamos įvairios teisinės priemonės, skirtos finansinių priemonių rinkoms ir kredito įstaigų ir investicinių įmonių veiklai reglamentuoti[319]. Kitos teisinės priemonės padeda kovoti su prekyba vertybiniais popieriais naudojantis viešai neatskleista informacija ir rinkos manipuliacija[320]. Esminiai šių sričių klausimai, kurie daro poveikį duomenų apsaugai, yra susiję su:

- finansinių sandorių įrašų saugojimu;

318 ET, Ministrų Komitetas (1990 m.), 1990 m. rugsėjo 13 d. Rekomendacija Nr. R (90) 19 dėl asmens duomenų, naudojamų apmokėjimui arba kitoms su tuo susijusioms operacijoms, apsaugos.

319 Europos Komisija (2011 m.), 2011 m. spalio 20 d. *Pasiūlymas Europos Parlamento ir Tarybos direktyva dėl finansinių priemonių rinkų, kuria panaikinama Europos Parlamento ir Tarybos direktyva 2004/39/EB*, KOM(2011) 656 galutinis, Briuselis; Europos Komisija (2011 m.), 2011 m. spalio 20 d. *Pasiūlymas Europos Parlamento ir Tarybos reglamentas dėl finansinių priemonių rinkų, kuriuo iš dalies keičiamas Reglamentas dėl ne biržos išvestinių finansinių priemonių, pagrindinių sandorio šalių ir sandorių duomenų saugyklų*, KOM(2011) 652 galutinis, Briuselis; Europos Komisija (2011 m.), 2011 m. liepos 20 d. *Pasiūlymas Europos Parlamento ir Tarybos direktyva dėl galimybės verstis kredito įstaigų veikla ir dėl rizikos ribojimu pagrįstos kredito įstaigų ir investicinių įmonių priežiūros, kuria iš dalies keičiama Europos Parlamento ir Tarybos direktyva 2002/87/EB dėl finansiniam konglomeratui priklausančių kredito įstaigų, draudimo įmonių ir investicinių įmonių papildomos priežiūros*, KOM(2011) 453 galutinis, Briuselis.

320 Europos Komisija (2011 m.), 2011 m spalio 20 d. *Pasiūlymas Europos Parlamento ir Tarybos reglamentas dėl prekybos vertybiniais popieriais naudojantis viešai neatskleista informacija ir manipuliavimo rinka (piktnaudžiavimo rinka)*, KOM(2011) 651 galutinis, Briuselis; Europos Komisija (2011 m.), 2011 m spalio 20 d. *Pasiūlymas Europos Parlamento ir Tarybos direktyva dėl baudžiamųjų sankcijų už prekybą vertybiniais popieriais naudojantis viešai neatskleista informacija ir už manipuliavimą rinka*, KOM(2011) 654 galutinis, Briuselis.

- asmens duomenų perdavimu trečiosioms valstybėms;
- pokalbių telefonu arba elektroninių ryšių įrašinėjimu, įskaitant kompetentingų institucijų įgaliojimus prašyti pateikti telefono ir srauto duomenų įrašus;
- asmeninės informacijos atskleidimu, įskaitant sankcijų paskelbimą;
- kompetentingų institucijų priežiūros ir tyrimų įgaliojimais, įskaitant patikrinimus vietoje ir patekimą į privačias patalpas siekiant paimti dokumentus;
- pranešimų apie pažeidimus mechanizmais, t. y. informatorių schemomis, ir
- valstybių narių kompetentingų institucijų ir Europos vertybinių popierių ir rinkos institucijos (EVPRI) bendradarbiavimu.

Šiose srityse taip pat kyla kitų klausimų, kurie sprendžiami konkrečiomis priemonėmis, įskaitant duomenų apie jų subjektų finansinę padėtį rinkimą[321] arba tarpvalstybinius mokėjimus atliekant banko pavedimus, kurie neišvengiamai yra susiję su asmens duomenų srautais[322].

