II

*(Ne teisėkūros procedūra priimami aktai)*

# SPRENDIMAI

## KOMISIJOS ĮGYVENDINIMO REGLAMENTAS (ES) 2021/1772

**2021 m. birželio 28 d.**

**pagal Europos Parlamento ir Tarybos reglamentą (ES) 2016/679 dėl tinkamos asmens duomenų apsaugos Jungtinėje Karalystėje**

*(pranešta dokumentu Nr. C(2021) 4800)*

**(Tekstas svarbus EEE)**

EUROPOS KOMISIJA,

atsižvelgdama į Sutartį dėl Europos Sąjungos veikimo,

atsižvelgdama į 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentą (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (toliau – Bendrasis duomenų apsaugos reglamentas) ([1]), ypač į jo 45 straipsnio 3 dalį,

kadangi:

### 1. ĮVADAS

(1) Reglamente (ES) 2016/679 nustatytos asmens duomenų perdavimo iš Europos Sąjungoje įsikūrusių duomenų valdytojų arba duomenų tvarkytojų į trečiąsias valstybes ir tarptautinėms organizacijoms taisyklės, susijusios su tomis duomenų perdavimo operacijomis, kurioms taikomas minėtas reglamentas. Tarptautinio duomenų perdavimo taisyklės yra nustatytos to reglamento V skyriuje, t. y. 44–50 straipsniuose. Nors asmens duomenų srautas į Europos Sąjungai nepriklausančias valstybes ir iš jų yra labai svarbus siekiant plėsti tarptautinį bendradarbiavimą ir tarpvalstybinę prekybą, Europos Sąjungoje užtikrinamas asmens duomenų apsaugos lygis negali sumažėti perduodant duomenis į trečiąsias valstybes ([2]).

(2) Pagal Reglamento (ES) 2016/679 45 straipsnio 3 dalį Komisija, priimdama įgyvendinimo aktą, gali nuspręsti, kad trečioji valstybė, teritorija arba vienas ar daugiau nurodytų sektorių toje trečiojoje valstybėje, arba tarptautinė organizacija užtikrina tinkamo lygio apsaugą. Tokiu atveju asmens duomenys į trečiąją valstybę gali būti perduodami nereikalaujant jokio papildomo leidimo, kaip nustatyta to reglamento 45 straipsnio 1 dalyje ir 103 konstatuojamojoje dalyje.

(3) Kaip nurodyta Reglamento (ES) 2016/679 45 straipsnio 2 dalyje, priimant sprendimą dėl tinkamumo, turi būti remiamasi išsamia trečiosios valstybės teisinės sistemos analize, susijusia ir su duomenų importuotojams taikomomis taisyklėmis, ir su apribojimais bei apsaugos priemonėmis, taikomomis valdžios institucijoms gaunant prieigą prie asmens duomenų. Savo vertinime Komisija privalo nustatyti, ar atitinkama valstybė garantuoja tokio lygio apsaugą, kuri yra „iš esmės lygiavertė“ Europos Sąjungoje užtikrinamai apsaugai (Reglamento (ES) 2016/679104 konstatuojamoji dalis). Standartai, kuriais remiantis vertinamas „esminis lygiavertiškumas“, yra nustatyti Europos Sąjungos teisės aktuose, visų pirma Reglamente (ES) 2016/679, taip pat Europos Sąjungos Teisingumo Teismo jurisprudencijoje ([3]). Šiuo atžvilgiu taip pat svarbią reikšmę turi Europos duomenų apsaugos valdybos (EDAV) tinkamumo pavyzdžiai ([4]).

([1]) OL L 119, 2016 5 4, p. 1.
([2]) Žr. Reglamento (ES) 2016/679101 konstatuojamąją dalį.
([3]) Žr. naujausią Sprendimą *Facebook Ireland ir Schrems*, C-311/18 (toliau – *Schrems II*) ECLI:EU:C:2020:559.
([4]) Europos duomenų apsaugos valdyba, Tinkamumo pavyzdžiai, WP 254, 1-oji peržiūrėta versija, galima rasti šiuo adresu: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.

(4) Kaip išaiškino Europos Sąjungos Teisingumo Teismas, šia nuostata nėra reikalaujama prieiti prie išvados, kad apsauga būtų identiško lygio ([5]). Visų pirma, priemonės, kurių gali imtis atitinkama trečioji valstybė, siekdama apsaugoti asmens duomenis, gali skirtis nuo Europos Sąjungoje taikomų priemonių, jeigu šios priemonės padeda veiksmingai užtikrinti praktinę tinkamo lygio apsaugą ([6]). Todėl tinkamumo standartu nereikalaujama papunkčiui atkartoti ES taisykles. Veikiau turi būti patikrinama, ar visoje užsienio sistemoje užtikrinamas reikiamas apsaugos lygis – teisių į duomenų apsaugą esmė, veiksmingas jų įgyvendinimas, priežiūra ir įgyvendinimo užtikrinimas ([7]).

(5) Komisija atidžiai išanalizavo Jungtinės Karalystės teisę ir praktiką. Remdamasi (8)–(270) konstatuojamosiose dalyse išplėtotomis išvadomis, Komisija daro išvadą, kad Jungtinė Karalystė užtikrina tinkamą asmens duomenų, pagal Reglamentą (ES) 2016/679 perduotų iš Europos Sąjungos į Jungtinę Karalystę, apsaugos lygį.

(6) Ši išvada nesusijusi su asmens duomenimis, perduotais Jungtinės Karalystės imigracijos kontrolės tikslais arba kitaip patenkančiais į tam tikrų duomenų subjektų teisių išimties taikymo sritį siekiant išlaikyti veiksmingą imigracijos kontrolę (imigracijos išimtis) pagal Jungtinės Karalystės duomenų apsaugos akto 2 priedo 4 straipsnio 1 dalį. Po 2021 m. gegužės 26 d. Anglijos ir Velso apeliacinio teismo sprendimo Jungtinės Karalystės teisėje nebuvo sureguliuotas imigracijos išimties galiojimas ir aiškinimas. Nors apeliacinis teismas pripažino, kad duomenų subjektų teisės iš esmės gali būti ribojamos imigracijos kontrolės tikslais, nes tai „svarbus viešojo intereso aspektas“, jis nustatė, kad dabartinė imigracijos išimtis yra nesuderinama su Jungtinės Karalystės teise, nes teisės akte nėra konkrečių nuostatų, kuriomis būtų nustatytos Jungtinės Karalystės Bendrojo duomenų apsaugos reglamento (JK BDAR) 23 straipsnio 2 dalyje išvardytos apsaugos priemonės ([8]). Tokiomis aplinkybėmis asmens duomenų perdavimas iš Sąjungos į Jungtinę Karalystę, jei jam gali būti pritaikyta imigracijos išimtis, turėtų nebūti įtrauktas į šio sprendimo taikymo sritį ([9]). Kai tik nesuderinamumas su Jungtinės Karalystės teise bus pašalintas, reikėtų iš naujo įvertinti imigracijos išimtį ir tai, ar reikia išlaikyti šio sprendimo taikymo srities apribojimą.

(7) Šis sprendimas neturėtų daryti poveikio tiesioginiam Reglamento (ES) 2016/679 taikymui Jungtinėje Karalystėje įsisteigusioms organizacijoms, jeigu įvykdomos to reglamento 3 straipsnyje nustatytos jo teritorinės taikymo srities sąlygos.

## 2. **ASMENS DUOMENŲ TVARKYMUI TAIKOMOS TAISYKLĖS**

### 2.1. **Konstitucinė sistema**

(8) Jungtinė Karalystė yra parlamentinė demokratija, kurios konstitucinis suverenas yra valstybės vadovas. Joje veikia suverenus parlamentas, kuris yra viršiausias tarp visų vyriausybės institucijų, įstatymų vykdomoji valdžia, kuri renkama iš parlamento narių ir yra jam atskaitinga, ir nepriklausoma teisminė valdžia. Įstatymų vykdomosios valdžios įgaliojimai kildinami iš to, kad ji pelnė išrinktų Bendruomenių Rūmų pasitikėjimą, ir ji yra atskaitinga abiem parlamento rūmams, kurie privalo prižiūrėti vyriausybės veiklą ir diskutuoti dėl įstatymų bei juos priimti.

([5]) Sprendimas *Schrems* (*Schrems I*), C-362/14, ECLI:EU:C:2015:650, 73 punktas.

([6]) *Schrems II*, 74 punktas.

([7]) Žr. 2017 m. sausio 10 d. Komisijos komunikato Europos Parlamentui ir Tarybai „Keitimasis duomenimis ir jų apsauga globalizuotame pasaulyje“, COM(2017) 7, 3.1 skirsnį, p. 6–7, skelbiamas adresu: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0007&from=EN.

([8]) Apeliacinis teismas (Civilinių bylų skyrius), *Open Rights Group v Secretary of State for the Home Department and Secretary of State for Digital, Culture, Media and Sport*, [2021] EWCA Civ 800, 53–56 punktai. Apeliacinis teismas panaikino Aukštojo teisingumo teismo sprendimą, kuriuo išimtis prieš tai buvo įvertinta pagal Reglamentą (ES) 2016/679 (visų pirma jo 23 straipsnį) ir Europos Sąjungos pagrindinių teisių chartiją – juo išimtis buvo pripažinta teisėta (*Open Rights Group & Anor, R (On the Application Of) prieš Secretary of State for the Home Department & Anor* [2019] EWHC 2562).

([9]) Jei taikytinos sąlygos tenkinamos, Jungtinėje Karalystėje imigracijos kontrolės tikslais duomenys gali būti perduodami taikant Reglamento (ES) 2016/679 46–49 straipsniuose numatytus perdavimo mechanizmus.

(9) Jungtinės Karalystės Parlamentas atsakomybę priimti teisės aktus Škotijos, Velso ir Šiaurės Airijos vidaus klausimais perdavė Škotijos Parlamentui, Velso Parlamentui (*Senedd Cymru*) ir Šiaurės Airijos Asamblėjai, ir šios atsakomybės Jungtinės Karalystės Parlamentas sau nepasiliko. Nors duomenų apsauga yra išimtinis klausimas, t. y. tas pats teisės aktas taikomas visoje šalyje, kitos politikos sritys, susijusios su šiuo sprendimu, yra deleguotos. Pavyzdžiui, Škotijos ir Šiaurės Airijos baudžiamosios teisėsaugos sistemų, įskaitant policijos veiklą, klausimai yra perduoti atitinkamai Škotijos Parlamentui ir Šiaurės Airijos Asamblėjai. Jungtinė Karalystė neturi kodifikuotos konstitucijos, kuri būtų įtvirtinta konstituciniame dokumente. Konstituciniai principai vystėsi ilgą laiką, yra kildinami iš teismų praktikos, ypač papročių. Teismai pripažino konstitucinę tam tikrų statutų, pvz., *Magna Carta*, 1689 m. Teisių bilio ir 1998 m. Žmogaus teisių akto, svarbą. Pagrindinės asmenų teisės, kurios yra sudedamoji konstitucijos dalis, išplėtotos bendrojoje teisėje, minėtuose statutuose ir tarptautinėse sutartyse, visų pirma Europos žmogaus teisių konvencijoje, kurią Jungtinė Karalystė ratifikavo 1951 m. 1987 m. Jungtinė Karalystė taip pat ratifikavo Tarybos konvenciją dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (108-oji konvencija) ([10]).

(10) 1998 m. Žmogaus teisių aktu Europos žmogaus teisių konvencijoje nustatytos teisės perkeltos į Jungtinės Karalystės teisę. Žmogaus teisių aktu bet kuriam asmeniui suteikiamos Europos žmogaus teisių konvencijos 2–12 ir 14 straipsniuose, jos Pirmojo protokolo 1, 2 ir 3 straipsniuose ir jos Tryliktojo protokolo 1 straipsnyje (skaitant juos kartu su tos Konvencijos 16, 17 ir 18 straipsniais) nustatytos pagrindinės teisės ir laisvės. Šioms teisėms ir laisvėms taip pat priklauso teisė į privatų ir šeimos gyvenimą (ir teisė į duomenų apsaugą, kaip tos teisės sudedamoji dalis), taip pat teisė į teisingą bylos nagrinėjimą ([11]). Visų pirma pagal tos konvencijos 8 straipsnį valdžios institucija teisę į privatumą pagal įstatymą gali apriboti, kai tai būtina demokratinėje visuomenėje atsižvelgiant į valstybės saugumo, visuomenės apsaugos ar šalies ekonominės gerovės interesus, siekiant užkirsti kelią viešosios tvarkos pažeidimams ar nusikaltimams, taip pat apsaugoti žmonių sveikatą ar moralę arba kitų asmenų teises ir laisves.

(11) Pagal 1998 m. Žmogaus teisių aktą bet koks valdžios institucijų veiksmas turi derėti su Konvencijoje įtvirtinta teise ([12]). Be to, pirminiai teisės aktai ir poįstatyminiai teisės aktai turi būti skaitomi ir jie turi būti įgyvendinami su Konvencijoje nustatytomis teisėmis suderinamu būdu ([13]).

### 2.2. **Jungtinės Karalystės duomenų apsaugos sistema**

(12) 2020 m. sausio 31 d. Jungtinė Karalystė išstojo iš Europos Sąjungos. Pagal Susitarimą dėl Jungtinės Didžiosios Britanijos ir Šiaurės Airijos Karalystės išstojimo iš Europos Sąjungos ir Europos atominės energijos bendrijos ([14]), Sąjungos teisė toliau taikoma Jungtinei Karalystei pereinamuoju laikotarpiu iki 2020 m. gruodžio 31 d. Iki išstojimo ir pereinamuoju laikotarpiu asmens duomenų apsaugos teisės aktų sistemą Jungtinėje Karalystėje sudarė atitinkami ES teisės aktai (visų pirma Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 ir Direktyva (ES) 2016/680 ([15])) ir nacionalinės teisės aktai, visų pirma 2018 m. Duomenų apsaugos aktas (toliau – 2018 m. DAA) ([16]), kuriame Reglamente (ES) 2016/679 leistinais atvejais nustatytos nacionalinės taisyklės, kuriose nurodytos konkrečios Reglamento (ES) 2016/679 taikymo ir jo ribojimo taisyklės ir kuriomis į nacionalinę teisę buvo perkelta Direktyva (ES) 2016/680.

([10]) 108-osios konvencijos principai Jungtinės Karalystės teisėje iš pradžių buvo įgyvendinti priėmus 1984 m. Duomenų apsaugos aktą, kurį pakeitė 1998 m. DAA, o paskui – 2018 m. DAA (skaitomas kartu su Jungtinės Karalystės BDAR). Jungtinė Karalystė 2018 m. taip pat pasirašė Protokolą, kuriuo iš dalies keičiama Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (dar vadinama 108+ konvencija), ir dabar atlieka darbą, reikalingą jai ratifikuoti.

([11]) EŽTK 6 ir 8 straipsniai (taip pat žr. 1998 m. Žmogaus teisių akto 1 priedą).

([12]) 1998 m. Žmogaus teisių akto 6 straipsnis.

([13]) 1998 m. Žmogaus teisių akto 3 straipsnis.

([14]) Susitarimas dėl Jungtinės Didžiosios Britanijos ir Šiaurės Airijos Karalystės išstojimo iš Europos Sąjungos ir Europos atominės energijos bendrijos 2019/C 384 I/01, XT/21054/2019/INIT, (OL C 384I, 2019 11 12, p. 1), galima rasti šiuo adresu: https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:12019W/TXT(02)&from=LT.

([15]) 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, ir kuriuo panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR (OL L 119, 2016 5 4, p. 89), galima rasti šiuo adresu: https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32016L0680&from=LT.

([16]) 2018 m. Duomenų apsaugos aktas, galima rasti šiuo adresu: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.

(13) Siekdama pasirengti išstojimui iš ES, Jungtinės Karalystės vyriausybė priėmė 2018 m. (išstojimo iš) Europos Sąjungos aktą ([17]), kuriuo į Jungtinės Karalystės teisę tiesiogiai perkeliami taikytini Sąjungos teisės aktai ([18]). Ši vadinamoji palikta galioti ES teisė apima visą Reglamentą (ES) 2016/679 (įskaitant jo konstatuojamąsias dalis) ([19]). Pagal tą aktą nepakeistą paliktą galioti ES teisę Jungtinės Karalystės teismai privalo aiškinti paisydami atitinkamos Europos Teisingumo Teismo jurisprudencijos ir bendrųjų Sąjungos teisės principų, nes jie galiojo prieš pat pereinamojo laikotarpio pabaigą (atitinkamai vadinama palikta galioti ES teise ir paliktais galioti bendraisiais ES teisės principais) ([20]).

(14) Pagal 2018 m. (išstojimo iš) Europos Sąjungos aktą Jungtinės Karalystės ministrai turi įgaliojimus įstatymų nustatytomis priemonėmis priimti antrinės teisės aktus, kad, atsižvelgdami į Jungtinės Karalystės išstojimo iš Europos Sąjungos pasekmes, atliktų būtinus paliktos galioti Europos Sąjungos teisės pakeitimus. Šiais įgaliojimais naudojamasi remiantis 2019 m. Duomenų apsaugos, privatumo ir elektroninių ryšių (su pakeitimais) (išstojimo iš ES) taisyklėmis (toliau – DAPER taisyklės) ([21]). Tomis taisyklėmis iš dalies keičiamas į Jungtinės Karalystės teisę pagal 2018 m. (išstojimo iš) Europos Sąjungos aktą, 2018 m. DAA ir kitus duomenų apsaugos teisės aktus perkeltas Reglamentas (ES) 2016/679, siekiant užtikrinti jo atitiktį vidaus aplinkybėms ([22]).

(15) Todėl asmens duomenų apsaugos teisinę sistemą Jungtinėje Karalystėje pasibaigus pereinamajam laikotarpiui sudaro:

— Jungtinės Karalystės BDAR, įtrauktas į 2018 m. (išstojimo iš) Europos Sąjungos aktą, iš dalies pakeistas DAPER taisyklėmis ([23]), ir

— 2018 m. DAA ([24]), iš dalies pakeistas DAPER taisyklėmis.

(16) Kadangi Jungtinės Karalystės BDAR yra grindžiamas ES teisės aktais, Jungtinės Karalystės duomenų apsaugos taisyklės daugeliu aspektų beveik sutampa su Europos Sąjungoje taikomomis atitinkamomis taisyklėmis.

(17) Be valstybės sekretoriaus įgaliojimų, kurie jam suteikti pagal 2018 m. (išstojimo iš) Europos Sąjungos aktą, keliose 2018 m. DAA nuostatose valstybės sekretoriui suteikti įgaliojimai priimti antrinės teisės aktus, kuriais iš dalies keičiamos tam tikros akto nuostatos arba nustatomos papildomos taisyklės ([25]). Valstybės sekretorius iki šiol

([17]) 2018 m. (išstojimo iš) Europos Sąjungos aktas, skelbiamas šiuo adresu: https://www.legislation.gov.uk/ukpga/2018/16/contents.

([18]) 2018 m. (išstojimo iš) Europos Sąjungos aktu siekiama užtikrinti, kad visi tiesioginiai Sąjungos teisės aktai, kurie buvo perkelti į Jungtinės Karalystės teisę baigiantis pereinamajam laikotarpiui, būtų įtraukti į Jungtinės Karalystės teisę, nes jie ES galiojo prieš pat pereinamojo laikotarpio pabaigą, žr. 2018 m. (išstojimo iš) Europos Sąjungos akto 3 straipsnį.