321 2009 m. rugsėjo 16 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 1060/2009 dėl kredito reitingų agentūrų, OL L 302, 2009; Europos Komisija, *Pasiūlymas Europos Parlamento ir Tarybos reglamentas, kuriuo iš dalies keičiamas Reglamentas (EB) Nr. 1060/2009 dėl kredito reitingų agentūrų*, KOM(2010) 289 galutinis, Briuselis, 2010 m. birželio 2 d.

322 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.

Papildoma literatūra

1 skyrius

Araceli Mangas, M. (ed.) (2008), *Carta de los derechos fundamentales de la Unión Europea*, Bilbao, Fundación BBVA.

Berka, W. (2012), *Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit*, Vienna, Manzsche Verlags- und Universitätsbuchhandlung.

EDRi, *An introduction to data protection*, Briuselis, galima rasti adresu www.edri.org/files/paper06_datap.pdf.

Frowein, J. and Peukert, W. (2009), *Europäische Menschenrechtskonvention*, Berlin, N. P. Engel Verlag.

Grabenwarter, C. and Pabel, K. (2012), *Europäische Menschenrechtskonvention*, Munich, C. H. Beck.

Harris, D., O'Boyle, M., Warbrick, C. and Bates, E. (2009), *Law of the European Convention on Human Rights*, Oxford, Oxford University Press.

Jarass, H. (2010), *Charta der Grundrechte der Europäischen Union*, Munich, C. H. Beck.

Mayer, J. (2011), *Charta der Grundrechte der Europäischen Union*, Baden-Baden, Nomos.

Mowbray, A. (2012), *Cases, materials, and commentary on the European Convention on Human Rights*, Oxford, Oxford University Press.

Nowak, M., Januszewski, K. and Hofstätter, T. (2012), *All human rights for all – Vienna manual on human rights*, Antwerp, intersentia N. V., Neuer Wissenschaftlicher Verlag.

Picharel, C. and Coutron, L. (2010), *Charte des droits fondamentaux de l'Union européenne et convention européenne des droits de l'homme*, Brussels, Emile Bruylant.

Simitis, S. (1997), „Die EU-Datenschutz-Richtlinie – Stillstand oder Anreiz?", *Neue Juristische Wochenschrift*, Nr. 5, p. 281–288.

Warren, S. and Brandeis, L. (1890), „The right to privacy', *Harvard Law Review,* Vol. 4, Nr. 5, p. 193–220, galima rasti adresu www.english.illinois.edu/-people-/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf.

White, R. and Ovey, C. (2010), *The European Convention on Human Rights*, Oxford, Oxford University Press.

2 skyrius

Carey, P. (2009), *Data protection: A practical guide to UK and EU law*, Oxford, Oxford University Press.

Delgado, L. (2008), *Vida privada y protección de datos en la Unión Europea*, Madrid, Dykinson S. L.

Desgens-Pasanau, G. (2012), *La protection des données à caractère personnel*, Paris, LexisNexis.

Di Martino, A. (2005), *Datenschutz im europäischen Recht*, Baden-Baden, Nomos.

Morgan, R. and Boardman, R. (2012), *Data protection strategy: Implementing data protection compliance*, London, Sweet & Maxwell.

Ohm, P. (2010), „Broken promises of privacy: Responding to the surprising failure of anonymization", *UCLA Law Review*, Vol. 57, Nr. 6, p. 1701–1777.

Tinnefeld, M., Buchner, B. and Petri, T. (2012), *Einführung in das Datenschutzrecht: Datenschutz und Informationsfreiheit in europäischer Sicht*, Munich, Oldenbourg Wissenschaftsverlag.

United Kingdom Information Commissioner's Office (2012), *Anonymisation: managing data protection risk. Code of practice*, galima rasti adresu www.ico.org.uk/for_organisations/data_protection/topic_guides/anonymisation.

3–5 skyriai

Brühann, U. (2012), „Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr", pateikiama Grabitz, E., Hilf, M. ir NESTTesheim, M. (eds.), *Das Recht der Europäischen Union*, Band IV, A. 30, Munich, C. H. Beck.