([19]) 2018 m. (išstojimo iš) Europos Sąjungos akto aiškinamosiose pastabose nurodyta, kad: „Jeigu pagal šį straipsnį teisės aktas pakeičiamas, vidaus teisės akto sudedamąja dalimi bus paties teisės akto tekstas. Tai reiškia visą bet kurio ES teisės akto (įskaitant jo konstatuojamąsias dalis) tekstą.“ (2018 m. (išstojimo iš) Europos Sąjungos akto aiškinamųjų pastabų 83 dalis, galima rasti šiuo adresu: https://www.legislation.gov.uk/ukpga/2018/16/pdfs/ukpgaen_20180016_en.pdf). Remiantis Jungtinės Karalystės institucijų pateikta informacija, kadangi konstatuojamosios dalys neturi privalomų teisės taisyklių statuso, jų nebuvo būtina pakeisti taip pat, kaip iš dalies DAPER taisyklėmis buvo pakeisti Reglamento (ES) 2016/679 straipsniai.

([20]) 2018 m. (išstojimo iš) Europos Sąjungos akto 6 straipsnis.

([21]) 2019 m. Duomenų apsaugos, privatumo ir elektroninių ryšių (su pakeitimais) (išstojimo iš ES) taisyklės, galima rasti šiuo adresu: https://www.legislation.gov.uk/uksi/2019/419/contents/made, iš dalies pakeistos 2020 m. DAPER taisyklėmis, galima rasti šiuo adresu: https://www.legislation.gov.uk/ukdsi/2020/9780348213522.

([22]) Šie Jungtinės Karalystės BDAR ir 2018 m. DAA pakeitimai iš esmės yra techninio pobūdžio, pvz., išbraukiamos nuorodos į sąvoką „valstybės narės“ arba patikslinama terminija, pvz., nuorodos į Reglamentą (ES) 2016/679 pakeičiamos nuorodomis į Jungtinės Karalystės BDAR. Kai kuriomis aplinkybėmis pakeitimus buvo būtina atlikti, kad Jungtinės Karalystės BDAR atitiktų išimtinai vidaus pobūdžio nuostatas, pvz., susijusias su tuo, „kas“ priima „tinkamumo taisykles“, taikomas Jungtinės Karalystės duomenų apsaugos teisės aktų sistemoje (žr. 2018 m. DAA 17A straipsnį), t. y. valstybės sekretorius vietoje Europos Komisijos.

([23]) Bendrojo duomenų apsaugos reglamento Keelingo priedas, skelbiamas šiuo adresu: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/946117/20201102_-_GDPR_-__MASTER__Keeling_Schedule__with_changes_highlighted__V3.pdf.

([24]) 2018 m. Duomenų apsaugos akto Keelingo priedas, skelbiamas šiuo adresu: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/946100/20201102_-_DPA_-__MASTER__Keeling_Schedule__with_changes_highlighted__V3.pdf.

([25]) Tokie įgaliojimai numatyti, pvz., 2018 m. DAA 16 straipsnyje (įgaliojimai konkrečiomis, siaurai apibūdintomis aplinkybėmis nustatyti papildomas konkrečių Jungtinės Karalystės BDAR nuostatų išimtis), 17A straipsnyje (įgaliojimai priimti tinkamumo taisykles), 212 ir 213 straipsniuose (įgaliojimai pradėti rengti teisės aktą ir numatyti pereinamojo laikotarpio nuostatą) ir 211 straipsnyje (įgaliojimai atlikti nežymius vėlesnius pakeitimus).

pasinaudojo tik 2018 m. DAA 137 straipsniu suteiktais įgaliojimais priimti 2019 m. Duomenų apsaugos (mokesčiai ir informacija) (iš dalies pakeistas) taisykles, kuriose išdėstytos aplinkybės, kuriomis duomenų valdytojai privalo mokėti metinį mokestį nepriklausomai Jungtinės Karalystės duomenų apsaugos institucijai, t. y. informacijos komisarui.

(18) Galiausiai informacijos komisaro priimtuose praktikos kodeksuose ir kitose gairėse pateikiamos tolesnės rekomendacijos dėl Jungtinės Karalystės duomenų apsaugos teisės aktų. Nors šios rekomendacijos teisiškai neprivalomos, jos turi įtakos aiškinant nuostatas ir jose aptariama, kaip komisaras praktiškai taiko duomenų apsaugos teisės aktus ir užtikrina jų vykdymą. Visų pirma 2018 m. DAA 121–125 straipsniuose reikalaujama, kad komisaras parengtų dalijimosi duomenimis, tiesioginės rinkodaros, prie amžiaus pritaikyto dizaino ir duomenų apsaugos bei žurnalistikos praktikos kodeksus.

(19) Todėl Jungtinės Karalystės teisės sistema, kuri taikoma pagal šį sprendimą perduotiems duomenims, savo struktūra ir pagrindinėmis sudedamosiomis dalimis yra labai panaši į Europos Sąjungoje taikomą teisinę sistemą. Taip pat pažymėtina, kad šią teisinę sistemą sudaro ne tik pagal ES teisę suformuotos vidaus teisės normos, bet ir tarptautinėje teisėje nustatyti įpareigojimai, kurių Jungtinė Karalystė laikosi, visų pirma, pagal EŽTK ir 108-ąją konvenciją bei paklusdama Europos Žmogaus Teisių Teismo jurisdikcijai. Todėl šie įpareigojimai, kylantys iš teisiškai privalomų tarptautinių dokumentų, visų pirma susijusių su asmens duomenų apsauga, yra ypač svarbus šiame sprendime vertinamos teisinės sistemos aspektas.

### 2.3. **Materialinė ir teritorinė taikymo sritis**

(20) Panašiai kaip ir Reglamentas (ES) 2016/679, Jungtinės Karalystės BDAR taikomas visiškai arba iš dalies automatizuotomis priemonėmis arba kitaip tvarkomiems asmens duomenims, jeigu asmens duomenys yra duomenų rinkinio sudedamoji dalis ([26]). Jungtinės Karalystės BDAR vartojamų sąvokų „asmens duomenys“, „duomenų subjektas“ ir „duomenų tvarkymas“ apibrėžtys yra tapačios Reglamente (ES) 2016/679 pateiktoms analogiškų sąvokų apibrėžtims ([27]). Be to, Jungtinės Karalystės BDAR taikomas rankiniam nestruktūrizuotų asmens duomenų tvarkymui ([28]), kai šiuos duomenis laiko tam tikros Jungtinės Karalystės valdžios institucijos ([29]), nors Jungtinės Karalystės BDAR principai ir teisės, kurie nėra susiję su tokiais asmens duomenimis, netaikomi pagal 2018 m. DAA 24 ir 25 straipsnius. Panašiai, kaip numatyta Reglamente (ES) 2016/679, Jungtinės Karalystės BDAR netaikomas tais atvejais, kai asmens duomenis pavienis asmuo tvarko vykdydamas išimtinai asmeninę arba namų ūkio veiklą ([30]).

(21) Jungtinės Karalystės BDAR taip pat taikomas duomenų tvarkymui vykdant bet kokią veiklą, kuriai prieš pat pereinamojo laikotarpio pabaigą nebuvo taikoma Europos Sąjungos teisė (pvz., nacionalinis saugumas) ([31]), arba jai buvo taikomas Europos Sąjungos sutarties 5 antraštinės dalies 2 skyrius (Veikla bendros užsienio ir saugumo politikos srityje) ([32]). Kaip ir Europos Sąjungos sistemoje, Jungtinės Karalystės BDAR netaikomas asmens duomenų tvarkymui, kai tai daro kompetentinga institucija baudžiamųjų veikų prevencijos, tyrimo, nustatymo ar patraukimo

([26]) Jungtinės Karalystės BDAR 2 straipsnio 1 ir 5 dalys.

([27]) Jungtinės Karalystės BDAR 4 straipsnio 1 ir 2 dalys.

([28]) Rankinis nestruktūrizuotas asmens duomenų tvarkymas 2 straipsnio 5 dalies b punkte apibrėžiamas kaip asmens duomenų tvarkymas, kuris nėra automatizuotas arba struktūrizuotas asmens duomenų tvarkymas.

([29]) Jungtinės Karalystės BDAR 2 straipsnio 1A dalyje numatyta, kad Reglamentas taip pat taikomas rankiniam nestruktūrizuotam asmens duomenų tvarkymui, kai tokius duomenis turi ILA valdžios institucija. Nuoroda į ILA valdžios institucijas reiškia nuorodą į bet kurias 2000 m. Informacijos laisvės akte apibrėžtas institucijas arba bet kurias Škotijos valdžios institucijas, kaip apibrėžta 2002 m. Škotijos informacijos laisvės akte (asp 13). 2018 m. DAA 21 straipsnio 5 dalis.

([30]) Jungtinės Karalystės BDAR 2 straipsnio 2 dalies a punktas.

([31]) Nacionalinio saugumo veiklai Jungtinės Karalystės BDAR taikomas tik tiek, kiek jos teisėsaugos tikslais nevykdo kompetentinga institucija (tokiu atveju taikoma 2018 m. DAA 3 dalis) arba jos nevykdo žvalgybos tarnyba arba tai nėra daroma jos vardu, nes tokiu atveju žvalgybos tarnybai taikomas ne Jungtinės Karalystės BDAR, bet 2018 m. DAA 4 dalis, kaip numatyta Jungtinės Karalystės BDAR 2 straipsnio 2 dalies c punkte. Pavyzdžiui, policijos pajėgos gali atlikti darbuotojo saugumo patikrinimus, siekdamos užtikrinti jo patikimumą tais atvejais, kai toks darbuotojas susipažįsta su nacionalinio saugumo medžiaga. Nepaisant to, kad policija yra kompetentinga institucija teisėsaugos tikslais, atitinkamas duomenų tvarkymas vykdomas ne teisėsaugos tikslais ir tokiu atveju bus taikomas Jungtinės Karalystės BDAR. Žr. Diskusijoms dėl duomenų apsaugos tinkamumo skirto Jungtinės Karalystės aiškinamojo dokumento H skirsnį „Nacionalinio saugumo duomenų apsaugos ir tyrimo įgaliojimų sistema“, p. 8, galima rasti šiuo adresu: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872239/H_-_National_Security.pdf.

([32]) Jungtinės Karalystės BDAR 2 straipsnio 1 dalies a ir b punktai.

baudžiamojon atsakomybėn už jas arba bausmių vykdymo tikslais, įskaitant apsaugą nuo grėsmių visuomenės saugumui ir tokių grėsmių prevenciją (tai vadinama teisėsaugos tikslais), – tokiu atveju duomenų tvarkymas reglamentuojamas pagal 2018 m. DAA 3 dalį arba pagal Direktyvą (ES) 2016/680 Europos Sąjungos teisėje, – arba asmens duomenų tvarkymui, kai tai daro žvalgybos tarnybos (Saugumo tarnyba, Slaptoji žvalgybos tarnyba ir Vyriausybės ryšių būstinė), – šiuo atveju taikoma 2018 m. DAA 4 dalis ([33]).

(22) Jungtinės Karalystės BDAR teritorinė taikymo sritis aprašyta jo 3 straipsnyje ([34]): ji apima asmens duomenų tvarkymą (nepaisant to, kur jis vyksta), duomenų valdytojo arba duomenų tvarkytojo buveinei vykdant veiklą Jungtinėje Karalystėje, taip pat Jungtinėje Karalystėje esančių duomenų subjektų asmens duomenų tvarkymą, kai duomenų tvarkymo veikla yra susijusi su prekių arba paslaugų siūlymu tokiems duomenų subjektams arba jų elgesio stebėsena ([35]). Tai atitinka Reglamento (ES) 2016/679 3 straipsnyje nustatytą požiūrį.

### 2.4. **Asmens duomenų apibrėžtys ir duomenų valdytojo ir duomenų tvarkytojo sąvokos**

(23) Asmens duomenų, duomenų tvarkymo, duomenų valdytojo, duomenų tvarkytojo, taip pat pseudoniminimo sąvokų apibrėžtys, kurios nustatytos Reglamente (ES) 2016/679, be esminių pakeitimų išlaikytos Jungtinės Karalystės BDAR ([36]). Be to, Jungtinės Karalystės BDAR 9 straipsnio 1 dalyje specialių kategorijų duomenys apibrėžiami taip pat kaip ir Reglamente (ES) 2016/679 („atskleidžian[tys] rasinę ar etninę kilmę, politines pažiūras, religinius ar filosofinius įsitikinimus ar narystę profesinėse sąjungose, taip pat tvarkyti genetinius duomenis, biometrinius duomenis, siekiant konkrečiai nustatyti fizinio asmens tapatybę, sveikatos duomenis arba duomenis apie fizinio asmens lytinį gyvenimą ir lytinę orientaciją“). 2018 m. DAA 205 straipsnyje nustatytos sąvokų „biometriniai duomenys ([37])“, „sveikatos duomenys“ ([38]) ir „genetiniai duomenys“ ([39]) apibrėžtys.

### 2.5. **Apsaugos priemonės, teisės ir prievolės**

#### 2.5.1. *Duomenų tvarkymo teisėtumas ir sąžiningumas*

(24) Asmens duomenys turėtų būti tvarkomi teisėtai ir sąžiningai.

(25) Teisėtumo, sąžiningumo ir skaidrumo principai ir teisėto duomenų tvarkymo pagrindai Jungtinės Karalystės teisėje garantuojami pagal Jungtinės Karalystės BDAR 5 straipsnio 1 dalies a punktą ir 6 straipsnio 1 dalį, kurie yra tapatūs atitinkamoms Reglamento (ES) 2016/679 nuostatoms ([40]). 2018 m. DAA 8 straipsnis papildo 6 straipsnio 1 dalies e punktą jame numatant, kad asmens duomenų tvarkymas pagal Jungtinės Karalystės 6 straipsnio 1 dalies e punktą (būtinas užduočiai, susijusiai su viešuoju interesu, atlikti arba duomenų valdytojui vykdant savo oficialius

([33]) Jungtinės Karalystės BDAR 2 straipsnio 2 dalies b ir c punktai.

([34]) Ta pati teritorinio taikymo taisyklė galioja tvarkant asmens duomenis pagal 2018 m. DAA 2 dalį, kuri papildo Jungtinės Karalystės BDAR (207 straipsnio 1A dalį).

([35]) Tai visų pirma reiškia, kad 2018 m. DAA, taigi ir šis sprendimas, netaikomi Jungtinės Karalystės Karūnos priklausiniams (Džersiui, Gernsiui ir Meno salai) ir Jungtinės Karalystės užjūrio teritorijoms, pavyzdžiui, Folklendo saloms ir Gibraltaro teritorijai.

([36]) Jungtinės Karalystės BDAR 4 straipsnio 1, 2, 5, 7 ir 8 dalys.

([37]) Biometriniai duomenys – po specialaus techninio apdorojimo gauti asmens duomenys, susiję su fizinio asmens fizinėmis, fiziologinėmis arba elgesio savybėmis, pagal kurias galima konkrečiai nustatyti arba patvirtinti to fizinio asmens tapatybę, pvz., veido atvaizdai arba daktiloskopiniai duomenys.

([38]) Sveikatos duomenys – asmens duomenys, susiję su fizine ar psichine fizinio asmens sveikata, įskaitant duomenis apie sveikatos priežiūros paslaugų teikimą, atskleidžiantys informaciją apie to fizinio asmens sveikatos būklę.

([39]) Genetiniai duomenys – asmens duomenys, susiję su paveldėtomis ar įgytomis fizinio asmens genetinėmis savybėmis, suteikiančiomis unikalios informacijos apie to fizinio asmens fiziologiją ar sveikatą, ir kurie gauti visų pirma analizuojant biologinį atitinkamo fizinio asmens mėginį.

([40]) Pagal Jungtinės Karalystės BDAR 6 straipsnio 1 dalį duomenys yra tvarkomi teisėtai tik jeigu: a) duomenų subjektas davė sutikimą, kad jo asmens duomenys būtų tvarkomi vienu ar keliais konkrečiais tikslais; b) tvarkyti duomenis būtina siekiant įvykdyti sutartį, kurios šalis yra duomenų subjektas, arba siekiant imtis veiksmų duomenų subjekto prašymu prieš sudarant sutartį; c) tvarkyti duomenis būtina, kad būtų įvykdyta duomenų valdytojui taikoma teisinė prievolė; d) tvarkyti duomenis būtina siekiant apsaugoti gyvybinius duomenų subjekto ar kito fizinio asmens interesus; e) tvarkyti duomenis būtina siekiant atlikti užduotį, vykdomą viešojo intereso labui arba vykdant duomenų valdytojui pavestas viešosios valdžios funkcijas, arba f) tvarkyti duomenis būtina siekiant teisėtų duomenų valdytojo arba trečiosios valstybės interesų, išskyrus atvejus, kai tokie duomenų subjekto interesai arba pagrindinės teisės ir laisvės, dėl kurių būtina užtikrinti asmens duomenų apsaugą, yra už juos viršesni, ypač kai duomenų subjektas yra vaikas.

įgaliojimus) taip pat apima asmens duomenų tvarkymą, kai tai yra būtina teisingumui vykdyti, kurių nors parlamento rūmų funkcijai įvykdyti, asmeniui pagal priimtą įstatymą arba teisinės valstybės principą suteiktai funkcijai įvykdyti, Karalienės, Karalienės ministro arba vyriausybės departamento funkcijai įvykdyti, arba veiklai, kuria remiamas arba skatinamas demokratinis dalyvavimas, vykdyti.

(26) Dėl sutikimo (t. y. vieno iš teisėto duomenų tvarkymo pagrindų) pažymėtina, kad Jungtinės Karalystės BDAR taip pat išlaikytos nepakeistos Reglamento (ES) 2016/679 7 straipsnyje nustatytos sąlygos, t. y. duomenų valdytojas privalo sugebėti įrodyti, kad duomenų subjektas sutiko, rašytinis sutikimas turi būti pateiktas aiškia ir paprasta kalba, duomenų subjektas turi turėti teisę bet kuriuo metu atsisakyti savo sutikimo, o vertinant, ar sutikimas buvo duotas laisvai, reikėtų atsižvelgti į tai, kad sutarties įvykdymas priklauso nuo sutikimo tvarkyti asmens duomenis, kurie nėra būtini tai sutarčiai vykdyti. Be to, pagal Jungtinės Karalystės BDAR 8 straipsnį teikiant informacinės visuomenės paslaugas vaiko sutikimas yra teisėtas tik jeigu vaikas yra ne jaunesnis nei 13 metų. Tai atitinka Reglamento (ES) 2016/679 8 straipsnyje nustatytas amžiaus ribas.

2.5.2. *Specialių kategorijų asmens duomenų tvarkymas*

(27) Tais atvejais, kai tvarkomi „specialių kategorijų“ duomenys, turėtų būti taikomos konkrečios apsaugos priemonės.

(28) Jungtinės Karalystės BDAR ir 2018 m. DAA nustatytos konkrečios taisyklės dėl specialių kategorijų asmens duomenų tvarkymo, kurios Jungtinės Karalystės BDAR 9 straipsnio 1 dalyje apibrėžiamos taip pat kaip ir Reglamente (ES) 2016/679 (žr. (23) above konstatuojamąją dalį). Pagal Jungtinės Karalystės BDAR 9 straipsnį specialių kategorijų asmens duomenų tvarkymas iš esmės draudžiamas, išskyrus konkrečias taikomas išimtis.

(29) Šios išimtys (išvardytos Jungtinės Karalystės BDAR 9 straipsnio 2 ir 3 dalyse) iš esmės nesiskiria nuo Reglamento (ES) 2016/679 9 straipsnio 2 ir 3 dalyse nustatytų išimčių. Išskyrus atvejus, kai duomenų subjektas duoda aiškų sutikimą, kad jo asmens duomenys būtų tvarkomi, specialių kategorijų asmens duomenis tvarkyti leidžiama tik konkrečiomis ir ribotomis aplinkybėmis. Dažniausiai neskelbtinus duomenis turi būti būtina tvarkyti konkrečiu atitinkamoje nuostatoje nurodytu tikslu (žr. 9 straipsnio 2 dalies b, c, f, g, h, i ir j punktus).

(30) Be to, jeigu pagal Jungtinės Karalystės BDAR 9 straipsnio 2 dalyje nustatytą išimtį reikalaujama pagal įstatymą išduoto leidimo arba toje išimtyje pateikiama nuoroda į viešąjį interesą, 2018 m. DAA 10 straipsnyje kartu su 2018 m. DAA 1 priedu išsamiau apibūdinamos sąlygos, kurios turi būti įvykdytos norint remtis išimtimis. Pavyzdžiui, jeigu tvarkomi neskelbtini duomenys, siekiant apsaugoti „visuomenės sveikatą“ (Jungtinės Karalystės BDAR 9 straipsnio 2 dalies i punktas), pagal 1 priedo 1 dalies 3 straipsnio b punktą reikalaujama, kad, be būtinumo patikrinimo, tokius duomenis tvarkytų „sveikatos priežiūros specialistas arba jis už tai būtų atsakingas“ arba „kitas asmuo, kuriam taikoma konfidencialumo pareiga pagal priimtą įstatymą arba teisinės valstybės principą“, įskaitant nusistovėjusioje bendrojoje teisėje galiojančią konfidencialumo pareigą.

(31) Jeigu neskelbtini duomenys tvarkomi dėl esminio viešojo intereso (Jungtinės Karalystės BDAR 9 straipsnio 2 dalies g punktas, 2018 m. DAA 1 priedo 2 dalyje pateikiamas išsamus sąrašas tikslų, kurie gali būti laikomi esminiu viešuoju interesu, ir dėl kiekvieno iš šių tikslų nustatomos konkrečios papildomos sąlygos. Pavyzdžiui, rasinės ir etninės įvairovės tarp aukštesnio lygmens organizacijų vadovų skatinimas pripažįstamas esminiu viešuoju interesu. Neskelbtini duomenys šiuo konkrečiu tikslu tvarkomi laikantis išsamių reikalavimų, įskaitant tai, kad duomenys tvarkomi nustatant asmenis, kurie turi eiti vyresniųjų vadovų pareigas, juos tvarkyti būtina siekiant skatinti rasinę ir etninę įvairovę, ir mažai tikėtina, kad jie padarys didelę žalą arba sukels didelių nepatogumų duomenų subjektui.

(32) 2018 m. DAA 11 straipsnio 1 dalyje nustatytos sąlygos, kuriomis asmens duomenys turi būti tvarkomi atsižvelgiant į Jungtinės Karalystės BDAR 9 straipsnio 3 dalyje aprašytas aplinkybes, susijusias su profesine paslaptimi. Tai yra aplinkybės, kuriomis duomenis tvarko sveikatos priežiūros specialistas arba socialinis darbuotojas, arba kitas asmuo, kuris, atsižvelgiant į aplinkybes, privalo laikytis konfidencialumo pareigos pagal priimtą įstatymą arba teisinės valstybės principą, arba duomenys tvarkomi šių asmenų vardu.

(33) Be to, dauguma išimčių, išvardytų Jungtinės Karalystės BDAR 9 straipsnio 2 dalyje, gali būti taikomos tik nustačius tinkamas ir konkrečias apsaugos priemones. Priklausomai nuo duomenų tvarkymo pobūdžio ir duomenų subjektų teisėms ir laisvėms kylančio rizikos lygio, 2018 m. DAA 1 priede nustatytose duomenų tvarkymo sąlygose įtvirtintos skirtingos apsaugos priemonės. 1 priede paeiliui išvardijamos duomenų tvarkymo kiekvienu atveju sąlygos.

(34) Kai kuriais atvejais 2018 m. DAA reglamentuojama ir ribojama neskelbtinų duomenų, kuriuos galima tvarkyti remiantis konkrečiu teisiniu pagrindu, kurio privalu paisyti, rūšis. Pavyzdžiui, pagal 1 priedo 8 dalį neskelbtinus duomenis tvarkyti leidžiama siekiant skatinti vienodas galimybes arba elgesį. Ši duomenų tvarkymo sąlyga gali būti taikoma tik jeigu duomenys atspindi rasinę arba etninę kilmę, religinius arba filosofinius įsitikinimus, seksualinę orientaciją arba jeigu tai yra sveikatos duomenys.

(35) Kai kuriais atvejais pagal 2018 m. DAA apribojimai taikomi duomenų valdytojui, kuris gali naudotis duomenų tvarkymo sąlyga. Pavyzdžiui, 1 priedo 23 dalyje numatyta galimybė tvarkyti neskelbtinus duomenis, susijusius su išrinktų atstovų atsakymais visuomenei. Ši duomenų tvarkymo sąlyga gali būti taikoma tik jeigu duomenų valdytojas yra išrinktas atstovas arba veikia remdamasis jo įgaliojimais.

(36) Kai kuriais kitais atvejais pagal 2018 m. DAA apribojimai nustatomi toms duomenų kategorijoms, kurių tvarkymui turi būti taikoma tam tikra sąlyga. Pavyzdžiui, 1 priedo 21 dalyje reglamentuojamas neskelbtinų duomenų, susijusių su profesinėmis pensijų sistemomis, tvarkymas. Ši sąlyga gali būti taikoma tik jeigu atitinkamas duomenų subjektas yra sistemos dalyvio brolis (sesuo), tėvas (motina), senelis (senelė) arba prosenelis (prosenelė).

(37) Be to, jeigu duomenų valdytojas remiasi Jungtinės Karalystės BDAR 9 straipsnio 2 dalyje nustatytomis išimtimis, kurios išsamiau apibūdintos 2018 m. DAA 10 straipsnyje ir 2018 m. DAA 1 priede, jis dažniausiai privalo parengti „tinkamos politikos dokumentą“. Jame turi būti aprašytos duomenų valdytojo procedūros, kuriomis jis užtikrina atitiktį Jungtinės Karalystės BDAR 5 straipsnyje nustatytiems principams. Jis taip pat turi nustatyti duomenų saugojimo ir ištrynimo politiką ir nurodyti tikėtiną saugojimo laikotarpį. Duomenų valdytojai privalo, kai tinkama, peržiūrėti ir atnaujinti šį dokumentą. Duomenų valdytojas privalo laikyti politikos dokumentą šešis mėnesius po duomenų tvarkymo pabaigos ir privalo leisti su juo susipažinti informacijos komisarui, jei jis to prašo ([41]).

(38) Pagal 2018 m. DAA 1 priedo 41 straipsnį prie politikos dokumento visada turi būti pridedamas išsamus dokumentas apie duomenų tvarkymą. Šiame dokumente turi būti registruojama, kaip vykdomi politikos dokumente nustatyti įsipareigojimai, t. y. ar duomenys ištrinami ar saugomi pagal nustatytą politiką. Jeigu politika nebuvo vadovaujamasi, žurnale turi būti nurodomos to priežastys. Jame taip pat būtina aprašyti, kaip duomenų tvarkymas atitinka Jungtinės Karalystės BDAR 6 straipsnį (tvarkymo teisėtumas) ir 2018 m. DAA 1 priede nustatytą konkrečią sąlygą, kuria remiamasi.

(39) Galiausiai tiek Reglamente (ES) 2016/679, tiek Jungtinės Karalystės BDAR taip pat nustatytos bendrosios apsaugos priemonės, susijusios su tam tikromis specialių kategorijų duomenų tvarkymo operacijomis. Pagal Jungtinės Karalystės BDAR 35 straipsnį reikalaujama atlikti poveikio duomenų apsaugai vertinimą, jeigu dideliu mastu tvarkomi specialių kategorijų duomenys. Pagal Jungtinės Karalystės BDAR 37 straipsnį duomenų valdytojas arba duomenų tvarkytojas privalo paskirti duomenų apsaugos pareigūną, jeigu jo pagrindinė veikla yra susijusi su specialių kategorijų duomenų tvarkymu dideliu mastu.

(40) Dėl asmens duomenų, susijusių su apkaltinamaisiais nuosprendžiais ir nusikalstamomis veikomis, pažymėtina, kad Jungtinės Karalystės BDAR 10 straipsnis yra identiškas Reglamento (ES) 2016/679 10 straipsniui. Pagal jį asmens duomenis, susijusius su apkaltinamaisiais nuosprendžiais ir nusikalstamomis veikomis, leidžiama tvarkyti tik oficialiai institucijai kontroliuojant arba kai duomenis tvarkyti leidžiama pagal vidaus teisę, kurioje numatytos tinkamos duomenų subjektų teisių ir laisvių apsaugos priemonės.

(41) Jeigu duomenys, susiję su apkaltinamaisiais nuosprendžiais ir nusikalstamomis veikomis, tvarkomi oficialiai institucijai nevykdant kontrolės, 2018 m. DAA 10 straipsnio 5 dalyje numatyta, kad toks duomenų tvarkymas gali būti atliekamas tik konkrečiais tikslais / konkrečiomis aplinkybėmis, kaip nustatyta 2018 m. DAA 1 priedo 1, 2 ir 3 dalyse ir jeigu tokiam tvarkymui taikomi konkretūs reikalavimai, nustatyti dėl kiekvieno iš šių tikslų / aplinkybių. Pavyzdžiui, su apkaltinamaisiais nuosprendžiais susijusius duomenis gali tvarkyti ne pelno įstaigos, jeigu duomenis tvarko a) politinių, filosofinių, religinių ar profesinių sąjungų tikslų siekiantis fondas, asociacija ar kita pelno nesiekianti organizacija, vykdydami savo veiklą ir b) su sąlyga, kad taip tvarkomi tik i) tos organizacijos narių ar buvusių narių arba asmenų, kurie reguliariai palaiko ryšius su šia organizacija dėl jos siekiamų tikslų, duomenys ir ii) kad duomenys neperduodami už organizacijos ribų be duomenų subjektų sutikimo.

([41]) 2018 m. DAA 1 priedo 38–40 dalys.

(42) Be to, 2018 m. DAA 1 priedo 3 dalyje nustatytos papildomos aplinkybės, kuriomis galima naudoti su apkaltinamaisiais nuosprendžiais susijusius duomenis ir kurios atitinka neskelbtinų duomenų tvarkymo teisėtus pagrindus pagal Reglamento (ES) 2016/679 9 straipsnio 2 dalį ir Jungtinės Karalystės BDAR (pvz., duomenų subjekto sutikimas, gyvybiškai svarbūs asmens interesai, jeigu duomenų subjektas teisiškai arba fiziškai negali duoti sutikimo, jeigu duomenų subjektas jau aiškiai paskelbė duomenis viešai, jeigu duomenis tvarkyti būtina siekiant pareikšti, vykdyti arba apginti teisinius reikalavimus ir pan.).

2.5.3. *Tikslo apribojimo principas, tikslumas, duomenų kiekio mažinimas, saugojimo trukmės apribojimo principas ir duomenų saugumas*

(43) Asmens duomenys turėtų būti tvarkomi konkrečiu tikslu ir vėliau naudojami tik tuo atveju, jei tai nėra nesuderinama su jų tvarkymo tikslu.

(44) Šis principas nustatytas Reglamento (ES) 2016/679 5 straipsnio 1 dalies b punkte ir be pakeitimų paliktas galioti Jungtinės Karalystės BDAR 5 straipsnio 1 dalies b punkte. Tolesnio suderinamo duomenų tvarkymo sąlygos pagal Reglamento (ES) 2016/679 6 straipsnio 4 dalį, neatlikus jokių esminių pakeitimų, taip pat išlaikytos Jungtinės Karalystės BDAR 6 straipsnio 4 dalies a–e punktuose.

(45) Be to, duomenys turėtų būti tikslūs ir prireikus atnaujinami. Duomenys taip pat turi būti tinkami, susiję ir neperteklinai atsižvelgiant į tikslus, kuriais jie tvarkomi, ir iš esmės saugomi ne ilgiau nei tai būtina atsižvelgiant į tikslus, kuriais asmens duomenys tvarkomi.

(46) Šie duomenų kiekio mažinimo, tikslumo ir saugojimo trukmės apribojimo principai išdėstyti Reglamento (ES) 2016/679 5 straipsnio 1 dalies c–e punktuose ir be pakeitimų išlaikyti Jungtinės Karalystės BDAR 5 straipsnio 1 dalies c–e punktuose.

(47) Asmens duomenys taip pat turėtų būti tvarkomi taip, kad būtų užtikrintas jų saugumas, įskaitant apsaugą nuo neleistino ar neteisėto tvarkymo ir netyčinio praradimo, sunaikinimo ar sugadinimo. Todėl verslo subjektai turėtų imtis tinkamų techninių ir organizacinių priemonių, kad asmens duomenis apsaugotų nuo galimų grėsmių. Tokios priemonės turėtų būti įvertintos atsižvelgiant į techninių galimybių išsivystymo lygį ir susijusias sąnaudas.

(48) Duomenų saugumo reikalavimas Jungtinės Karalystės teisėje nustatytas atsižvelgiant į duomenų vientisumo ir konfidencialumo principą, kuris numatytas Jungtinės Karalystės BDAR 5 straipsnio 1 dalies f punkte ir Jungtinės Karalystės BDAR 32 straipsnyje dėl duomenų tvarkymo saugumo. Šios nuostatos yra tapačios atitinkamoms Reglamento (ES) 2016/679 nuostatoms. Be to, laikantis tų pačių sąlygų, kurios nustatytos Reglamento (ES) 2016/679 33 ir 34 straipsniuose, pagal Jungtinės Karalystės BDAR reikalaujama, kad apie asmens duomenų saugumo pažeidimą būtų pranešta priežiūros institucijai (Jungtinės Karalystės BDAR 33 straipsnis) ir kad pranešimas apie asmens duomenų saugumo pažeidimą taip pat būtų nusiųstas duomenų subjektui (Jungtinės Karalystės BDAR 34 straipsnis).

2.5.4. *Skaidrumas*

(49) Duomenų subjektai turėtų būti informuoti apie pagrindinius jų asmens duomenų tvarkymo aspektus.

(50) Tai užtikrinama pagal Jungtinės Karalystės BDAR 13 ir 14 straipsnius, kuriuose, be bendrojo skaidrumo principo, numatytos taisyklės dėl duomenų subjektams teikiamos informacijos ([42]). Jungtinės Karalystės BDAR nenustatyti jokie reikšmingi šių taisyklių pakeitimai, palyginti su atitinkamais Reglamento (ES) 2016/679 straipsniais. Vis dėlto, kitaip nei Reglamente (ES) 2016/679, šiuose straipsniuose nustatytiems skaidrumo reikalavimams taikomos kelios 2018 m. DAA nustatytos išimtys (žr. (55)–(72) konstatuojamąsias dalis).

([42]) 13 straipsnio 1 dalies f punkte ir 14 straipsnio 1 dalies f punkte nuorodos į Komisijos sprendimus dėl tinkamumo pakeistos nuorodomis į lygiavertę Jungtinės Karalystės priemonę, t. y. tinkamumo taisykles pagal 2018 m. DAA. Be to, 14 straipsnio 5 dalies c–d punktuose nuorodos į ES arba valstybės narės teisę pakeistos nuoroda į vidaus teisę (kaip tokios vidaus teisės, kuriai gali būti taikomas 14 straipsnio 5 dalies c punktas, pavyzdžius Jungtinė Karalystė nurodė 2013 m. Prekiautojų metalo laužu akto 7 straipsnį, kuriame pateikiamos taisyklės dėl metalo laužo licencijų registravimo, arba 2006 m. Įmonių akto 35 dalį, kurioje nustatytos įmonių registravimo taisyklės. Be to, vidaus teisės, kuriai gali būti taikomas 14 straipsnio 5 dalies d punktas, pavyzdys galėtų būti teisės aktas, kuriame nustatytos taisyklės dėl profesinės paslapties arba pareigos, kurios atsispindi darbo sutartyse, arba pagal bendrąją teisę suformuota konfidencialumo pareiga (pvz., sveikatos priežiūros specialistų, žmogiškųjų išteklių darbuotojų, socialinių darbuotojų ir pan. tvarkomi asmens duomenys).

2.5.5. *Asmens teisės*

(51) Duomenų subjektai turėtų turėti tam tikras teises, kurias būtų galima įgyvendinti duomenų valdytojo arba duomenų tvarkytojo atžvilgiu, visų pirma tai pasakytina apie teisę susipažinti su duomenimis, teisę nesutikti su duomenų tvarkymu ir teisę ištaisyti arba ištrinti duomenis. Be to, tokioms teisėms gali būti taikomi apribojimai, jeigu jie yra būtini ir proporcingi siekiant apsaugoti visuomenės saugumą arba siekiant kitų su bendruoju viešuoju interesu susijusių svarbių tikslų.

2.5.5.1. Esminės teisės

(52) Jungtinės Karalystės BDAR asmenims suteikiamos tokios pat įgyvendinamos teisės, kurios numatytos Reglamente (ES) 2016/679. Nuostatos, kuriose įtvirtintos asmenų teisės, Jungtinės Karalystės BDAR išlaikytos be jokių esminių pakeitimų.

(53) Tai yra duomenų subjekto teisė susipažinti su duomenimis (Jungtinės Karalystės BDAR 15 straipsnis), teisė reikalauti ištaisyti duomenis (Jungtinės Karalystės BDAR 16 straipsnis), teisė ištrinti duomenis (Jungtinės Karalystės BDAR 17 straipsnis), teisė apriboti duomenų tvarkymą (Jungtinės Karalystės BDAR 18 straipsnis), prievolė pranešti apie asmens duomenų ištaisymą ar ištrynimą arba duomenų tvarkymo apribojimą (Jungtinės Karalystės BDAR 19 straipsnis), teisė į duomenų perkeliamumą (Jungtinės Karalystės BDAR 20 straipsnis) ir teisė nesutikti (Jungtinės Karalystės BDAR 21 straipsnis) ([43]). Pastaroji teisė taip pat apima duomenų subjekto teisę nesutikti su asmens duomenų tvarkymu tiesioginės rinkodaros tikslais, kaip nustatyta Reglamento (ES) 2016/679 21 straipsnio 2 ir 3 dalyse. Be to, pagal 2018 m. DAA 122 straipsnį informacijos komisaras privalo parengti tiesioginės rinkodaros veiklos vykdymo pagal duomenų apsaugos teisės aktų (ir 2003 m. Privatumo ir elektroninių ryšių (EB direktyvos) taisykles) reikalavimus praktikos kodeksą ir kitas panašias gaires, kuriomis būtų skatinama geroji tiesioginės rinkodaros patirtis, kuri, komisaro manymu, yra tinkama. Informacijos komisaro biuras dabar rengia tiesioginės rinkodaros kodeksą ([44]).

(54) Duomenų subjekto teisė, kad jam nebūtų taikomas tik automatizuotu duomenų tvarkymu grindžiamas sprendimas, dėl kurio jam kyla teisinės pasekmės arba kuris jam panašiu būdu daro didelį poveikį, kaip nustatyta BDAR 22 straipsnyje, Jungtinės Karalystės BDAR taip pat palikta galioti be jokių esminių pakeitimų. Tačiau buvo įterpta nauja 3A dalis, kurioje nurodoma, kad 2018 m. DAA 14 straipsnyje išdėstytos duomenų subjektų teisių, laisvių ir teisėtų interesų, susijusių su duomenų tvarkymu pagal Jungtinės Karalystės BDAR 22 straipsnio 2 dalies b punktą, apsaugos priemonės. Ši taisyklė taikoma tik tais atvejais, kai tokio sprendimo pagrindas yra Jungtinės Karalystės teisėje nustatytas leidimas arba reikalavimas, ir ji negalioja, jeigu sprendimą būtina priimti pagal sutartį arba jis priimamas turint aiškų duomenų subjekto sutikimą. Jeigu taikomas 2018 m. DAA 14 straipsnis, duomenų valdytojas privalo kuo greičiau, kai tik tai pagrįstai įmanoma, raštu informuoti duomenų subjektą, kad buvo priimtas tik automatizuotu duomenų tvarkymu grindžiamas sprendimas. Duomenų subjektas turi teisę reikalauti, kad duomenų valdytojas per vieną mėnesį nuo pranešimo gavimo dienos persvarstytų sprendimą arba priimtų naują sprendimą, kuris nebūtų grindžiamas tik automatizuotu duomenų tvarkymu. Valstybės sekretorius turi įgaliojimus nustatyti papildomas apsaugos priemones, susijusias su automatizuotų sprendimų priėmimu. Šiais įgaliojimais dar nebuvo pasinaudota.