Conde Ortiz, C. (2008), *La protección de datos personales*, Cadiz, Dykinson.

Coudray, L. (2010), *La protection des données personnelles dans l'Union européenne*, Saarbrücken, Éditions universitaires européennes.

Dammann, U. and Simitis, S. (1997), *EG-Datenschutzrichtlinie*, Baden-Baden, Nomos.

FRA (Europos Sąjungos pagrindinių teisių agentūra) (2010), *Data Protection in the European Union: the role of National Data Protection Authorities (Strengthening the fundamental rights architecture in the EU II)*, Liuksemburgas, Europos Sąjungos leidinių biuras (Leidinių biuras).

FRA (2010), *Developing indicators for the protection, respect and promotion of the rights of the child in the European Union* (Conference edition), Vienna, FRA.

FRA (2011), *Access to justice in Europe: an overview of challenges and opportunities*, Liuksemburgas, Leidinių Biuras.

Simitis, S. (2011), *Bundesdatenschutzgesetz*, Baden-Baden, Nomos.

United Kingdom Information Commissioner's Office, *Privacy Impact Assessment*, galima rasti adresu www.ico.org.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment.

6 skyrius

Gutwirth, S., Poullet, Y., De Hert, P., De Terwangne, C. and Nouwt, S. (2009), *Reinventing data protection?*, Berlin, Springer.

Kuner, C. (2007), *European data protection law*, Oxford, Oxford University Press.

Kuner, C. (2013), *Transborder data flow regulation and data privacy law*, Oxford, Oxford University Press.

7 skyrius

Europolas (2012), *Data Protection at Europol*, Liuksemburgas, Leidinių biuras, galima rasti adresu www.europol.europa.eu/sites/default/files/publications/europol_dpo_booklet_0.pdf.

Eurojustas, *Data protection at Eurojust: A robust, effective and tailor-made regime*, Haga, Eurojustas.

Drewer, D., Ellermann, J. (2012), *Europol's data protection framework as an asset in the fight against cybercrime,* ERA Forum, Vol. 13, Nr. 3, p. 381–395.

Gutwirth, S., Poullet, Y. and De Hert, P. (2010), *Data protection in a profiled world*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. and Leenes, R. (2011), *Computers, privacy and data protection: An element of choice*, Dordrecht, Springer.

Konstadinides, T. (2011), *Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem*, *European Law Review*, Vol. 36, Nr. 5, p. 722–776.

Santos Vara, J. (2013), *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, galima rasti adresu www.asser.nl/upload/documents/20130226T013310-cleer_13-2_web.pdf.

8 skyrius

Büllesbach, A., Gijrath, S., Poullet, Y. and Hacon, R. (2010), *Concise European IT law*, Amsterdam, Kluwer Law International.

Gutwirth, S., Leenes, R., De Hert, P. and Poullet, Y. (2012), *European data protection: In good health?*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y. and De Hert, P. (2010), *Data protection in a profiled world*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. and Leenes, R. (2011), *Computers, privacy and data protection: An element of choice*, Dordrecht, Springer.

Konstadinides, T. (2011), Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem, *European Law Review*, Vol. 36, Nr. 5, p. 722–776.

Rosemary, J. and Hamilton, A. (2012), *Data protection law and practice*, London, Sweet & Maxwell.

Teismų praktika

Europos Žmogaus Teisių Teismo atrinkta praktika

Galimybė susipažinti su asmens duomenimis

1989 m. liepos 7 d. EŽTT sprendimas *Gaskin prieš Jungtinę Karalystę*, Nr. 10454/83.
2012 m. rugsėjo 25 d. EŽTT sprendimas *Godelli prieš Italiją*, Nr. 33783/09.
2009 m. balandžio 28 d. EŽTT sprendimas *K. H. ir kiti prieš Slovakiją*, Nr. 32881/04.
1987 m. kovo 26 d. EŽTT sprendimas *Leander prieš Švediją*, Nr. 9248/81.
2003 m. vasario 13 d. EŽTT sprendimas *Odièvre prieš Prancūziją* (DK), Nr. 42326/98.