2.5.5.2. Asmens teisių apribojimai ir kitos nuostatos

(55) 2018 m. DAA nustatyta keletas pavienių teisių apribojimų, atitinkančių Jungtinės Karalystės BDAR 23 straipsnio sistemą. Pagal šią sistemą teisei nesutikti, kad duomenys būtų tvarkomi tiesioginės rinkodaros tikslais, kaip numatyta Jungtinės Karalystės BDAR 21 straipsnio 2 ir 3 dalyse, arba teisei, kad duomenų subjektui nebūtų taikomas automatizuotas sprendimų priėmimas, kaip numatyta Jungtinės Karalystės BDAR 22 straipsnyje, nenustatyti jokie apribojimai.

(56) Apribojimai išsamiai aprašyti 2018 m. DAA 2–4 prieduose. Jungtinės Karalystės institucijos paaiškino, kad jos taiko du principus: specifiškumo principą (laikomasi smulkmeniško požiūrio, apribojimus išskaidant į daugybę konkretesnių nuostatų) ir sąlygų taikymo principą (kiekvieną nuostatą papildo apsaugos priemonės, pagrįstos apribojimais arba sąlygomis, kuriomis siekiama užkirsti kelią piktnaudžiavimui) ([45]).

([43]) 17 straipsnio 1 dalies e punkte ir 17 straipsnio 3 dalies b punkte nuorodos į ES arba valstybės narės teisę buvo pakeistos nuoroda į vidaus teisę (kaip tokios vidaus teisės pagal 17 straipsnio 1 dalies e punktą pavyzdžius Jungtinė Karalystė nurodė 2006 m. Anglijos švietimo (mokinių informavimo) taisykles, pagal kurias reikalaujama ištrinti mokinių vardus ir pavardes iš mokyklos žurnalų po to, kai jie baigia mokyklą, arba 1983 m. Medicinos įstatymo 34F straipsnį, kuriame išdėstytos taisyklės dėl vardų ir pavardžių pašalinimo iš bendrosios praktikos gydytojų registro ir gydytojų specialistų registro.

([44]) Praktikos kodekso projektą galima rasti šiuo adresu: https://ico.org.uk/media/about-the-ico/consultations/2616882/direct-marketing-code-draft-guidance.pdf.

([45]) Diskusijoms dėl duomenų apsaugos tinkamumo skirto Jungtinės Karalystės aiškinamojo dokumento E skirsnis „Apribojimai“, p. 1, galima rasti šiuo adresu: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872232/E_-_Narrative_on_Restrictions.pdf.

(57) Jungtinės Karalystės BDAR 23 straipsnio 1 dalyje aprašytų apribojimų paskirtis – užtikrinti, kad jie būtų taikomi tik konkrečiomis aplinkybėmis, kai tai yra būtina demokratinėje visuomenėje ir proporcinga jų siekiamam tikslui. Be to, pagal suformuotą jurisprudenciją dėl apribojimų aiškinimo duomenų apsaugos režimo išimtis bet kuriuo konkrečiu atveju gali būti taikoma, jeigu tai daryti yra būtina ir proporcinga ([46]). Reikalaujama, kad būtinumo patikrinimas būtų „griežtas, o bet koks subjekto teisių ribojimas turi būti proporcingas grėsmės viešajam interesui mastui. Todėl patikrinimo metu atliekama įprasta proporcingumo analizė ([47])“.

(58) Tikslai, kurių siekiama šiais apribojimais, atitinka Reglamento (ES) 2016/679 23 straipsnyje išvardytus tikslus, išskyrus su nacionaliniu saugumu ir gynyba susijusius apribojimus, kurie vietoje to yra reglamentuojami 2018 m. DAA 26 straipsnyje, tačiau jiems taikomi tie patys būtinumo ir proporcingumo reikalavimai (žr. (63)–(66) konstatuojamąsias dalis).

(59) Kai kurie apribojimai, pvz., susiję su nusikaltimų prevencija arba nustatymu, nusikaltėlių sulaikymu ar baudžiamuoju persekiojimu, ir mokesčio arba rinkliavos dydžio nustatymu arba surinkimu ([48]), gali būti taikomi visoms asmenų teisėms ir skaidrumo įsipareigojimams (išskyrus 21 straipsnio 2 dalyje ir 22 straipsnyje nustatytas teises). Kiti apribojimai taikomi tik skaidrumo įsipareigojimams ir teisėms susipažinti su duomenimis, pvz., advokato teisei neatskleisti profesinės paslapties ([49]), teisei netaikyti reikalavimo pateikti informaciją, dėl kurios būtų duodami parodymai prieš save ([50]), ir įmonėms finansams, visų pirma prekybos pasinaudojant viešai neatskleista informacija prevencijai ([51]). Pagal keletą apribojimų leidžiama apriboti duomenų valdytojo pareigą pranešti duomenų subjektui apie duomenų apsaugos pažeidimą, taip pat tikslo apribojimo ir duomenų tvarkymo teisėtumo, sąžiningumo ir skaidrumo principus ([52]).

(60) Kai kurie apribojimai „visa apimtimi“ automatiškai taikomi tam tikros rūšies asmens duomenų tvarkymui (pvz., išimtis taikoma skaidrumo įsipareigojimams ir asmenų teisėms, jeigu asmens duomenys tvarkomi siekiant įvertinti, ar asmuo yra tinkamas eiti teisėjo pareigas, arba asmens duomenis tvarko bendrosios kompetencijos ar specializuotas teismas, arba asmuo, kuris veikia kaip teisėjas).

(61) Tačiau daugeliu atvejų 2018 m. DAA 2 priedo atitinkamoje dalyje konkrečiai nurodyta, kad apribojimas taikomas tik kai (ir tiek, kiek) nuostatų taikymas „galėtų pakenkti“ teisėtam tikslui, kurio siekiama tuo apribojimu: pvz., išvardytos Jungtinės Karalystės BDAR nuostatos netaikomos asmens duomenims, kurie tvarkomi nusikaltimų prevencijos ar nustatymo, nusikaltėlių sulaikymo ar baudžiamojo persekiojimo tikslais aura siekiant nustatyti mokesčio arba rinkliavos dydį ir ją surinkti „tiek, kiek tų nuostatų taikymas galėtų pakenkti“ bet kuriam iš šių tikslų ([53]).

(62) Sąvoką „galėtų pakenkti“, kuria nustatomas standartas, Jungtinės Karalystės teismai nuosekliai aiškino kaip reiškiančią „labai reikšmingą ir svarią galimybę pažeisti nustatytą viešąjį interesą“ ([54]). Todėl apribojimas vadovaujantis žalos kriterijumi gali būti pritaikytas tik tada ir tik tiek, kiek yra didelė ir reali tikimybė, kad tam tikros teisės suteikimas pakenktų viešajam interesui. Duomenų valdytojas yra atsakingas už tai, kad kiekvienu konkrečiu atveju būtų įvertinta, ar šios sąlygos yra tenkinamos ([55]).

(63) Be 2018 m. DAA 2 priede nustatytų apribojimų, 2018 m. DAA 26 straipsnyje numatyta išimtis, kurią galima taikyti tam tikroms Jungtinės Karalystės BDAR ir 2018 m. DAA nuostatoms, jeigu tą išimtį taikyti reikalinga nacionalinio saugumo arba gynybos tikslais. Ši išimtis taikoma duomenų apsaugos principams (išskyrus teisėtumo principą), skaidrumo įsipareigojimams, duomenų subjekto teisėms, prievolei pranešti apie duomenų saugumo pažeidimą,

([46]) Sprendimas *Open Rights Group & Anor, R (On the Application Of) prieš Secretary of State for the Home Department & Anor* [2019] EWHC 2562 (Admin), 40 ir 41 punktai.

([47]) Sprendimas *Guriev prieš Community Safety Development (United Kingdom) Ltd* [2016] EWHC 643 (QB), 43 punktas. Šiuo klausimu taip pat žr. sprendimą *Lin prieš Commissioner of Police for the Metropolis* [2015] EWHC 2484 (QB), 80 punktas.

([48]) 2018 m. DAA 2 priedo 2 dalis.

([49]) 2018 m. DAA 2 priedo 19 dalis.

([50]) 2018 m. DAA 2 priedo 20 dalis.

([51]) 2018 m. DAA 2 priedo 21 dalis.

([52]) Pavyzdžiui, teisės į pranešimus apie duomenų saugumo pažeidimus apribojimai leidžiami tik jeigu tai susiję su nusikaltimu ir apmokestinimu (2018 m. DAA 2 priedo 2 dalis), parlamentine privilegija (2018 m. DAA 2 priedo 13 dalis) ir duomenų tvarkymu žurnalistikos, akademiniais, meniniais ir literatūriniais tikslais (2018 m. DAA 2 priedo 26 dalis).

([53]) 2018 m. DAA 2 priedo 2 dalis.

([54]) Sprendimas *R (Lord) prieš Secretary of State for the Home Department* [2003] EWHC 2073 (Admin), 100 punktas, ir Sprendimas *Guriev prieš Community Safety Development (United Kingdom) Ltd* [2016] EWHC 643 (QB), 43 punktas.

([55]) Sprendimas *Open Rights Group & Anor, R (On the Application Of) prieš Secretary of State for the Home Department & Anor,* 31 punktas.

tarptautinio duomenų perdavimo taisyklėms, kai kurioms informacijos komisaro pareigoms ir įgaliojimams, taip pat taisyklėms dėl teisių gynimo priemonių, atsakomybės ir baudų, išskyrus nuostatą dėl administracinių baudų skyrimo bendrųjų sąlygų, kaip nustatyta Jungtinės Karalystės BDAR 83 straipsnyje, ir nuostatą dėl baudų, nustatytų Jungtinės Karalystės BDAR 84 straipsnyje. Be to, 2018 m. 28 straipsniu pakeičiamas 9 straipsnio 1 dalies taikymas, kad būtų sudarytos sąlygos tvarkyti Jungtinės Karalystės BDAR 9 straipsnio 1 dalyje nustatytų specialių kategorijų duomenis ir tai daryti tiek, kiek duomenys tvarkomi nacionalinio saugumo arba gynybos užtikrinimo tikslais ir nustatant tinkamas duomenų subjektų teisių ir laisvių apsaugos priemones ([56]).

(64) Išimtis gali būti taikoma tik tiek, kiek tai yra reikalinga nacionalinio saugumo arba gynybos užtikrinimo tikslais. Kadangi tą patį galima pasakyti apie kitas 2018 m. DAA nustatytas išimtis, duomenų valdytojas jas taikyti ir jomis remtis gali kiekvienu konkrečiu atveju. Be to, bet koks išimties taikymas turi atitikti žmogaus teisių standartus (grindžiamus 1998 m. Žmogaus teisių aktu), pagal kuriuos bet koks privatumo teisių ribojimas demokratinėje visuomenėje turėtų būti būtinas ir proporcingas ([57]).

(65) Tokį išimties aiškinimą patvirtino ir Informacijos komisaras, pateikęs išsamias gaires dėl nacionalinio saugumo ir gynybos išimties taikymo, kuriose aiškiai nurodyta, kad duomenų valdytojas turi įvertinti išimties taikymo poreikį kiekvienu konkrečiu atveju ([58]). Visų pirma gairėse pabrėžiama, kad „tai nėra bendra išimtis“ ir kad norint ja remtis, „nepakanka nurodyti, kad duomenys būtų tvarkomi nacionalinio saugumo tikslais“. Kita vertus, duomenų valdytojas, kuris išimtimi remiasi, privalo „įrodyti, kad yra reali neigiamo poveikio nacionaliniam saugumui galimybė“ ir, jei reikia, „turėtų pateikti [Informacijos komisarui] įrodymų, kodėl buvo pasinaudota šia išimtimi“. Gairėse pateikiamas kontrolinis sąrašas ir keletas pavyzdžių, kuriais siekiama išsamiau paaiškinti sąlygas, kuriomis galima taikyti šią išimtį.

(66) Todėl faktinė aplinkybė, kad duomenys tvarkomi nacionalinio saugumo arba gynybos tikslais, pati savaime nėra pakankama tam, kad būtų galima taikyti išimtį. Jei duomenų valdytojas turėjo laikytis konkrečios su duomenų apsauga susijusios nuostatos, jis privalo išnagrinėti faktines pasekmes nacionaliniam saugumui. Išimtis gali būti taikoma tik toms konkrečioms nuostatoms, kurios, kaip nustatyta, kelia riziką, ir jas būtina taikyti kuo griežčiau ([59]).

(67) Šį požiūrį patvirtino Informacijos specializuotas teismas ([60]). Sprendime *Baker prieš Secretary of State for the Home Department* (toliau – Sprendimas *Baker prieš Secretary of State*) jis nustatė, kad nacionalinio saugumo išimties, kaip bendros išimties, taikymas buvo neteisėtas. Vietoje to, išimtis turėjo būti taikoma kiekvienu konkrečiu atveju išnagrinėjant kiekvieną prašymą iš esmės ir atsižvelgiant į asmenų teisę į jų privataus gyvenimo gerbimą ([61]).

---

([56]) Remiantis Jungtinės Karalystės institucijų pateikta informacija, tais atvejais, kai duomenys tvarkomi nacionalinio saugumo tikslais, duomenų valdytojai paprastai taikys griežtesnes su tvarkymu susijusias apsaugos ir saugumo priemones, kurios dera su slaptu tvarkymo pobūdžiu. Klausimas dėl tinkamų apsaugos priemonių bus sprendžiamas atsižvelgiant į riziką, kurią kelia duomenų tvarkymas. Šios priemonės galėtų būti susijusios su teisės susipažinti su duomenimis apribojimais, kuriuos taikant duomenys būtų prieinami tik įgaliotiems asmenims, dėl kurių atliktas atitinkamas patikimumo patikrinimas, griežtais dalijimosi duomenimis apribojimais ir aukštu saugumo standartu, taikomu saugojimo ir tvarkymo procedūroms.

([57]) Taip pat žr. Sprendimo *Guriev prieš Community Safety Development (United Kingdom) Ltd* [2016] EWHC 643 (QB), 45 punktą; Sprendimo *Lin prieš Commissioner of Police for the Metropolis* [2015] EWHC 2484 (QB), 80 punktą.

([58]) Žr. Informacijos komisaro gaires dėl nacionalinio saugumo ir gynybos išimties, kurias galima rasti adresu https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/national-security-and-defence/.

([59]) Remiantis Jungtinės Karalystės institucijų pateiktu pavyzdžiu, jeigu įtariamas teroristas, dėl kurio saugumo tarnyba MI5 atlieka tyrimą, Vidaus reikalų ministerijai pateikė prašymą leisti susipažinti su duomenimis (pvz., dėl to, kad jis dalyvauja ginče su Vidaus reikalų ministerija dėl imigracijos klausimų), gali prireikti užtikrinti, kad duomenų subjektui nebūtų atskleisti jokie duomenys, kuriais MI5 galėjo dalytis su Vidaus reikalų ministerija dėl vykdomų tyrimų, nes tai gali pakenkti slaptiems informacijos šaltiniams, metodams arba būdams ir (arba) padidinti asmens keliamą grėsmę. Tokiomis aplinkybėmis tikėtina, kad 26 straipsnio išimties taikymo riba nebūtų pažeista ir išimtį dėl informacijos neatskleidimo būtų reikalinga taikyti, siekiant apsaugoti nacionalinį saugumą. Tačiau jeigu Vidaus reikalų ministerija taip pat turėjo atitinkamo asmens duomenų, nesusijusių su MI5 tyrimu, ir tą informaciją buvo galima pateikti nesukeliant rizikos pakenkti nacionaliniam saugumui, tuomet nacionalinio saugumo išimtis, nagrinėjant informacijos atskleidimo asmeniui klausimą, nebūtų taikoma. Informacijos komisaras dabar rengia gaires, kaip duomenų valdytojai turėtų naudoti 26 straipsnyje nustatytą išimtį. Gaires tikimasi paskelbti iki 2021 m. kovo mėn. pabaigos.

([60]) Specializuotas informacijos bylų teismas buvo įsteigtas tam, kad pagal 1984 m. Duomenų apsaugos aktą nagrinėtų skundus dėl duomenų apsaugos. 2010 m. vykdant Jungtinės Karalystės specializuotų teismų reformą Specializuotas informacijos teismas tapo Pirmosios instancijos specializuoto teismo bendruosius reguliavimo klausimus sprendžiančia kolegija.

([61]) Žr. Sprendimą *Baker prieš Secretary of State for the Home Department* [2001] UKIT NSA2 („*Baker prieš Secretary of State*“).

2.5.6. *Žurnalistikos, akademiniais, meniniais ir literatūriniais, taip pat archyvavimo ir mokslinių tyrimų tikslais tvarkomų asmens duomenų apribojimai*

(68) Pagal Jungtinės Karalystės BDAR 85 straipsnio 2 dalį leidžiama numatyti atvejus, susijusius su asmens duomenų tvarkymu žurnalistikos, akademiniais, meniniais ir literatūriniais tikslais, kuriems netaikomos kelios Jungtinės Karalystės BDAR nuostatos. 2018 m. DAA 2 priedo 5 dalyje nustatytos duomenų tvarkymo šiais tikslais išimtys. Joje numatytos duomenų apsaugos principų (išskyrus vientisumo ir konfidencialumo principą) išimtys, duomenų tvarkymo teisiniai pagrindai (įskaitant specialias duomenų kategorijas ir su apkaltinamaisiais nuosprendžiais susijusius duomenis ir pan.), sutikimo sąlygos, skaidrumo įpareigojimai, duomenų subjektų teisės, pareiga pranešti apie duomenų saugumo pažeidimus, reikalavimas konsultuotis su informacijos komisaru prieš pradedant tvarkyti su ypač didele rizika susijusius duomenis ir taisyklės dėl tarptautinio duomenų perdavimo ([62]). Šiuo atžvilgiu Jungtinės Karalystės BDAR iš esmės nenukrypstama nuo Reglamento (ES) 2016/679, kurio 85 straipsnyje taip pat numatyta galimybė žurnalistiniais tikslais arba akademinės, meninės ar literatūrinės saviraiškos tikslais tvarkomiems duomenims netaikyti kelių Reglamento (ES) 2016/679 reikalavimų. 2018 m. DAA nuostatos, ypač 2 priedo 5 dalis, yra suderinamos su Junginės Karalystės BDAR.

(69) Pagrindinė pusiausvyros nustatymo užduotis, kuri turi būti atlikta pagal Jungtinės Karalystės BDAR 85 straipsnį, yra susijusi su tuo, ar (68) konstatuojamojoje dalyje paminėtos duomenų apsaugos taisyklės yra „būtinos, kad teisė į asmens duomenų apsaugą būtų suderinta su saviraiškos ir informacijos laisve“ ([63]). Pagal 2018 m. DAA 2 priedo 26 straipsnio 2 ir 3 dalis Jungtinė Karalystė, siekdama nustatyti šią pusiausvyrą, taiko „pagrįsto įsitikinimo“ kriterijų. Kad išimtis būtų pateisinama, duomenų valdytojas privalo pagrįstai įsitikinti, kad i) paskelbimas atitinka viešąjį interesą ir ii) atitinkamos BDAR nuostatos taikymas būtų nesuderinamas su žurnalistiniais, akademiniais, meniniais arba literatūriniais tikslais. Kaip nustatyta teismų praktikoje ([64]), „pagrįsto įsitikinimo“ patikrinimas yra grindžiamas subjektyviu ir objektyviu aspektais: duomenų valdytojui nepakanka įrodyti, kad, jo manymu, nuostatos laikymasis buvo nesuderinamas. Jo įsitikinimas turi būti pagrįstas, t. y. taip galėtų manyti protingas asmuo, žinantis susijusias aplinkybes. Todėl duomenų valdytojas, formuodamas savo įsitikinimą, turėtų atlikti deramą patikrinimą ir taip įrodyti protingumą. Remiantis Jungtinės Karalystės institucijų pateiktais paaiškinimais, „pagrįsto įsitikinimo“ patikrinimas turi būti atliekamas dėl kiekvienos išimties ([65]). Jeigu sąlygos tenkinamos, laikoma, kad išimtis yra būtina ir proporcinga pagal Jungtinės Karalystės teisę.