Duomenų apsaugos ir žodžio laisvės derinimas

2012 m. vasario 7 d. EŽTT sprendimas *Axel Springer AG prieš Vokietiją* (DK), Nr. 39954/08.
2004 m. birželio 24 d. EŽTT sprendimas *Von Hannover prieš Vokietiją*, Nr. 59320/00.
2012 m. vasario 7 d. EŽTT sprendimas *Von Hannover prieš Vokietiją (Nr. 2)* (DK), Nr. 40660/08 ir 60641/08.

Duomenų apsaugos internete problemos

2008 m. gruodžio 2 d. EŽTT sprendimas *K. U. prieš Suomiją*, Nr. 2872/02.

Susirašinėjimas

2000 m. vasario 16 d. EŽTT sprendimas *Amann prieš Šveicariją* (DK), Nr. 27798/95.

2013 m. kovo 14 d. EŽTT sprendimas *Bernh Larsen Holding AS ir kiti prieš Norvegiją*, Nr. 24117/08.
2008 m. lapkričio 18 d. EŽTT sprendimas *Cemalettin Canli prieš Turkiją*, Nr. 22427/04.
2010 m. vasario 2 d. EŽTT sprendimas *Dalea prieš Prancūziją,* Nr. 964/07.
1989 m. liepos 7 d. EŽTT sprendimas *Gaskin prieš Jungtinę Karalystę*, Nr. 10454/83.
2009 m. spalio 27 d. EŽTT sprendimas *Haralambie prieš Rumuniją*, Nr. 21737/03.
2011 m. spalio 18 d. EŽTT sprendimas *Khelili prieš Šveicariją*, Nr. 16188/07.
1987 m. kovo 26 d. EŽTT sprendimas *Leander prieš Švediją*, Nr. 9248/81.
1985m. balandžio 26 d. EŽTT sprendimas *Malone prieš Jungtinę Karalystę*, Nr. 8691/79.
1995 m. vasario 24 d. EŽTT sprendimas *McMichael prieš Jungtinę Karalystę*, Nr. 16424/90.
2002 m. rugsėjo 24 d. EŽTT sprendimas *M. G. prieš Jungtinę Karalystę*, Nr. 39393/98.
2000 m. gegužės 4 d. EŽTT sprendimas *Rotaru prieš Rumuniją* (DK), Nr. 28341/95.
2008 m. gruodžio 4 d. EŽTT sprendimas *S. ir Marper prieš Jungtinę Karalystę*, Nr. 30562/04 ir 30566/04.
2011 m. birželio 21 d. EŽTT sprendimas *Shimovolos prieš Rusiją*, Nr. 30194/09.
2006 m. vasario 14 d. EŽTT sprendimas *Turek prieš Slovakiją*, Nr. 57986/00.

Nuosprendžių registro duomenų bazės

2009 m. gruodžio 17 d. EŽTT sprendimas *B. B. prieš Prancūziją*, Nr. 5335/06.
2012 m. lapkričio 13 d. EŽTT sprendimas *M. M. prieš Jungtinę Karalystę*, Nr. 24029/07.

DNR duomenų bazės

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

GPS duomenys

2010 m. rugsėjo 2 d. EŽTT sprendimas *Uzun prieš Vokietiją*, Nr. 35623/05.

Sveikatos duomenys

2008 m. lapkričio 25 d. EŽTT sprendimas *Biriuk prieš Lietuvą*, Nr. 23373/03.
2008 m. liepos 17 d. EŽTT sprendimas *I. prieš Suomiją*, Nr. 20511/03.
2006 m. spalio 10 d. EŽTT sprendimas *L. L. prieš Prancūziją*, Nr. 7508/02.
2002 m. liepos 2 d. EŽTT sprendimas *M. S. prieš Švediją*, Nr. 34209/96.
2009 m. birželio 2 d. EŽTT sprendimas *Szuluk prieš Jungtinę Karalystę*, Nr. 36936/05.

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

Tapatybė

2010 m. balandžio 27 d. EŽTT sprendimas *Ciubotaru prieš Moldovą*, Nr. 27138/04.
2012 m. rugsėjo 25 d. EŽTT sprendimas *Godelli prieš Italiją*, Nr. 33783/09.
2003 m. vasario 13 d. EŽTT sprendimas *Odièvre prieš Prancūziją* (DK), Nr. 42326/98.

Su profesionalia veikla susijusi informacija

2012 m. gruodžio 6 d. EŽTT sprendimas *Michaud prieš Prancūziją*, Nr. 12323/11.
1992 m. gruodžio 16 d. EŽTT sprendimas *Niemietz prieš Vokietiją*, Nr. 13710/88.

Pranešimų perėmimas

2000 m. vasario 16 d. EŽTT sprendimas *Amann prieš Šveicariją* (DK), Nr. 27798/95.
2007 m. balandžio 3 d. EŽTT sprendimas *Copland prieš Jungtinę Karalystę*, Nr. 62617/00.
2003 m. birželio 3 d. EŽTT sprendimas *Cotlet prieš Rumuniją*, Nr. 38565/97.
1990 m. balandžio 24 d. EŽTT sprendimas *Kruslin prieš Prancūziją*, Nr. 11801/85.
1998 m. rugpjūčio 24 d. EŽTT sprendimas *Lambert prieš Prancūziją*, Nr. 23618/94.
2008 m. liepos 1 d. EŽTT sprendimas *Liberty ir kiti prieš Jungtinę Karalystę*, Nr. 58243/00.
1985 m. balandžio 26 d. EŽTT sprendimas *Malone prieš Jungtinę Karalystę*, Nr. 8691/79.
1997 m. birželio 25 d. EŽTT sprendimas *Halford prieš Jungtinę Karalystę*, Nr. 20605/92.
2009 m. birželio 2 d. EŽTT sprendimas *Szuluk prieš Jungtinę Karalystę*, Nr. 36936/05.

Subjektų, kuriems nustatytos pareigos, įsipareigojimai

2009 m. gruodžio 17 d. EŽTT sprendimas *B. B. prieš Prancūziją*, Nr. 5335/06.
2008 m. liepos 17 d. EŽTT sprendimas *I. prieš Suomiją*, Nr. 20511/03.
2011 m. gegužės 10 d. EŽTT sprendimas *Mosley prieš Jungtinę Karalystę*, Nr. 48009/08.

Nuotraukos

2005 m. sausio 11 d. EŽTT sprendimas *Sciacca prieš Italiją*, Nr. 50774/99.
2004 m. birželio 24 d. EŽTT sprendimas *Von Hannover prieš Vokietiją*, Nr. 59320/00.

Teisė būti pamirštam

2006 m. birželio 6 d. EŽTT sprendimas *Segerstedt-Wiberg ir kiti prieš Švediją*, Nr. 62332/00.

Teisė nesutikti

1987 m. kovo 26 d. EŽTT sprendimas *Leander prieš Švediją*, Nr. 9248/81.
2011 m. gegužės 10 d. EŽTT sprendimas *Mosley prieš Jungtinę Karalystę*, Nr. 48009/08.
2002 m. liepos 2 d. EŽTT sprendimas *M. S. prieš Švediją*, Nr. 34209/96.
2000 m. gegužės 4 d. EŽTT sprendimas *Rotaru prieš Rumuniją* (DK), Nr. 28341/95.

Ypatingų duomenų kategorijos

2008 m. liepos 17 d. EŽTT sprendimas *I. prieš Suomiją*, Nr. 20511/03.
2012 m. gruodžio 6 d. EŽTT sprendimas *Michaud prieš Prancūziją*, Nr. 12323/11.
2008 m. gruodžio 4 d. EŽTT sprendimas *S. ir Marper prieš Jungtinę Karalystę*, Nr. 30562/04 ir 30566/04.