(70) Pagal 2018 m. DAA 124 straipsnį informacijos komisaras privalo parengti Duomenų apsaugos ir žurnalistikos praktikos kodeksą. Šis kodeksas dabar rengiamas. Šiuo klausimu pagal 1998 m. Duomenų apsaugos aktą buvo paskelbtos gairės, kuriose visų pirma pažymima, kad, remiantis šia išimtimi, paprasčiausiai pakanka nurodyti, kad dėl nuostatos laikymosi kiltų nepatogumų žurnalistinei veiklai, tačiau šiuo atveju turi būti aiškus

([62]) Žr. Jungtinės Karalystės BDAR 85 straipsnį ir 2018 m. DAA 2 priedo 5 dalies 26 straipsnio 9 dalį.

([63]) Pagal 2018 m. DAA 2 priedo 5 dalies 26 straipsnio 2 dalį išimtis taikoma tais atvejais, kai asmens duomenys tvarkomi konkrečiais tikslais (žurnalistikos tikslais arba akademinės, meninės ar literatūrinės saviraiškos tikslais), jeigu asmuo duomenis tvarko tam, kad paskelbtų žurnalistinę, akademinę, meninę arba literatūrinę medžiagą, ir duomenų valdytojas pagrįstai mano, kad tos medžiagos paskelbimas atitiks viešąjį interesą. Nustatydamas, ar paskelbimas atitiks viešąjį interesą, duomenų valdytojas privalo atsižvelgti į ypatingą viešojo intereso svarbą užtikrinant saviraiškos ir informacijos laisvę. Be to, duomenų valdytojas privalo atsižvelgti į su atitinkamos informacijos paskelbimu susijusius praktikos kodeksus arba gaires (BBC redakcinės gairės, „Ofcom“ transliavimo kodeksas ir redaktorių praktikos kodeksas). Be to, tam, kad išimtį būtų galima taikyti, duomenų valdytojas privalo pagrįstai manyti, kad atitiktis susijusiai nuostatai būtų nesuderinama su konkrečiais tikslais (2018 m. DAA 2 priedo 26 straipsnio 3 dalis).

([64]) Sprendimo *NT1 prieš Google* [2018] EWHC 799 (QB) 102 punkte aptariama, ar duomenų valdytojas buvo pagrįstai įsitikinęs, kad informacijos atskleidimas atitiko viešąjį interesą ir kad atitinkamų nuostatų laikymasis buvo nesuderinamas su specialiais tikslais. Teismas nurodė, kad 1998 m. Duomenų apsaugos akto 32 straipsnio 1 dalies b ir c punktai turi subjektyvų ir objektyvų aspektą: duomenų valdytojas privalo nustatyti, kad jis buvo įsitikinęs, jog paskelbimas turėtų atitikti viešąjį interesą ir kad šis įsitikinimas buvo objektyviai pagrįstas; duomenų valdytojas privalo nustatyti subjektyvų įsitikinimą, kad nuostatos, kuriai jis nori taikyti išimtį, laikymasis būtų nesuderinamas su atitinkamu specialiu tikslu.

([65]) „Pagrįsto įsitikinimo“ patikrinimo taikymo pavyzdys pateiktas Informacijos komisaro sprendime skirti baudą *True Visions Productions*, priimtame pagal 1998 m. Duomenų apsaugos aktą. Informacijos komisaras sutiko, kad žiniasklaidos duomenų valdytojas buvo subjektyviai įsitikinęs, kad pirmojo duomenų apsaugos principo (sąžiningumas ir teisėtumas) laikymasis buvo nesuderinamas su žurnalistikos tikslais. Tačiau informacijos komisaras nesutiko su tuo, kad šis įsitikinimas buvo objektyviai pagrįstas. Informacijos komisaro sprendimą galima rasti šiuo adresu: https://ico.org.uk/media/action-weve-taken/mpns/2614746/true-visions-productions-20190408.pdf.

argumentas, kad atitinkama nuostata tampa kliuviniu atsakingai žurnalistikai ([66]). Jungtinės Karalystės telekomunikacijų reguliavimo institucija OFCOM ir BBC savo redakcinėse gairėse taip pat paskelbė viešojo intereso patikrinimo taikymo ir viešojo intereso suderinimo su asmeniniu privatumo interesu gaires ([67]). Gairėse visų pirma pateikiama informacijos, kuri gali būti laikoma atitinkanti viešąjį interesą, pavyzdžių ir paaiškinamas poreikis sugebėti įrodyti, kad viešasis interesas konkrečiomis bylos aplinkybėmis yra viršesnis už privatumo teises.

(71) Panašiai, kaip nurodyta BDAR 89 straipsnyje, archyvavimo tikslais, atsižvelgiant į viešąjį interesą, taip pat mokslinių arba istorinių tyrimų arba statistiniais tikslais tvarkomiems asmens duomenims taip pat gali būti taikomos įvairios Jungtinės Karalystės BDAR išvardytų nuostatų išimtys ([68]). Dėl mokslinių tyrimų ir statistinių duomenų pažymėtina, kad išimtis galima taikyti Jungtinės Karalystės BDAR nuostatoms, susijusioms su duomenų tvarkymo patvirtinimu, susipažinimu su duomenimis ir apsaugos priemonėmis, taikomomis duomenis perduodant į trečiąsias valstybes; teise reikalauti ištaisyti duomenis; duomenų tvarkymo apribojimu ir nesutikimu su duomenų tvarkymu. Dėl archyvavimo viešojo intereso labui pažymėtina, kad išimtis taip pat galima taikyti pareigai pranešti apie asmens duomenų ištaisymą arba ištrynimą, arba duomenų tvarkymo apribojimui ir teisei į duomenų perkeliamumą.

(72) Kaip nurodyta 2018 m. DAA 2 priedo 27 straipsnio 1 dalyje ir 28 straipsnio 1 dalyje, Jungtinės Karalystės BDAR išvardytų nuostatų išimtys yra pateisinamos, jeigu taikant nuostatas „būtų užkirstas kelias arba iš esmės pakenkta“ atitinkamo tikslo pasiekimui ([69]).

(73) Kadangi šių išimčių reikšmė užtikrinant veiksmingą asmens teisių įgyvendinimą yra didelė, vykdant nuolatinę šio sprendimo stebėseną bus deramai atsižvelgiama į visus svarbius pokyčius, susijusius su pirmiau minėtų išimčių (šalia išimties, susijusios su veiksmingos imigracijos kontrolės palaikymu, kaip paaiškinta 6 konstatuojamojoje dalyje) aiškinimu ir taikymu praktikoje , įskaitant bet kokius tolesnius teismų praktikos ir Informacijos komisaro gairių bei vykdymo užtikrinimo veiksmų pokyčius ([70]).

2.5.7. *Tolesnio duomenų perdavimo ribojimas*

(74) Asmens duomenims, perduodamiems iš Europos Sąjungos Jungtinės Karalystės duomenų valdytojams arba duomenų tvarkytojams, užtikrinamas apsaugos lygis neturėtų sumažėti tokius duomenis toliau perduodant gavėjams trečiojoje valstybėje. Toks „tolesnis perdavimas“, kuris Jungtinės Karalystės duomenų valdytojų arba duomenų tvarkytojų požiūriu laikomas tarptautiniu perdavimu iš Jungtinės Karalystės, turėtų būti leidžiamas tik tada, kai tolesniam gavėjui, esančiam už Jungtinės Karalystės ribų, taikomos taisyklės, kuriomis užtikrinama panašaus lygio apsauga kaip Jungtinės Karalystės teisinėje sistemoje. Dėl šios priežasties Jungtinės Karalystės BDAR ir 2018 m. DAA taisyklių dėl tarptautinio duomenų perdavimo taikymas yra svarbus veiksnys, siekiant užtikrinti apsaugos tęstinumą tuo atveju, kai asmens duomenys pagal šį sprendimą perduodami iš Europos Sąjungos į Jungtinę Karalystę.

([66]) Remiantis gairėmis, organizacijos privalo paaiškinti, kodėl 1998 m. Duomenų apsaugos akto atitinkamos nuostatos yra nesuderinamos su žurnalistikos tikslais. Visų pirma duomenų valdytojai privalo suderinti žalingą nuostatos laikymosi poveikį, kuris būtų daromas žurnalistikai, su žalingu nuostatos nesilaikymo poveikiu, kuris būtų daromas duomenų subjekto teisėms. Jeigu žurnalistas gali pagrįstai pasiekti savo redakcinius tikslus su DAA nuostatomis suderinamu būdu, jis tai privalo padaryti. Organizacijos privalo turėti galimybę pagrįsti apribojimo taikymą kiekvienai nuostatai, kurios jie nesilaikė. „Duomenų apsauga ir žurnalistika: žiniasklaidos vadovas“, galima rasti šiuo adresu: https://ico.org.uk/media/for-organisations/documents/1552/data-protection-and-journalism-media-guidance.pdf.

([67]) Viešojo intereso pavyzdžiai galėtų būti nusikaltimo atskleidimas arba nustatymas, visuomenės sveikatos apsauga arba saugumo užtikrinimas, asmenų arba organizacijų padarytų klaidinančių teiginių atskleidimas arba nekompetentingumo atvejų, darančių poveikį visuomenei, atskleidimas. Žr. OFCOM gaires, kurias galima rasti šiuo adresu: https://www.ofcom.org.uk/__data/assets/pdf_file/0017/132083/Broadcast-Code-Section-8.pdf ir BBC redakcines gaires, kurias galima rasti šiuo adresu: https://www.bbc.com/editorialguidelines/guidelines/privacy.

([68]) Žr. Jungtinės Karalystės BDAR 89 straipsnį ir 2018 m. DAA 2 priedo 6 dalies 27 straipsnio 2 dalį ir 28 straipsnio 2 dalį.

([69]) Šiuo atveju taikomas reikalavimas dėl asmens duomenų tvarkymo pagal Jungtinės Karalystės BDAR 89 straipsnio 1 dalį, papildytą 2018 m. DAA 19 straipsniu.

([70]) Žr. (281) – (287)konstatuojamąsias dalis.

(75) Asmens duomenų tarptautinio perdavimo iš Jungtinės Karalystės tvarka yra nustatyta Jungtinės Karalystės BDAR 44–49 straipsniuose, kaip papildyta 2018 m. DAA, kuri iš esmės yra tokia pat kaip Reglamento (ES) 2016/679 V skyriuje nustatyta tvarka ([71]). Asmens duomenys į trečiąją valstybę arba tarptautinei organizacijai gali būti perduodami tik remiantis tinkamumo taisyklėmis (Jungtinės Karalystės atitikmuo sprendimui dėl tinkamumo pagal Reglamentą (ES) 2016/679), arba, jeigu tinkamumo taisyklių nėra, duomenų valdytojui arba duomenų tvarkytojui numačius tinkamas apsaugos priemones pagal Jungtinės Karalystės BDAR 46 straipsnį. Jeigu nėra tinkamumo taisyklių arba tinkamų apsaugos priemonių, duomenys gali būti perduodami tik remiantis Jungtinės Karalystės BDAR 49 straipsnyje nustatytomis nukrypti leidžiančiomis nuostatomis.

(76) Valstybės sekretoriaus priimtose tinkamumo taisyklėse gali būti nustatyta, kad trečiojoje valstybėje (arba trečiosios valstybės teritorijoje arba sektoriuje), tarptautinėje organizacijoje arba tos valstybės, teritorijos, sektoriaus arba organizacijos aprašyme ([72]) užtikrinama tinkama asmens duomenų apsauga. Vertindamas apsaugos lygio tinkamumą, valstybės sekretorius privalo atsižvelgti į lygiai tuos pačius aspektus, kuriuos Komisija privalo įvertinti pagal Reglamento (ES) 2016/679 45 straipsnio 2 dalies a–c punktus, atsižvelgiant į tai, kaip jis išaiškintas Reglamento (ES) 2016/679104 konstatuojamojoje dalyje ir paliktoje galioti ES teismų praktikoje. Tai reiškia, kad vertinant trečiosios valstybės apsaugos lygio tinkamumą, bus taikomas atitinkamas standartas, susiję su tuo, ar ta atitinkama trečioji valstybė užtikrina apsaugos lygį, kuris yra „iš esmės lygiavertis“ Jungtinėje Karalystėje garantuojamai apsaugai.

(77) Kalbant apie procedūrą pažymėtina, kad tinkamumo taisyklėms taikomi „bendrieji“ procedūriniai reikalavimai, nustatyti 2018 m. DAA 182 straipsnyje. Pagal šią procedūrą valstybės sekretorius privalo konsultuotis su informacijos komisaru tais atvejais, kai siūloma priimti Jungtinės Karalystės tinkamumo taisykles ([73]). Valstybės sekretoriaus priimtos taisyklės pateikiamos parlamentui ir joms taikoma „neigiamos rezoliucijos“ procedūra, pagal kurią abeji parlamento rūmai gali tikrinti taisykles ir turi galimybę per 40 dienų priimti pasiūlymą dėl taisyklių panaikinimo ([74]).

(78) Pagal 2018 m. DAA 17B straipsnio 1 dalį tinkamumo taisyklės turi būti peržiūrimos ne rečiau kaip kas ketverius metus ir valstybės sekretorius privalo nuolat stebėti pokyčius trečiosiose valstybėse ir tarptautinėse organizacijose, kurie galėtų daryti poveikį sprendimams nustatyti tinkamumo taisykles arba jas iš dalies pakeisti ar panaikinti. Jeigu valstybės sekretorius sužino, kad nurodyta arba organizacija nebeužtikrina tinkamo asmens duomenų apsaugos lygio, jis privalo, kiek tai įmanoma, iš dalies pakeisti arba panaikinti taisykles ir pradėti konsultacijas su atitinkama trečiąja valstybe arba tarptautine organizacija, kad ištaisytų tinkamos apsaugos lygio trūkumą. Šie procedūriniai aspektai taip pat atsispindi atitinkamuose Reglamento (ES) 2016/679 reikalavimuose.

---

([71]) Išskyrus Reglamento (ES) 2016/679 48 straipsnį, kurio Jungtinė Karalystė nusprendė neįtraukti į Jungtinės Karalystės BDAR. Šiuo atžvilgiu pirmiausia reikėtų priminti, kad tinkamo apsaugos lygio standartu laikytinas esminio lygiavertiškumo, o ne tapatumo standartas, kaip išaiškino ESTT (Sprendimo *Schrems I* 73–74 punktai) ir pripažino Europos duomenų apsaugos valdyba („Orientaciniai tinkamumo kriterijai“, p. 3). Todėl, kaip Europos duomenų apsaugos valdyba paaiškino savo dokumente „Orientaciniai tinkamumo kriterijai“, „tikslas – ne atitikti kiekvieną Europos Sąjungos teisės akto punktą, o nustatyti pagrindinius, esmę perteikiančius nagrinėjamo teisės akto reikalavimus“. Šiuo atžvilgiu svarbu pažymėti, kad nors Jungtinės Karalystės teisinėje sistemoje formaliai nėra 48 straipsniui tapačios nuostatos, tą patį poveikį garantuoja kitos teisinės nuostatos ir principai, t. y. kad trečiosios šalies teismo ar administracinės institucijos prašymu asmens duomenys gali būti perduoti į tą trečiąją šalį tik tuo atveju, jei sudarytas tarptautinis susitarimas, kuriuo remiantis atitinkamas trečiosios šalies teismo sprendimas arba administracinis sprendimas pripažįstamas arba vykdomas Jungtinėje Karalystėje arba jei jis vykdomas pagal vieną iš Jungtinės Karalystės BDAR V skyriuje nustatytų mechanizmų. Konkrečiau kalbant, tam, kad galėtų vykdyti užsienio teismo sprendimą, Jungtinės Karalystės teismai privalo turėti galimybę pateikti nuorodą į bendrąją teisę arba statutą, pagal kurį sprendimą leidžiama vykdyti. Tačiau nei bendrojoje teisėje (žr. 1990 m. liepos 11 d. Sprendimą *Adams ir kt. prieš Cape Industries Plc.*, [1990] 2 W.L.R.657), nei kituose įstatymuose nenumatytas užsienio teismo sprendimų, pagal kuriuos reikalaujama perduoti duomenis be tarptautinio susitarimo, vykdymas. Todėl pagal Jungtinės Karalystės teisę, nesant tokio tarptautinio susitarimo, prašymai pateikti duomenis yra nevykdytini. Be to, bet kokiam asmens duomenų perdavimui trečiosioms šalims, be kita ko, užsienio teismo ar administracinės institucijos prašymu, toliau taikomi Jungtinės Karalystės BDAR V skyriuje nustatyti apribojimai, kurie yra identiški atitinkamoms Reglamento (ES) 2016/679 nuostatoms, todėl privaloma remtis vienu iš perdavimo pagrindų, numatytų V skyriuje, laikantis konkrečių jam taikomų sąlygų, kaip nustatyta tame skyriuje.

([72]) Jungtinės Karalystės institucijos paaiškino, kad valstybės arba tarptautinės organizacijos aprašymas reiškia situaciją, kai būtų reikalinga priimti konkretų arba dalinį sprendimą dėl tinkamumo, kuriame būtų nustatyti konkretūs apribojimai (pvz., tinkamumo taisyklės, susijusios tik su tam tikrų rūšių duomenų perdavimu).

([73]) Žr. valstybės sekretoriaus, veikiančio Skaitmeninių, kultūros, žiniasklaidos ir sporto reikalų departamento vardu, ir Informacijos komisaro biuro susitarimo memorandumą dėl Informacijos komisaro vaidmens pagal naują tvarką vertinant Jungtinėje Karalystėje užtikrinamos duomenų apsaugos tinkamumą, kurį galima rasti adresu https://www.gov.uk/government/publications/memorandum-of-understanding-mou-on-the-role-of-the-ico-in-relation-to-new-uk-adequacy-assessments.

([74]) Jeigu tokio balsavimo metu būtų gautas pritarimas, taisyklės galiausiai nebeturėtų jokios tolesnės teisinės galios.

(79) Jeigu tinkamumo taisyklių nėra, tarptautiniai perdavimai gali vykti tais atvejais, kai duomenų valdytojas arba duomenų tvarkytojas pateikė tinkamas apsaugos priemones pagal Jungtinės Karalystės BDAR 46 straipsnį. Šios apsaugos priemonės yra panašios į numatytąsias Reglamento (ES) 2016/679 46 straipsnyje. Jos apima valdžios institucijoms ar įstaigoms teisiškai privalomas ir įgyvendinamas priemones, įmonėms privalomas taisykles ([75]), standartines duomenų apsaugos sąlygas, patvirtintus elgesio kodeksus, patvirtintus sertifikavimo mechanizmus ir duomenų valdytojų (arba duomenų tvarkytojų) tarpusavio sutarčių sąlygas arba valdžios institucijų administracines taisykles, kurias leido nustatyti informacijos komisaras. Tačiau taisyklės buvo pakeistos procedūriniu požiūriu, kad jos veiktų Jungtinės Karalystės sistemoje, visų pirma kad valstybės sekretorius (17C straipsnis) arba informacijos komisaras (119A straipsnis) pagal 2018 m. DAA galėtų patvirtinti standartines duomenų apsaugos sąlygas.