Priežiūra ir vykdymo užtikrinimas (įvairių subjektų, įskaitant duomenų apsaugos institucijas, vaidmuo)

2008 m. liepos 17 d. EŽTT sprendimas *I. prieš Suomiją*, Nr. 20511/03.
2008 m. gruodžio 2 d. EŽTT sprendimas *K. U. prieš Suomiją*, Nr. 2872/02.
2004 m. birželio 24 d. EŽTT sprendimas *Von Hannover prieš Vokietiją*, Nr. 59320/00.
2012 m. vasario 7 d. EŽTT sprendimas *Von Hannover prieš Vokietiją (Nr. 2)* (DK), Nr. 40660/08 ir 60641/08.

Stebėjimo metodai

2002 m. lapkričio 5 d. EŽTT sprendimas *Allan prieš Jungtinę Karalystę*, Nr. 48539/99.
2011 m. gegužės 24 d. EŽTT sprendimas *Association „21 Décembre 1989" ir kiti prieš Rumuniją*, Nr. 33810/07 ir 18817/08.
2009 m. kovo 10 d. EŽTT sprendimas *Bykov prieš Rusiją* (DK), Nr. 4378/02.
2010 m. gegužės 18 d. EŽTT sprendimas *Kennedy prieš Jungtinę Karalystę*, Nr. 26839/05.
1978 m. rugsėjo 6 d. EŽTT sprendimas *Klass ir kiti prieš Vokietiją*, Nr. 5029/71.
2000 m. gegužės 4 d. EŽTT sprendimas *Rotaru prieš Rumuniją* (DK), Nr. 28341/95.
2002 m. spalio 22 d. EŽTT sprendimas *Taylor-Sabori prieš Jungtinę Karalystę*, Nr. 47114/99.

2010 m. rugsėjo 2 d. EŽTT sprendimas *Uzun prieš Vokietiją*, Nr. 35623/05.
2005 m. gegužės 31 d. EŽTT sprendimas *Vetter prieš Prancūziją*, Nr. 59842/00.

Stebėjimas vaizdo kameromis

2010 m. spalio 5 d. EŽTT sprendimas *Köpke prieš Vokietiją*, Nr. 420/07.
2003 m. sausio 28 d. EŽTT sprendimas *Peck prieš Jungtinę Karalystę*, Nr. 44647/98.

Balso ėminiai

2001 m. rugsėjo 25 d. EŽTT sprendimas *P. G. ir J. H. prieš Jungtinę Karalystę*, Nr. 44787/98.
2005 m. gruodžio 20 d. EŽTT sprendimas *Wisse prieš Prancūziją*, Nr. 71611/01.

Europos Sąjungos Teisingumo Teismo atrinkta praktika

Su Duomenų apsaugos direktyva susijusi jurisprudencija

2008 m. gruodžio 16 d. ESTT sprendimas *Tietosuojavaltuutettu prieš Satakunnan Markkinapörssi Oy ir Satamedia Oy*, C-73/07.
(„Žurnalistikos veiklos“ sąvoka pagal Duomenų apsaugos direktyvos 9 straipsnį.)

2010 m. lapkričio 9 d. ESTT sprendimas *Volker ir Markus Schecke GbR ir Hartmut Eifert prieš Land Hessen*, sujungtos bylos C-92/09 ir C-93/09.
(Teisinės pareigos skelbti duomenis apie tam tikrų ES žemės ūkio fondų pagalbos gavėjus proporcingumas.)

2003 m. lapkričio 6 d. ESTT sprendimas *Bodil Lindqvist*, C-101/01.
(Privataus asmens internete skelbiamų duomenų apie kitų asmenų privatų gyvenimą teisėtumas.)

2012 m. kovo 9 d. *Audiencia Nacional* (Ispanija) pateiktas prašymas priimti prejudicinį sprendimą byloje *Google Spain, S. L., Google Inc. prieš Agencia Española de Protección de Datos, Mario Costeja González*, C-131/12, išvada pateikta 2012 m. gegužės 25 d., byla nagrinėjama.
(Paieškos sistemų paslaugų teikėjų pareiga duomenų subjekto prašymu nerodyti asmens duomenų paieškos sistemos pateiktuose rezultatuose.)

2013 m. gegužės 30 d. ESTT sprendimas *Europos Komisija prieš Švedijos Karalystę*, C-270/11.
(Bauda, skirta už neįgyvendintą direktyvą.)

2008 m. sausio 29 d. ESTT sprendimas *Productores de Música de España (Promusicae) prieš Telefónica de España SAU*, C-275/06.
(Interneto paslaugų teikėjų pareiga atskleisti „KaZaA" failų keitimosi programų naudotojų tapatybę intelektinės nuosavybės apsaugos asociacijai.)

2014 m. balandžio 8 d., *Europos Komisija prieš Vengriją*, C-288/12.
(Nacionalinio duomenų apsaugos pareigūno tarnybos panaikinimo teisėtumas.)

Generalinio advokato išvada, pateikta 2013 m. birželio 13 d. byloje *Michael Schwarz prieš Stadt Bochum*, C-291/12.
(Reglamentu (EB) Nr. 2252/2004, kuriame nustatyta, kad pasuose turi būti saugomi pirštų atspaudai, padarytas ES pirminės teisės pažeidimas.)

2014 m. balandžio 8 d., *Digital Rights Ireland ir Seitling bei kiti*, Sujungtos bylos C-293/12 ir C-594/12.
(ES pirminę teisę pažeidžiančios Duomenų apsaugos direktyvos nuostatos.)

2012 m. vasario 16 d. ESTT sprendimas *SABAM prieš Netlog N. V.*, C-360/10.
(Socialinių tinklų paslaugų teikėjų pareiga užkirsti kelią tinklo naudotojams neteisėtai naudoti muzikos ir audiovizualinius kūrinius.)

2003 m. gegužės 20 d. ESTT sprendimas *Rechnungshof prieš Österreichischer Rundfunk ir kt. ir Neukomm ir Lauermann prieš Österreichischer Rundfunk*, sujungtos bylos C-465/00, C-138/01 ir C-139/01.
(Teisinės pareigos skelbti asmens duomenis, susijusius su tam tikrų viešojo sektoriaus institucijų darbuotojų kategorijų darbo užmokesčiu.)

2011 m. lapkričio 24 d. ESTT sprendimas *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) ir Federación de Comercio Electrónico y Marketing Directo (FECEMD) prieš Administración del Estado*, sujungtos bylos C-468/10 ir C-469/10.
(Teisingas Duomenų apsaugos direktyvos 7 straipsnio f punkto („teisėti kitų asmenų interesai") įgyvendinimas nacionalinėje teisėje.)

2010 m. kovo 9 d. ESTT sprendimas *Europos Komisija prieš Vokietijos Federacinę Respubliką*, C-518/07.
(Nacionalinės priežiūros institucijos nepriklausomumas.)

2008 m. gruodžio 16 d. ESTT sprendimas *Huber prieš Bundesrepublik Deutschland*, C-524/06.
(Duomenų apie užsieniečius saugojimo statistikos registruose teisėtumas.)

2011 m. gegužės 5 d. ESTT sprendimas *Deutsche Telekom AG prieš Bundesrepublik Deutschland*, C-543/09.
(Būtinybė gauti naują sutikimą.)

2009 m. gegužės 7 d. ESTT sprendimas *College van burgemeester en wethouders van Rotterdam prieš M. E. E. Rijkeboer*, C-553/07.
(Duomenų subjekto teisė susipažinti su duomenimis.)

2012 m. spalio 16 d. ESTT sprendimas *Europos Komisija prieš Austrijos Respubliką*, C-614/10.
(Nacionalinės priežiūros institucijos nepriklausomumas.)

Su ES institucijų duomenų apsaugos reglamentu susijusi jurisprudencija

2010 m. birželio 29 d. ESTT sprendimas *Europos Komisija prieš The Bavarian Lager Co. Ltd.*, C-28/08 P.
(Galimybė susipažinti su dokumentais.)