(80) Jeigu nėra sprendimo dėl tinkamumo arba tinkamų apsaugos priemonių, duomenys gali būti perduodami tik remiantis Jungtinės Karalystės BDAR 49 straipsnyje nustatytomis nukrypti leidžiančiomis nuostatomis ([76]). Jungtinės Karalystės BDAR nenustatyti jokie reikšmingi šių nukrypti leidžiančių nuostatų pakeitimai, palyginti su atitinkamomis Reglamento (ES) 2016/679 taisyklėmis. Pagal Jungtinės Karalystės BDAR, kaip ir pagal Reglamentą (ES) 2016/679, tam tikromis nukrypti leidžiančiomis nuostatomis galima remtis tik jeigu duomenys perduodami retkarčiais ([77]). Be to, savo gairėse dėl tarptautinių perdavimų informacijos komisaras paaiškina, kad: „Šias nuostatas turėtumėte naudoti kaip tikras bendrosios taisyklės, pagal kurią neturėtumėte atlikti apriboto perdavimo, „išimtis“, išskyrus atvejus, kai tokiam perdavimui taikomas sprendimas dėl tinkamumo arba galioja nustatytos tinkamos apsaugos priemonės“ ([78]). Dėl perdavimų, kurie yra būtini atsižvelgiant į svarbias su viešuoju interesu susijusias priežastis (49 straipsnio 1 dalies d punktas), valstybės sekretorius gali priimti taisykles, kuriose nurodo konkrečias aplinkybes, kuriomis asmens duomenų į trečiąją valstybę arba tarptautinei organizacijai perduoti nebūtina dėl svarbių su viešuoju interesu susijusių priežasčių. Be to, valstybės sekretorius taisyklėmis gali riboti į trečiąją valstybę arba tarptautinei organizacijai perduodamų asmens duomenų kategoriją, jeigu perdavimo negalima atlikti remiantis tinkamumo taisyklėmis ir jeigu valstybės sekretorius mano, kad apribojimas yra būtinas atsižvelgiant į svarbias priežastis, susijusias su viešuoju interesu. Iki šiol tokios taisyklės dar nepriimtos.

(81) Ši tarptautinių perdavimų sistema pradėta taikyti pasibaigus pereinamajam laikotarpiui ([79]). Tačiau 2018 m. DAA 21 priedo 4 dalyje (nustatytoje DAPER taisyklėmis) numatyta, kad pereinamojo laikotarpio pabaigoje laikoma, kad tam tikri asmens duomenų perdavimai yra pagrįsti tinkamumo taisyklėmis. Tai yra perdavimai į EEE valstybę, Gibraltaro teritoriją, Sąjungos institucijai, įstaigai, biurui arba agentūrai, įsteigtai pagal ES sutartį arba ja remiantis, ir į trečiąsias valstybes, kurioms pereinamojo laikotarpio pabaigoje buvo taikomas ES sprendimas dėl tinkamumo. Todėl perdavimai į šias valstybes gali būti toliau atliekami tokia pat tvarka, kaip

([75]) Jungtinės Karalystės BDAR paliktos galioti Reglamento (ES) 2016/679 47 straipsnyje nustatytos taisyklės ne tik keičiamos, kad atitiktų vidaus aplinkybes, pvz., nuorodas į kompetentingą priežiūros instituciją pakeičiant nuoroda į informacijos komisarą, 1 dalyje išbraukiant nuorodą į nuoseklumo užtikrinimo mechanizmą ir išbraukiant visą 3 dalį.

([76]) Pagal Jungtinės Karalystės BDAR 49 straipsnį duomenis perduoti įmanoma, jeigu įvykdoma viena iš toliau išvardytų sąlygų: a) duomenų subjektas aiškiai sutiko su siūlomu duomenų perdavimu po to, kai buvo informuotas apie galimus tokių perdavimų pavojus duomenų subjektui dėl to, kad nepriimtas sprendimas dėl tinkamumo ir nenustatytos tinkamos apsaugos priemonės; b) duomenų perdavimas yra būtinas duomenų subjekto ir duomenų valdytojo sutarčiai vykdyti arba ikisutartinėms priemonėms, kurių imtasi duomenų subjekto prašymu, įgyvendinti; c) duomenų perdavimas yra būtinas, kad būtų sudaryta arba įvykdyta duomenų subjekto interesais sudaroma duomenų valdytojo ir kito fizinio ar juridinio asmens sutartis; d) duomenų perdavimas yra būtinas dėl svarbių viešojo intereso priežasčių; e) duomenų perdavimas yra būtinas siekiant pareikšti, vykdyti ar ginti teisinius reikalavimus; f) duomenų perdavimas yra būtinas, kad būtų apsaugoti gyvybiniai duomenų subjekto arba kitų asmenų interesai, jeigu duomenų subjektas dėl fizinių ar teisinių priežasčių negali duoti sutikimo; g) duomenys perduodami iš registro, kuris pagal vidaus teisę yra skirtas teikti visuomenei informaciją ir kuriuo gali naudotis plačioji visuomenė arba bet kuris asmuo, galintis įrodyti savo teisėtą interesą, tačiau tik tiek, kiek kiekvienu konkrečiu atveju yra įvykdytos vidaus teisėje nustatytos sąlygos dėl susipažinimo su informacija. Be to, jeigu netaikoma nė viena iš pirmiau išvardytų sąlygų, duomenys gali būti perduodami tik jeigu tai nedaroma pakartotinai, perduodami tik kelių duomenų subjektų duomenys, duomenis perduoti būtina siekiant patenkinti įtikinamus teisėtus interesus, kurių siekia duomenų valdytojas ir už kuriuos nėra viršesni duomenų subjekto interesai arba teisės ir laisvės, ir duomenų valdytojas įvertino visas su duomenų perdavimu susijusias aplinkybes ir, remdamasis tuo vertinimu, nustatė tinkamas apsaugos priemones, susijusias su asmens duomenų apsauga.

([77]) Jungtinės Karalystės BDAR 111 konstatuojamojoje dalyje nurodyta, kad duomenų perdavimas pagal sutartį ar teisinį reikalavimą gali būti atliekamas tik jei tai daroma retkarčiais.

([78]) Informacijos komisaro gairės dėl tarptautinių perdavimų, galima rasti šiuo adresu: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/#ib7.

([79]) Per ilgiausią šešių mėnesių terminą, bet ne vėliau kaip iki 2021 m. birželio 30 d. ši nauja sistema turi būti taikoma atsižvelgiant į Europos Sąjungos bei Europos atominės energijos bendrijos ir Jungtinės Didžiosios Britanijos ir Šiaurės Airijos Karalystės prekybos ir bendradarbiavimo susitarimo 782 straipsnį (L 444/14, 2020 m. gruodžio 31 d.) (toliau – ES ir Jungtinės Karalystės prekybos ir bendradarbiavimo susitarimas), galima rasti šiuo adresu: https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:22020A1231(01)&from=LT.

iki Jungtinės Karalystės išstojimo iš ES. Pasibaigus pereinamajam laikotarpiui, valstybės sekretorius privalo per ketverių metų terminą, t. y. iki 2024 m. gruodžio mėn. pabaigos, peržiūrėti šias išvadas dėl tinkamumo. Kaip nurodyta Jungtinės Karalystės institucijų pateiktame paaiškinime, nors valstybės sekretorius tokią peržiūrą turi atlikti iki 2024 m. gruodžio mėn. pabaigos, į pereinamojo laikotarpio nuostatas laikino galiojimo sąlyga neįtraukta, todėl, jeigu peržiūra iki 2024 m. gruodžio mėn. pabaigos nebus užbaigta, atitinkamos pereinamojo laikotarpio nuostatos savaime nenustos galioti.

(82) Galiausiai, kalbant apie būsimą Jungtinės Karalystės tarptautinio perdavimo režimo raidą – priimant naujas tinkamumo taisykles, sudarant tarptautinius susitarimus arba plėtojant kitus perdavimo mechanizmus – Komisija atidžiai stebės padėtį ir vertins, ar įvairūs perdavimo mechanizmai naudojami visais atvejais užtikrinant reikiamą apsaugą, ir, jei ji užtikrinama nenuosekliai, prireikus imsis atitinkamų priemonių galimam neigiamam poveikiui pašalinti (žr. (278)–(287) konstatuojamąsias dalis). Kadangi ES ir Jungtinė Karalystė taiko panašias tarptautinio duomenų perdavimo taisykles, manoma, kad problemų taip pat būtų galima išvengti bendradarbiaujant, keičiantis informacija ir dalijantis patirtimi, be kita ko, tarp Informacijos komisaro ir EDAV.

2.5.8. *Atskaitomybė*

(83) Pagal atskaitomybės principą duomenis tvarkantys subjektai privalo nustatyti tinkamas technines ir organizacines priemones, kad veiksmingai laikytųsi savo duomenų apsaugos prievolių ir galėtų įrodyti (visų pirma kompetentingai priežiūros institucijai), kad jų laikosi.

(84) Reglamente (ES) 2016/679 numatytas atskaitomybės principas buvo paliktas galioti Jungtinės Karalystės BDAR 5 straipsnio 2 dalyje be jokių esminių pakeitimų, be to, tas pats pasakytina apie 24 straipsnį dėl duomenų valdytojo atsakomybės, 25 straipsnį dėl pritaikytosios ir standartizuotosios duomenų apsaugos ir 30 straipsnį dėl duomenų tvarkymo veiklos įrašų. Taip pat palikti galioti 35 ir 36 straipsniai dėl poveikio duomenų apsaugai vertinimo ir išankstinių konsultacijų su priežiūros institucija. Reglamento (ES) 2016/679 37–39 straipsniai dėl duomenų apsaugos pareigūnų paskyrimo ir užduočių Jungtinės Karalystės BDAR palikti galioti be jokių esminių pakeitimų. Be to, Reglamento (ES) 2016/679 40 ir 42 straipsnių dėl elgesio kodeksų ir sertifikavimo nuostatos buvo paliktos galioti Jungtinės Karalystės BDAR ([80]).

2.6. **Priežiūra ir vykdymo užtikrinimas**

2.6.1. *Nepriklausoma priežiūra*

(85) Siekiant užtikrinti, kad tinkamas duomenų apsaugos lygis būtų užtikrinamas praktiškai, reikalinga nepriklausoma priežiūros institucija, kuriai suteikti įgaliojimai stebėti, kaip laikomasi duomenų apsaugos taisyklių, ir užtikrinti, kad jų būtų laikomasi. Atlikdama savo pareigas ir naudodamasi savo įgaliojimais ši institucija turėtų veikti visiškai nepriklausomai ir nešališkai.

(86) Jungtinėje Karalystėje informacijos komisaras atsako už Jungtinės Karalystės BDAR ir 2018 m. DAA priežiūrą ir vykdymo užtikrinimą. Informacijos komisaras yra vienasmenis subjektas – atskiras juridinis asmuo, kurį sudaro vienas fizinis asmuo. Informacijos komisarui dirbti padeda biuras. 2020 m. kovo 31 d. Informacijos komisaro biure dirbo 768 nuolatiniai darbuotojai ([81]). Informacijos komisarui padeda Skaitmeninių, kultūros, žiniasklaidos ir sporto reikalų departamentas ([82]).

(87) Komisaro nepriklausomumas aiškiai nustatytas Jungtinės Karalystės BDAR 52 straipsnyje, kuris, palyginti su BDAR 52 straipsnio 1–3 dalimis, iš esmės nepakeistas. Vykdydamas savo užduotis ir įgyvendindamas savo įgaliojimus pagal Jungtinės Karalystės BDAR, komisaras privalo veikti visiškai nepriklausomai, išlikti nepriklausomas nuo

([80]) Prireikus šios nuorodos pakeičiamos nuorodomis į Jungtinės Karalystės institucijas. Pavyzdžiui, pagal 2018 m. DAA 17 straipsnį informacijos komisaras arba Jungtinės Karalystės nacionalinė akreditacijos įstaiga gali suteikti akreditaciją asmeniui stebėti, kaip laikomasi sertifikavimo procedūros, jeigu jis atitinka Jungtinės Karalystės BDAR 43 straipsnyje nustatytus reikalavimus.

([81]) Informacijos komisaro 2019–2020 m. metinę ataskaitą ir finansines ataskaitas galima rasti šiuo adresu: https://ico.org.uk/media/about-the-ico/documents/2618021/annual-report-2019-20-v83-certified.pdf.

([82]) Susitarime dėl valdymo reglamentuojami abiejų subjektų santykiai. Visų pirma pagrindinės DCMS, kaip pagalbinio departamento, pareigos yra: užtikrinti, kad informacijos komisaras gautų tinkamą finansavimą ir pakankamai išteklių; atstovauti informacijos komisaro interesams parlamente ir kituose vyriausybės departamentuose; užtikrinti patikimos nacionalinės duomenų apsaugos sistemos galiojimą ir teikti gaires bei paramą Informacijos komisaro biurui organizaciniais klausimais, pvz., susijusiais su nekilnojamuoju turtu, išperkamąja nuoma ir viešaisiais pirkimais (2018–2021 m. Susitarimas dėl valdymo, galima rasti šiuo adresu: https://ico.org.uk/media/about-the-ico/documents/2259800/management-agreement-2018-2021.pdf).

tiesioginės ar netiesioginės išorės įtakos, atsižvelgiant į tas užduotis ir įgaliojimus, taip pat neturėtų siekti gauti nurodymų iš kokių nors asmenų ar jais vadovautis. Komisaras taip pat privalo neatlikti jokių veiksmų, nesuderinamų su jo pareigomis, ir eidamas pareigas negali užsiimti jokia kita nesuderinama profesija, nepaisant to, ar už ją mokamas atlygis, ar ne.

(88) Informacijos komisaro skyrimo ir pašalinimo iš pareigų sąlygos nustatytos 2018 m. DAA 12 priede. Informacijos komisarą skiria Jos Didenybė, atsižvelgdama į vyriausybės rekomendaciją, ir paskelbdama sąžiningą ir atvirą konkursą. Kandidatas privalo turėti tinkamą kvalifikaciją, įgūdžius ir kompetenciją. Pagal Valstybės pareigūnų valdymo kodeksą ([83]) skiriamų kandidatų sąrašą sudaro patariamojo vertintojų kolegija. Prieš Skaitmeninių, kultūros, žiniasklaidos ir sporto reikalų departamentui priimant galutinį sprendimą, atitinkamas parlamento atskirasis komitetas privalo atlikti patikrinimą iki paskyrimo. Komiteto nuomonė skelbiama viešai ([84]).

(89) Informacijos komisaro kadencija trunka septynerius metus. Asmuo negali eiti informacijos komisaro pareigų dvi kadencijas iš eilės. Informacijos komisarą iš pareigų pašalinti gali Jos Didenybė, remdamasi abiejų parlamento rūmų prašymu ([85]). Nė vienam iš parlamento rūmų negalima pateikti prašymo atleisti iš pareigų informacijos komisarą, kol ministras nepateikė ataskaitos, kurioje nurodoma, kad jis yra įsitikinęs, jog informacijos komisaras yra kaltas dėl šiurkštaus nusižengimo ir (arba) komisaras nebeatitinka sąlygų, keliamų komisaro funkcijų vykdymui ([86]).

(90) Informacijos komisaro veikla finansuojama iš trijų šaltinių: i) duomenų valdytojų sumokamų duomenų apsaugos mokesčių, kurie nustatomi valstybės sekretoriaus taisyklėse ([87]) (2018 m. Duomenų apsaugos (mokesčiai ir informacija) taisyklės) ir sudaro 85–90 proc. metinio biuro biudžeto ([88]); ii) dotacijos forma vyriausybės informacijos komisarui sumokėtos pagalbos. Dotacijos forma sumokėta pagalba iš esmės naudojama informacijos komisaro veiklos išlaidoms, kurios patiriamos vykdant su duomenų apsauga nesusijusias užduotis, sumokėti ([89]), ir iii) už paslaugas sumokėtų mokesčių ([90]). Dabar tokie mokesčiai apskritai nerenkami.

(91) Informacijos komisaro bendrosios funkcijos, susijusios su asmens duomenų, kuriems taikomas Jungtinės Karalystės BDAR, tvarkymu, nustatytos Jungtinės Karalystės BDAR 57 straipsnyje, kuris yra beveik identiškas atitinkamoms Reglamento (ES) 2016/679 taisyklėms. Tarp jo funkcijų – Jungtinės Karalystės BDAR stebėsena ir vykdymo užtikrinimas, visuomenės informavimo skatinimas, duomenų subjektų pateiktų skundų nagrinėjimas, tyrimų atlikimas ir pan. Be to, 2018 m. DAA 115 straipsnyje nustatytos kitos bendrosios komisaro funkcijos, tarp kurių – pareiga konsultuoti parlamentą, vyriausybę ir kitas institucijas bei įstaigas teisės aktų ir administracinių priemonių,

([83]) Valstybės pareigūnų skyrimo valdymo kodeksas, galima rasti šiuo adresu: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/578498/governance_code_on_public_appointments_16_12_2016.pdf.

([84]) 2015–2016 m. Skaitmeninių, kultūros, žiniasklaidos ir sporto reikalų departamento sesijos Bendruomenių Rūmuose antroji ataskaita, galima rasti šiuo adresu: https://publications.parliament.uk/pa/cm201516/cmselect/cmcumeds/990/990.pdf.

([85]) Kreipimasis – tai parlamentui pateiktas prašymas, kuriuo siekiama informuoti monarchą apie parlamento nuomones konkrečiu klausimu.

([86]) 2018 m. DAA 12 priedo 3 dalies 3 punktas.

([87]) 2018 m. DAA 137 straipsnis, žr. (17) konstatuojamąją dalį.

([88]) 2018 m. DAA 137 ir 138 straipsniuose numatytos įvairios apsaugos priemonės, kuriomis siekiama užtikrinti, kad nustatyti mokesčiai būtų tinkamo dydžio. Visų pirma 137 straipsnio 4 dalyje išvardijami klausimai, į kuriuos valstybės sekretorius privalo atsižvelgti priimdamas taisykles, kuriose nurodoma suma, kurią privalo sumokėti įvairios organizacijos. Antra, 2018 m. DAA 138 straipsnio 1 dalyje ir 182 straipsnyje valstybės sekretoriui taip pat nustatytas teisinis reikalavimas konsultuotis su informacijos komisaru ir kitais asmenų, kuriems taisyklės gali daryti poveikį, atstovais ir taisykles priimti atsižvelgus į jų nuomones. Be to, pagal 2018 m. DAA 138 straipsnio 2 dalį reikalaujama, kad informacijos komisaras taikomas mokesčių taisykles nuolat peržiūrėtų, be to, jis gali pateikti valstybės sekretoriui pasiūlymus pakeisti taisykles. Galiausiai, išskyrus atvejus, kai taisyklės priimamos siekiant atsižvelgti į padidėjusį mažmeninių kainų indeksą (tokiu atveju, joms bus taikoma neigiama rezoliucijos procedūra), taisyklėms taikoma patvirtinamoji rezoliucijos procedūra ir jos negali būti priimtos tol, kol jų savo rezoliucija nepatvirtino kiekvieni parlamento rūmai.

([89]) Susitarime dėl valdymo paaiškinta, kad „valstybės sekretorius gali atlikti mokėjimus informacijos komisarui naudodamas parlamento numatytus pinigus pagal 2018 m. DAA 12 priedo 9 dalį. Pasikonsultavęs su informacijos komisaru, DCMS sumokės Informacijos komisaro biurui atitinkamas sumas (dotaciją pagalbos forma) už informacijos komisaro administracines išlaidas ir funkcijų, susijusių su įvairiomis konkrečiomis užduotimis, vykdymą, įskaitant informacijos laisvę“ (2018–2021 m. susitarimo dėl valdymo 1.12 dalis, žr. 82 išnašą).