2003 m. kovo 6 d. ESTT sprendimas *Interporc Im- und Export GmbH prieš Europos Bendrijų Komisiją*, C-41/00 P.
(Galimybė susipažinti su dokumentais.)

2010 m. birželio 15 d. Tarnautojų teismo sprendimas *Pachtitis prieš Komisiją ir EPSO*, F-35/08.
(Asmens duomenų naudojimas įsidarbinant ES institucijose.)

2011 m. liepos 5 d. Tarnautojų teismo sprendimas *V prieš Parlamentą*, F-46/09.
(Asmens duomenų naudojimas įsidarbinant ES institucijose.)

Bylų sąrašas

Europos Teisingumo Teismo praktika

Europos Žmogaus Teisių Teismo praktika

Nacionalinių teismų praktika

Europos Sąjungos pagrindinių teisių agentūra
Europos žmogaus teisių teismas – Europos Taryba

Europos duomenų apsaugos teisės vadovas

2014 — 202 p. — 14,8 × 21 cm

ISBN 978-92-871-9943-0 (Europos Taryba)
ISBN 978-92-9239-336-6 (FRA)
doi:10.2811/54643

Daugiau informacijos apie Europos Sąjungos pagrindinių teisių agentūrą (FRA) yra pasiekiama Internete. Ji prieinama FRA internetiniame puslapyje fra.europa.eu.

Daugiau informacijos apie Europos Tarybą rasite interneto svetainėje hub.coe.int.

Daugiau informacijos apie Europos žmogaus teisių teismo bylų praktiką yra prieinama Teismo internetiniame puslapyje: echr.coe.int. HUDOC paieškos portale yra prieinami teismų sprendimai anglų ir/ arba prancūzų kalbomis, vertimai į papildomas kalbas, informaciniai pranešimai apie mėnesio teismo bylas, pranešimuai spaudai ir kita informacija, susijusi su Teismo darbo praktika.

10.2811/54643
TK-01-13-772-LT-C

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

Atsižvelgiant į sparčią informacinių ir ryšių technologijų plėtrą, didėja poreikis griežtinti asmens duomenų apsaugą, kuri užtikrinama Europos Sąjungos (ES) ir Europos Tarybos (ET) priemonėmis. Pažangios technologinės priemonės naudojamos nepaisant sienų, pvz., stebėjimas, pranešimų perėmimas ir duomenų saugojimas, ir dėl šios priežasties kyla svarbūs uždaviniai, susiję su teise į duomenų apsaugą. Šio vadovo tikslas – supažindinti teisės specialistus, kurie nesispecializuoja domenų apsaugos srityje, su duomenų apsaugos teise. Jame apžvelgiamos ES ir ET taikytinos teisės sistemos. Vadove paaiškinami svarbiausi jurisprudencijos aspektai, apibendrinami Europos Žmogaus Teisių Teismo (EŽTT) ir Europos Sąjungos Teisingumo Teismo (ESTT) pagrindiniai sprendimai. Jeigu konkrečiu klausimu teismų praktikoje nieko nepasakyta, vadove pateikiami praktiniai pavyzdžiai, kuriuose aptariami hipotetiniai scenarijai. Iš esmės šiuo vadovu siekiama padėti užtikrinti, kad teisės į duomenų apsaugą būtų paisoma veiksmingai ir ryžtingai.

EUROPOS SĄJUNGOS PAGRINDINIŲ TEISIŲ AGENTŪRA
Schwarzenbergplatz 11, 1040 Viena - Austrija
Tel. +43 (1) 580 30-60 – Faksas +43 (1) 580 30-693
fra.europa.eu – info@fra.europa.eu

EUROPOS TARYBA
EUROPOS ŽMOGAUS TEISIŲ TEISMAS
67075 Strasbourg Cedex – Prancūzija
Tel. +33 (0) 3 88 41 20 00 – Faksas +33 (0) 3 88 41 27 30
echr.coe.int – publishing@echr.coe.int

Leidinių biuras

ISBN 978-92-871-9943-0 (Europos Taryba)
ISBN 978-92-9239-336-6 (FRA)