([90]) Žr. 2018 m. DAA 134 straipsnį.

susijusių su asmenų teisių ir laisvių apsauga tvarkant asmens duomenis, klausimais, ir įgaliojimai komisaro iniciatyva arba paprašius priimti parlamentui, vyriausybei ir kitoms institucijoms ir įstaigoms bei visuomenei skirtas nuomones bet kuriuo su asmens duomenų apsauga susijusiu klausimu. Siekiant išlaikyti teismų nepriklausomumą, informacijos komisarui neleidžiama vykdyti savo funkcijų tais atvejais, kai asmens duomenis tvarko teisminius įgaliojimus turintis fizinis asmuo arba teismines funkcijas vykdantis bendrosios kompetencijos arba specializuotas teismas. Tačiau teismų priežiūrą užtikrina specializuotos įstaigos (žr. (99)–(103) konstatuojamąsias dalis).

2.6.2. *Vykdymo užtikrinimas, įskaitant sankcijas*

(92) Informacijos komisaro įgaliojimai išdėstyti Jungtinės Karalystės BDAR 58 straipsnyje, kuriame nėra jokių esminių pakeitimų, palyginti su atitinkamu Reglamento (ES) 2016/679 straipsniu. 2018 m. DAA nustatytos papildomos taisyklės, kuriose apibūdinti šių įgaliojimų įgyvendinimo būdai. Komisaras turi įgaliojimus visų pirma: a) įpareigoti duomenų valdytoją ir duomenų tvarkytoją (ir tam tikrais atvejais bet kurį kitą asmenį) pateikti būtiną informaciją informacinio pranešimo forma („informacinis pranešimas“ ([91]); b) atlikti tyrimus ir auditus ir pateikti vertinimo pranešimą, kuriame gali reikalauti, kad duomenų valdytojas arba duomenų tvarkytojas leistų komisarui patekti į konkrečias patalpas, patikrinti arba išnagrinėti dokumentus arba patikrinti ir apžiūrėti įrangą, duomenų valdytojų vardu apklausti asmens duomenis tvarkančius asmenis („vertinimo pranešimas“) ([92]); c) kitais būdais gauti prieigą prie duomenų valdytojų ir duomenų tvarkytojų dokumentų ir patekti į jų patalpas pagal 2018 m. DAA 154 straipsnį („įgaliojimai patekti į patalpas ir atlikti patikrinimą“); d) įgyvendinti taisomuosius įgaliojimus, įskaitant įspėjimų arba papeikimų skyrimą, arba duoti nurodymus parengtame vykdymo pranešime, kuriame reikalaujama, kad duomenų valdytojai / duomenų tvarkytojai imtųsi konkrečių veiksmų arba jų nesiimtų, įskaitant nurodymą duomenų valdytojui arba duomenų tvarkytojui atlikti bet kurį Jungtinės Karalystės BDAR 58 straipsnio 2 dalies c–g ir j punktuose nurodytą veiksmą („vykdymo pranešimas“) ([93]), ir e) skirti administracines baudas paskelbdamas pranešimą apie nuobaudą („pranešimas apie nuobaudą“) ([94]). Šis dokumentas gali būti išduotas ir tuo atveju, jei valdžios institucija nesilaikė Jungtinės Karalystės BDAR nuostatų ([95]).

(93) Informacijos komisaro reguliavimo veiksmų plane aprašytos aplinkybės, kuriomis jis priima informacinį, vertinimo, vykdymo pranešimą arba pranešimą apie nuobaudą ([96]). Vykdymo pranešime, pateiktame reaguojant į duomenų valdytojo arba duomenų tvarkytojo klaidą, gali būti tik nustatyti reikalavimai, kurie, komisaro manymu, yra tinkami siekiant ištaisyti klaidą. Vykdymo pranešimas ir pranešimas apie nuobaudą gali būti priimami tik dėl duomenų valdytojo arba duomenų tvarkytojo padarytų Jungtinės Karalystės BDAR II skyriaus (duomenų tvarkymo principai), 12–22 straipsnių (duomenų subjekto teisės), 25–39 straipsnių (duomenų valdytojų ir duomenų tvarkytojų pareigos) ir 44–49 straipsnių (tarptautiniai duomenų perdavimai) pažeidimų. Vykdymo pranešimas taip pat gali būti teikiamas, jeigu duomenų valdytojas nesilaikė reikalavimo sumokėti mokesčio, nustatyto pagal 2018 m. DAA 137 straipsnį priimtose taisyklėse. Be to, vykdymo pranešimas gali būti pateikiamas stebėsenos įstaigai pagal 41 straipsnį arba sertifikavimo paslaugų teikėjui, jeigu jie nesilaiko savo pareigų pagal Jungtinės Karalystės BDAR. Pranešimas apie nuobaudą taip pat gali būti įteikiamas asmeniui, kuris nesilaikė informacinio pranešimo, vertinimo pranešimo arba vykdymo pranešimo.

(94) Pranešime apie nuobaudą reikalaujama, kad asmuo sumokėtų informacijos komisarui pranešime nurodytą sumą. Nuspręsdamas, ar asmeniui įteikti pranešimą apie nuobaudą, ir nustatydamas nuobaudos dydį, informacijos komisaras privalo atsižvelgti į Jungtinės Karalystės BDAR 83 straipsnio 1 ir 2 dalyse išvardytus aspektus, kurie yra identiški Reglamente (ES) 2016/679 nustatytoms atitinkamoms taisyklėms ([97]). Pagal 83 straipsnio 4 ir 5 dalis

([91]) 2018 m. DAA 142 straipsnis (taikomi 2018 m. DAA 143 straipsnyje nustatyti apribojimai).
([92]) 2018 m. DAA 146 straipsnis (taikomi 2018 m. DAA 147 straipsnyje nustatyti apribojimai).
([93]) 2018 m. DAA 149–151 straipsniai (taikomi 2018 m. DAA 152 straipsnyje nustatyti apribojimai).
([94]) 2018 m. DAA 155 straipsnis ir JK BDAR 83 straipsnis.
([95]) Tai matyti iš 2018 m. DAA 155 straipsnio 1 dalies, siejamos su 2018 m. DAA 149 straipsnio 2 ir 5 dalimis, ir iš 2018 m. DAA 156 straipsnio 4 dalies, pagal kurią pranešimų apie nuobaudas išdavimas taikant 2018 m. DAA 209 straipsnio 4 dalį ribojamas tik Karūnos turto valdybos ir Karališkųjų rūmų valdytojų atžvilgiu.
([96]) Reguliavimo veiksmų politika, galima rasti šiuo adresu: https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf.
([97]) Įskaitant pažeidimo pobūdį ir rimtumą (atsižvelgiant į atitinkamų duomenų tvarkymo pobūdį, mastą arba tikslą, taip pat į nukentėjusių duomenų subjektų skaičių ir jų patirtos žalos dydį), tyčinį arba netyčinį pažeidimo pobūdį, bet kokius veiksmus, kurių duomenų valdytojas ėmėsi, siekdamas sumažinti duomenų subjektų patirtą žalą, duomenų valdytojo arba duomenų tvarkytojo atsakomybės laipsnį (atsižvelgiant į duomenų valdytojo arba duomenų tvarkytojo įgyvendintas technines ir organizacines priemones), bet kokį atitinkamą ankstesnį duomenų valdytojo ar duomenų tvarkytojo pažeidimą; bendradarbiavimo su komisaru laipsnį, asmens duomenų kategorijas, susijusias su pažeidimu, bet kurias kitas atsakomybę sunkinančias arba švelninančias bylos aplinkybes, pvz., dėl pažeidimo gauta tiesioginė arba netiesioginė finansinė nauda arba išvengtų nuostolių dydis.

didžiausia administracinių baudų už tose nuostatose nurodytų pareigų nesilaikymą suma atitinkamai yra 8 700 000 arba 17 500 000 GBP. Jeigu pažeidimą padaro įmonė, informacijos komisaras, skirdamas baudas, taip pat gali nurodyti, kad jos dydis atitinka pasaulinės metinės apyvartos procentinę dalį, jei ji didesnė. Kaip ir lygiavertėse Reglamento (ES) 2016/679 nuostatose, šios sumos 83 straipsnio 4 ir 5 dalyse atitinkamai sudaro 2 proc. ir 4 proc. Jeigu nesilaikoma informacinio pranešimo, vertinimo pranešimo arba vykdymo pranešimo reikalavimų, didžiausia nuobaudos, kurią galima skirti įteikiant pranešimą apie nuobaudą, yra 17 500 000 GBP arba įmonės atveju – 4 proc. pasaulinės metinės apyvartos, priklausomai nuo to, kuri suma yra didesnė.

(95) Jungtinės Karalystės BDAR ir 2018 m. DAA taip pat sustiprinti kiti informacijos komisaro įgaliojimai. Pavyzdžiui, komisaras dabar gali atlikti privalomus visų duomenų valdytojų ir duomenų tvarkytojų auditus naudodamas vertinimo pranešimus, o pagal ankstesnius teisės aktus, t. y. 1998 m. Duomenų apsaugos aktą, komisarui šie įgaliojimai buvo suteikti tik dėl centrinės valdžios ir sveikatos organizacijų, o kiti subjektai turėjo duoti sutikimą būti audituojami.

(96) Nuo Reglamento (ES) 2016/679 įsigaliojimo informacijos komisaras kasmet išnagrinėja apytiksliai 40 000 duomenų subjektų skundų ([98]) ir, , be kita ko, atlieka apytiksliai 2 000 *ex officio* tyrimų ([99]). Dauguma skundų yra susiję su teisėmis susipažinti ir duomenų atskleidimu. Atsižvelgdamas į savo tyrimus, komisaras įvairiuose sektoriuose imasi vykdymo priemonių. Konkrečiau, remiantis naujausia Informacijos komisaro (2019–2020 m.) metine ataskaita ([100]), ataskaitiniu laikotarpiu komisaras priėmė 54 informacijos pranešimus, 8 vertinimo pranešimus, 7 vykdymo pranešimus, 4 įspėjimus, 8 pranešimus dėl patraukimo atsakomybėn ir 15 pranešimų dėl baudų ([101]).

(97) Šiuo atveju taip pat skirtos kelios didelės baudos pagal Reglamentą (ES) 2016/679 ir 2018 m. DAA. Visų pirma 2020 m. spalio mėn. informacijos komisaras Didžiosios Britanijos oro bendrovei skyrė 20 mln. GBP baudą už duomenų apsaugos pažeidimą, nuo kurio nukentėjo daugiau nei 400 000 klientų. 2020 m. spalio pabaigoje tarptautiniam viešbučių tinklui skirta 18,4 mln. GBP bauda už tai, kad jis neužtikrino milijonų klientų asmens duomenų saugumo, o 2020 m. lapkričio mėn. Didžiosios Britanijos paslaugų teikėjui, internete parduodančiam bilietus į renginius, buvo skirta 1,25 mln. GBP bauda už tai, kad jis neapsaugojo klientų mokėjimų duomenų ([102]).

(98) Be informacijos komisarui suteiktų vykdymo įgaliojimų, kurie aprašyti (92) konstatuojamojoje dalyje, tam tikri duomenų apsaugos teisės aktų pažeidimai laikomi nusikalstamomis veikomis, todėl už jų padarymą gali būti skiriamos baudžiamosios sankcijos (2018 m. DAA 196 straipsnis). Tai taikoma, pvz., kai sąmoningai arba dėl neatsargumo gaunami arba atskleidžiami asmens duomenys be duomenų valdytojo sutikimo, sudaromos sąlygos be duomenų valdytojo sutikimo atskleisti asmens duomenis kitam asmeniui ([103]), iš naujo nustatoma informacija, kuri yra nuasmeninti asmens duomenys, be duomenų valdytojo, atsakingo už asmens duomenų nuasmeninimą, sutikimo ([104]), tyčia trukdoma komisarui įgyvendinti savo įgaliojimus, susijusius su asmens duomenų patikrinimu laikantis tarptautinių pareigų ([105]), pateikiami neteisingi pareiškimai atsakant į informacinį pranešimą arba sunaikinama su informaciniu pranešimu ir vertinimo pranešimu susijusi informacija ([106]).

([98]) Remiantis Jungtinės Karalystės institucijų pateikta informacija, Informacijos komisaro 2019–2020 m. metinėje ataskaitoje aptariamu laikotarpiu 25 proc. bylų nenustatytas joks pažeidimas, apytiksliai 29 proc. bylų duomenų subjekto buvo prašoma spręsti klausimą iš pradžių kreipiantis į duomenų valdytoją, sulaukti duomenų valdytojo atsakymo arba tęsti dialogą su duomenų valdytoju, apytiksliai 17 proc. bylų pažeidimas apskritai nenustatytas, tačiau duomenų valdytojui buvo duotas patarimas, apie 25 proc. bylų informacijos komisaras nustatė pažeidimą ir pateikė duomenų valdytojui rekomendaciją arba duomenų valdytojo paprašyta imtis tam tikrų veiksmų, apie 3 proc. bylų buvo nustatyta, kad skundas nepatenka į Reglamento (ES) 2016/679 taikymo sritį, o apytiksliai 1 proc. bylų buvo perduotos kitai duomenų apsaugos institucijai, priklausančiai Europos duomenų apsaugos valdybos sistemai.

([99]) Informacijos komisaras tuos tyrimus gali inicijuoti remdamasis iš įvairių šaltinių, įskaitant pranešimus apie duomenų saugumo pažeidimus, kitų Jungtinės Karalystės valdžios institucijų arba užsienio duomenų apsaugos institucijų perduotus dokumentus ir fizinių asmenų arba pilietinės visuomenės organizacijų skundus, gauta informacija.

([100]) Informacijos komisaro 2019–2020 m. metinė ataskaita ir finansinės ataskaitos (žr. 81išnašą).

([101]) Remiantis ankstesne 2018–2019 m. laikotarpio metine ataskaita, informacijos komisaras ataskaitiniu laikotarpiu pagal 1998 m. DAA priėmė 22 pranešimus apie nuobaudą, kuriais iš viso skirta 3 010 610 GBP baudų, įskaitant dvi baudas po 500 000 GBP (t. y. didžiausia leistina baudos suma pagal 1998 m. DAA). 2018 m. informacijos komisaras po „Cambridge Analytica“ atskleistos informacijos visų pirma visų pirma atliko duomenų analitikos naudojimo politiniais tikslais tyrimą. Atlikus tyrimą, buvo parengta politikos ataskaita, rekomendacijų rinkinys, „Facebook“ skirta 500 000 GBP bauda, o Kanados duomenų tarpininkui įteiktas vykdymo pranešimas, kuriame įmonei liepiama ištrinti turimus duomenis apie Jungtinės Karalystės piliečius ir gyventojus (žr. Informacijos komisaro 2018–2019 m. metinę ataskaitą ir finansines ataskaitas, galima rasti šiuo adresu: https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf).

([102]) Vykdymo veiksmų, kurių buvo imtasi, santrauka pateikiama informacijos komisaro svetainėje, galima rasti šiuo adresu: https://ico.org.uk/action-weve-taken/enforcement/.

([103]) 2018 m. DAA 170 straipsnis.

([104]) 2018 m. DAA 171 straipsnis.

([105]) 2018 m. DAA 119 straipsnis.

([106]) 2018 m. DAA 144 ir 148 straipsniai.

2.6.3. *Teismų vykdoma priežiūra*

(99) Teismų ir teisminių institucijų vykdomo asmens duomenų tvarkymo priežiūra yra dvejopa. Jeigu teisėjo pareigas einantis asmuo arba teismas veikia neturėdamas teisminių įgaliojimų, priežiūrą vykdo informacijos komisaras. Jeigu duomenų valdytojas veikia turėdamas teisminius įgaliojimus, Informacijos komisaras negali vykdyti savo priežiūros funkcijų ([107]), o priežiūrą vykdo specialios įstaigos. Šis požiūris atsispindi Reglamente (ES) 2016/679 (55 straipsnio 3 dalis).

(100) Visų pirma pažymėtina, kad antruoju atveju Anglijos ir Velso teismų ir Anglijos ir Velso pirmosios ir aukštesnės instancijos specializuotų teismų priežiūrą atlieka Teisminė duomenų apsaugos kolegija ([108]). Be to, lordas vyriausiasis teisėjas ir vyresnysis specializuotų teismų pirmininkas paskelbtame pareiškime dėl privatumo ([109]) nurodo, kaip Anglijos ir Velso teismai tvarko asmens duomenis teisminių funkcijų vykdymo tikslais. Panašų pranešimą yra paskelbę Šiaurės Airijos ([110]) ir Škotijos teisėjai ([111]).

(101) Be to, Šiaurės Airijoje Šiaurės Airijos lordas vyriausiasis teisėjas paskyrė Aukštojo teismo teisėją eiti už duomenų priežiūrą atsakingo teisėjo pareigas ([112]). Jis taip pat paskelbė Šiaurės Airijos teisėjams skirtas gaires dėl veiksmų, kurių reikia imtis praradus duomenis arba tuo atveju, jeigu jie gali būti prarasti, ir gaires dėl to, kokia tvarka reikia spręsti visus su tuo susijusius klausimus ([113]).

(102) Škotijoje lordas pirmininkas paskyrė už duomenų priežiūrą atsakingą teisėją tirti bet kokius skundus, kurie teikiami remiantis su duomenų apsauga susijusiais pagrindais. Tai nustatyta teisminio skundų nagrinėjimo taisyklėse, kurios yra identiškos Anglijoje ir Velse nustatytoms taisyklėms ([114]).

(103) Galiausiai Aukščiausiajame Teisme vienam iš jo teisėjų pavedama duomenų apsaugos priežiūros funkcija.

2.6.4. *Teisių gynimas*

(104) Siekiant užtikrinti tinkamą apsaugą ir, visų pirma, individualių teisių įgyvendinimą, duomenų subjektui turėtų būti suteikta veiksmingų administracinių ir teisminių teisių gynimo priemonių, įskaitant kompensaciją už patirtą žalą.

---

([107]) 2018 m. DAA 117 straipsnis.

([108]) Kolegija privalo teikti rekomendacijas teisėjams ir juos mokyti. Ji taip pat nagrinėja duomenų subjektų skundus, susijusius su bendrosios kompetencijos teismų, specializuotų teismų ir fizinių asmenų, vykdančių teisminės funkcijas, tvarkomais asmens duomenimis. Kolegija siekia suteikti priemones, kuriomis būtų galima išspręsti bet kurį skundą. Jeigu skundo pateikėjas nebuvo patenkintas kolegijos sprendimu ir pateikė papildomus įrodymus, kolegija gali pakartotinai nagrinėti jo skundą. Pati kolegija finansinių sankcijų neskiria, tačiau jeigu ji mano, kad buvo padarytas pakankamai šiurkštus 2018 m. DAA pažeidimas, ji bylą gali perduoti Teisėjų elgesio tyrimo biurui (angl. JCIO), kuris išnagrinės skundą. Jeigu skundas tenkinamas, sprendimą dėl veiksmų, kurių reikėtų imtis pareigūno atžvilgiu, priima lordas kancleris arba vyriausiasis teisėjas (jo vardu deleguotas arba vyresnysis teisėjas). Tai galėtų būti (pagal griežtumą): oficialus patarimas, oficialius įspėjimas ir papeikimas, ir galiausiai pašalinimas iš pareigų. Jeigu fizinis asmuo nepatenkintas tuo, kaip JCIO išnagrinėjo skundą, jis gali toliau skųstis Teisėjų skyrimo ir elgesio ombudsmenui (žr. https://www.gov.uk/government/organisations/judicial-appointments-and-conduct-ombudsman). Ombudsmenas turi įgaliojimus prašyti JCIO iš naujo ištirti skundą ir gali pasiūlyti skundo pateikėjui sumokėti kompensaciją, jeigu mano, kad dėl netinkamo administravimo jis patyrė žalą.

([109]) Lordo vyriausiojo teisėjo ir vyriausiojo specializuotų teismų pirmininko pareiškimą dėl privatumo galima rasti šiuo adresu: https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice

([110]) Šiaurės Airijos lordo vyriausiojo teisėjo paskelbtą pareiškimą dėl privatumo galima rasti šiuo adresu: https://judiciaryni.uk/data-privacy.

([111]) Škotijos bendrosios kompetencijos ir specializuotų teismų pareiškimą dėl privatumo galima rasti šiuo adresu: https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice

([112]) Už duomenų priežiūrą atsakingas teisėjas teikia teisėjams rekomendacijas ir tiria pažeidimus ir (arba) skundus, susijusius su teismų arba fizinių asmenų, kurie veikia turėdami teisminius įgaliojimus, tvarkomais asmens duomenimis.

([113]) Jeigu manoma, kad skundas arba pažeidimas yra rimtas, jis pagal Šiaurės Airijos lordo vyriausiojo teisėjo paskelbtą skundų nagrinėjimo praktikos kodeksą perduodamas toliau tirti teisminių skundų pareigūnui. Išnagrinėjus tokį skundą: tolesnių veiksmų apskritai gali būti nesiimama, gali būti duodamas patarimas arba skiriamas mentorius, įteikiamas neoficialus įspėjimas, oficialus įspėjimas, galutinis įspėjimas, nustatomi praktikos apribojimai arba byla perduodama specializuotam statutinių pareigūnų teismui. Šiaurės Airijos lordo vyriausiojo teisėjo paskelbtą skundų nagrinėjimo praktikos kodeksą galima rasti šiuo adresu: https://judiciaryni.uk/sites/judiciary/files/media-files/14G.%20CODE%20OF%20PRACTICE%20Judicial%20~%2028%20Feb%2013%20%28Final%29%20updated%20with%20new%20comp..__1.pdf

([114]) Bet kurį pagrįstą skundą tiria duomenų priežiūros teisėjas ir jis perduodamas lordui pirmininkui, kuris turi įgaliojimus pateikti patarimą, oficialų įspėjimą arba papeikimą, jei, jo manymu, tai yra būtina (lygiavertės taisyklės taikomos specializuoto teismo nariams ir jas galima rasti šiuo adresu: https://www.judiciary.scot/docs/librariesprovider3/judiciarydocuments/complaints/complaintsaboutthejudiciaryscotlandrules2017_1d392ab6e14f6425aa0c7f48d062f5cc5.pdf?sfvrsn=5d3eb9a1_2).

(105) Pirma, duomenų subjektas turi teisę pateikti skundą informacijos komisarui, jeigu mano, kad, atsižvelgiant į jo asmens duomenis, buvo padarytas Jungtinės Karalystės BDAR pažeidimas ([115]). Jungtinės Karalystės BDAR paliktos galioti Reglamento (ES) 2016/679 77 straipsnio taisyklės dėl tos teisės neatliekant jokių esminių pakeitimų. Tą patį galima pasakyti apie 57 straipsnio 1 dalies f punkto ir 2 dalies nuostatas, kuriose nustatytos komisaro užduotys, susijusios su skundų nagrinėjimu. Kaip aprašyta (92)–(98) above konstatuojamosiose dalyse, informacijos komisaras turi įgaliojimus įvertinti, ar duomenų valdytojas ir duomenų tvarkytojas laikosi Jungtinės Karalystės BDAR ir 2018 m. DAA, reikalauti, kad jie imtųsi būtinų veiksmų arba nesiimtų tokių veiksmų reikalavimų nesilaikymo atveju, ir skirti baudas.

(106) Antra, Jungtinės Karalystės BDAR ir 2018 m. DAA nustatyta teisė į teisinę gynybą prieš informacijos komisarą. Pagal Jungtinės Karalystės BDAR 78 straipsnio 1 dalį fizinis asmuo turi teisę imtis veiksmingų teisminių teisių gynimo priemonių prieš su juo susijusį privalomą komisaro sprendimą. Teisminės peržiūros atveju teisėjas nagrinėja ieškinyje ginčijamą sprendimą ir ar informacijos komisaras veikė teisėtai. Be to, pagal Jungtinės Karalystės BDAR 78 straipsnio 2 dalį, jeigu komisaras nesugeba tinkamai išnagrinėti duomenų subjekto pateikto skundo ([116]), skundo pateikėjas turi teisę imtis teisminių teisių gynimo priemonių. Jis gali kreiptis į specializuotą pirmosios instancijos teismą, kad komisaras būtų įpareigotas imtis tinkamų veiksmų, susijusių su skundo nagrinėjimu, arba informuotų skundo pateikėją apie skundo nagrinėjimo eigą ([117]). Be to, bet kuris asmuo, kuriam komisaras įteikia vieną iš minėtų pranešimų (informacinį, vertinimo ar vykdymo pranešimą arba pranešimą dėl nuobaudos), gali skųstis specializuotam pirmosios instancijos teismui ([118]). Jeigu specializuotas teismas mano, kad komisaro sprendimas neatitinka įstatymo arba kad informacijos komisaras turėjo kitaip pasinaudoti savo diskrecija, specializuotas teismas privalo priimti skundą arba pakeisti kitą pranešimą arba sprendimą, kurį pateikė arba priėmė informacijos komisaras.

(107) Trečia, asmenys gali pasinaudoti teisminėmis teisių gynimo priemonėmis prieš duomenų valdytojus ir duomenų tvarkytojus tiesiogiai kreipdamiesi į teismus pagal Jungtinės Karalystės BDAR 79 straipsnį ir 2018 m. DAA 167 straipsnį. Jeigu, atsižvelgdamas į duomenų subjekto prašymą, teismas įsitikina, kad buvo pažeistos duomenų apsaugos teisės aktuose nustatytos duomenų subjekto teisės, teismas gali įpareigoti duomenų valdytoją arba jo vardu veikiantį duomenų tvarkytoją imtis nutartyje nurodytų veiksmų dėl duomenų tvarkymo arba nesiimti nutartyje nurodytų veiksmų.

(108) Be to, pagal Jungtinės Karalystės BDAR 82 straipsnį ir 2018 m. DAA 168 straipsnį bet kuris asmuo, kuris dėl Jungtinės Karalystės BDAR pažeidimo patyrė materialinę arba nematerialinę žalą, turi teisę iš duomenų valdytojo arba duomenų tvarkytojo gauti kompensaciją už patirtą žalą. Jungtinės Karalystės 82 straipsnio 1–5 dalyse nustatytos kompensacijos ir atsakomybės taisyklės yra identiškos Reglamento (ES) 2016/679 nustatytoms atitinkamoms taisyklėms. Pagal 2018 m. DAA 168 straipsnį nematerialinė žala taip pat reiškia stresą. Pagal Jungtinės Karalystės BDAR 80 straipsnį duomenų subjektas taip pat turi teisę įgalioti atstovaujančią įstaigą arba organizaciją jo vardu (pagal Jungtinės Karalystės BDAR 77 straipsnį) pateikti skundą komisarui ir jo vardu įgyvendinti Jungtinės Karalystės BDAR 78 straipsnyje (teisė imtis veiksmingų teisminių teisių gynimo priemonių prieš komisarą), 79 straipsnyje (teisė imtis veiksmingų teisminių teisių gynimo priemonių prieš duomenų valdytoją arba duomenų tvarkytoją) ir 82 straipsnyje (teisė į kompensaciją ir atsakomybę) nustatytas teises.

(109) Ketvirta, bet kuris asmuo, kuris mano, kad valdžios institucijos pažeidė jo teises, įskaitant teises į privatumą ir duomenų apsaugą, be pirmiau aprašytų numatytų teisių gynimo būdų, gali gintis Jungtinės Karalystės teismuose pagal 1998 m. Žmogaus teisių aktą ([119]). Asmuo, kuris teigia, kad valdžios institucija veikė (arba siūlo veikti) su Konvencijos teise nesuderinamu būdu, taip pažeidžiant 1998 m. Žmogaus teisių akto 6 straipsnio 1 dalį, atitinkamame bendrosios kompetencijos arba specializuotame teisme gali iškelti institucijai bylą arba bet kuriame teisminiame procese remtis atitinkamomis teisėmis, kai jis tapo (arba galėjo tapti) neteisėto veiksmo auka.

(110) Jeigu teismas nustato, kad kuris nors valdžios institucijos veiksmas yra neteisėtas, jis, atsižvelgdamas į savo įgaliojimus, gali nustatyti jo manymu teisingą ir tinkamą teisių gynimo priemonę arba priimti jo manymu teisingą ir tinkamą nutartį ([120]). Teismas taip pat gali pirminės teisės akto nuostatą paskelbti nesuderinama su Konvencijoje nustatyta teise.

---

([115]) Jungtinės Karalystės BDAR 77 straipsnis.

([116]) 2018 m. DAA 166 straipsnyje konkrečiai nurodyti šie atvejai: a) komisaras nesiima tinkamų veiksmų, kad reaguotų į skundą, b) komisaras nepateikia skundo pateikėjui informacijos apie skundo nagrinėjimo eigą arba rezultatą prieš pasibaigiant 3 mėnesių terminui, kuris pradedamas skaičiuoti nuo dienos, kurią komisaras gavo skundą, arba c) jeigu komisaras, per tą terminą nebaigęs nagrinėti skundo, nepateikia skundo pateikėjui tokios informacijos per paskesnį 3 mėnesių terminą.

([117]) Jungtinės Karalystės BDAR 78 straipsnio 2 dalis ir 2018 m. DAA 166 straipsnis.

([118]) Jungtinės Karalystės BDAR 78 straipsnio 1 dalis ir 2018 m. DAA 162 straipsnis.

([119]) 1998 m. Žmogaus teisių akto 7 straipsnio 1 dalis. Pagal 7 straipsnio 7 dalį laikoma, kad asmuo yra neteisėto veiksmo auka, jeigu jis tapo auka pagal Europos žmogaus teisių konvencijos 34 straipsnį ir dėl to veiksmo buvo pradėta byla Europos Žmogaus Teisių Teisme.

([120]) 1998 m. Žmogaus teisių akto 8 straipsnio 1 dalis.

(111) Galiausiai, išnaudojęs nacionalines teisių gynimo priemones, fizinis asmuo dėl Europos žmogaus teisių konvencijoje garantuojamų žmogaus teisių pažeidimų, susijusių su jo teisėmis, gali kreiptis į Europos Žmogaus Teisių Teismą.

### 3. JUNGTINĖS KARALYSTĖS VALDŽIOS INSTITUCIJŲ SUSIPAŽINIMAS SU ASMENS DUOMENIMIS, PERDUOTAIS IŠ EUROPOS SĄJUNGOS, IR JŲ NAUDOJIMAS

(112) Komisija taip pat įvertino Jungtinės Karalystės asmens duomenų, kuriuos Jungtinės Karalystės valdžios institucijos, atsižvelgdamos į viešąjį interesą, visų pirma baudžiamosios teisės vykdymą ir nacionalinio saugumo tikslus, perdavė Jungtinės Karalystės ekonominės veiklos vykdytojams, rinkimo ir paskesnio naudojimo teisinę sistemą (toliau – vyriausybės prieiga). Vertindama, ar sąlygos, kuriomis vyriausybė gauna prieigą prie duomenų, perduotų Jungtinei Karalystei pagal šį sprendimą, atitiktų „esminio lygiavertiškumo“ kriterijų pagal Reglamento (ES) 2016/679 45 straipsnio 1 dalį, kaip jį išaiškino Europos Sąjungos Teisingumo Teismas, atsižvelgdamas į Pagrindinių teisių chartiją, Komisija visų pirma atsižvelgė į toliau išvardytus kriterijus.

(113) Pirma, bet koks teisės į duomenų apsaugą apribojimas turi būti numatytas įstatyme, o pačiame teisiniame pagrinde, kuriuo remiantis leidžiama apriboti tokią teisę, turi būti apibrėžta apribojimo taikymo atitinkamos teisės įgyvendinimui sritis ([121]).

(114) Antra, siekiant įvykdyti proporcingumo reikalavimą, pagal kurį nuo asmens duomenų apsaugos nukrypti leidžiančios nuostatos ir asmens duomenų apsaugos apribojimai turi būti taikomi tik tiek, kiek tai griežtai būtina demokratinėje visuomenėje siekiant konkrečių viešojo intereso tikslų, kurie yra lygiaverčiai Sąjungos pripažįstamiems tikslams, atitinkamos trečiosios valstybės, kurioje leidžiami apribojimai, teisės aktuose turi būti nustatytos aiškios ir tikslios taisyklės, kuriomis reglamentuojamas atitinkamų priemonių mastas ir taikymas, ir nustatomos būtinosios apsaugos priemonės, kad asmenys, kurių duomenys buvo perduoti, turėtų pakankamai garantijų ir galėtų veiksmingai apsaugoti savo asmens duomenis nuo piktnaudžiavimo rizikos ([122]). Teisės akte visų pirma turi būti nurodyta, kokiomis aplinkybėmis ir sąlygomis galima priimti priemonę, kurią įgyvendinant numatyta tvarkyti tokius duomenis ([123]), taip pat tokiai priemonei taikomi nepriklausomos priežiūros reikalavimai ([124]).

(115) Trečia, tas teisės aktas turi būti teisiškai įpareigojantis pagal vidaus teisę ir šie teisiniai reikalavimai turi būti privalomi ne tik institucijoms, bet ir įvykdomi teismuose atitinkamų trečiosios valstybės institucijų atžvilgiu ([125]). Visų pirma, duomenų subjektai privalo turėti galimybę pareikšti ieškinį nepriklausomame ir nešališkame teisme, kad galėtų susipažinti su asmens duomenimis arba kad jiems būtų suteikta teisė ištaisyti arba ištrinti tokius duomenis ([126]).

#### 3.1. Bendroji teisinė sistema

(116) Vyriausybės prieiga prie duomenų Jungtinėje Karalystėje, atsižvelgiant į valdžios institucijos įgaliojimų įgyvendinimą, turi būti užtikrinama visapusiškai laikantis teisės aktų. Jungtinė Karalystė yra ratifikavusi Europos žmogaus teisių konvenciją (žr. (9) konstatuojamąją dalį) ir visos Jungtinės Karalystės valdžios institucijos privalo veikti laikydamosi Konvencijos ([127]). Konvencijos 8 straipsnyje nustatyta, kad bet koks privatumo apribojimas turi atitikti teisės aktus, derėti su vienu iš 8 straipsnio 2 dalyje nustatytų tikslų ir būti proporcingas atsižvelgiant į tą tikslą. Pagal 8 straipsnį taip pat reikalaujama, kad apribojimas būtų „prognozuojamas“, t. y. jo pagrindas turi būti aiškiai numatytas teisės akte, su kuriuo galima susipažinti, ir kad teisės akte būtų nustatytos tinkamos apsaugos nuo piktnaudžiavimo priemonės.

(117) Be to, savo jurisprudencijoje Europos Žmogaus Teisių Teismas konkrečiai nurodė, kad kiekvienam teisės į privatumą ir duomenų apsaugą apribojimui turėtų būti taikoma veiksminga, nepriklausoma ir nešališka priežiūros sistema, kurią turi įgyvendinti teismas arba kita nepriklausoma įstaiga ([128]) (pvz., administracinė institucija arba parlamento organas).

---

([121]) Žr. Sprendimo *Schrems II*, 174–175 punktus ir juose minimą jurisprudenciją. Dėl valstybių narių valdžios institucijų galimybės susipažinti taip pat žr. Sprendimo *Privacy International*, C-623/17, ECLI:EU:C:2020:790, 65 punktą ir Sprendimo *La Quadrature du Net ir kt.*, C-511/18, C-512/18 ir C-520/18 ,ECLI:EU:C:2020:791, 175 punktą.

([122]) Žr. Sprendimo *Schrems II* 176 ir 181 punktus ir juose minimą jurisprudenciją. Dėl valstybių narių valdžios institucijų galimybės susipažinti taip pat žr. Sprendimo *Privacy International* 68 punktą ir Sprendimo *La Quadrature du Net ir kt*. 132 punktą.

([123]) Žr. Sprendimo *Schrems II* 176 punktą. Dėl valstybių narių valdžios institucijų galimybės susipažinti taip pat žr. Sprendimo *Privacy International* 68 punktą ir Sprendimo *La Quadrature du Net ir kt*. 132 punktą.

([124]) Žr. Sprendimo *Schrems II* 179 punktą.

([125]) Žr. Sprendimo *Schrems II* 181–182 punktus.

([126]) Žr. Sprendimo *Schrems I* 95 punktą ir Sprendimo *Schrems II* 194 punktą. Šiuo atžvilgiu ESTT visų pirma pažymėjo, kad Pagrindinių teisių chartijos straipsnio 47 straipsnio, kuriame garantuojama teisė į veiksmingą teisinę gynybą nepriklausomame ir nešališkame teisme, laikymasis yra „svarbus užtikrinant Sąjungos teisėje reikalaujamą apsaugos lygį [ir jo] laikymąsi Komisija turi konstatuoti prieš priimdama sprendimą dėl tinkamumo pagal [Reglamento (ES) 2016/679 45 straipsnio 1 dalį“ (Sprendimo *Schrems II* 186 punktas).

([127]) 1998 m. Žmogaus teisių akto 6 straipsnis.

([128]) Europos Žmogaus Teisių Teismo sprendimas *Klass ir kt. prieš Vokietiją*, paraiškos Nr. 5029/71, 17–51 punktai.

(118) Be to, asmenims turi būti suteiktos veiksmingos teisių gynimo priemonės, o Europos Žmogaus Teisių Teismas paaiškino, kad teisių gynimo priemones turi suteikti nepriklausoma ir nešališka įstaiga, kuri yra nustačiusi savo darbo tvarkos taisykles, kurią sudaro aukštas teisėjų pareigas einantys arba ėję nariai arba patyrę advokatai, ir kad siekiant jai pateikti skundą nebūtų nustatytos jokios prievolės įrodyti. Įsipareigodama nagrinėti asmenų skundus, nepriklausoma ir nešališka įstaiga turėtų turėti galimybę susipažinti su visa atitinkama informacija, įskaitant slaptą medžiagą. Galiausiai ji turėtų turėti įgaliojimus ištaisyti reikalavimo nesilaikymo atvejus ([129]).

(119) Jungtinė Karalystė taip pat ratifikavo Tarybos konvenciją dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (108-oji konvencija) ir 2018 m. pasirašė Protokolą, kuriuo iš dalies keičiama Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (dar vadinama 108+ konvencija) ([130]). 108-osios konvencijos 9 straipsnyje nustatyta, kad nuo bendrųjų duomenų apsaugos principų (5 straipsnis, duomenų kokybė), taisyklių, kuriomis reglamentuojamos specialios duomenų kategorijos (6 straipsnis, specialių kategorijų duomenys) ir duomenų subjektų teisių (8 straipsnis, papildomos duomenų subjekto apsaugos priemonės) nukrypti leidžiančios nuostatos yra leistinos tik jeigu jos numatytos susitariančiosios šalies teisės aktuose ir yra būtina priemonė demokratinėje visuomenėje siekiant užtikrinti valstybės saugumą, visuomenės saugumą, valstybės piniginius interesus arba stabdyti nusikalstamas veikas arba apsaugoti duomenų subjektą arba kitų asmenų teises ir laisves ([131]).

(120) Todėl, dalyvaudama Europos Taryboje, laikydamasi Europos žmogaus teisių konvencijos ir pritardama Europos Žmogaus Teisių Teismo jurisdikcijai, Jungtinė Karalystė privalo laikytis įvairių įpareigojimų, nustatytų tarptautinėje teisėje, kurie sudaro Jungtinės Karalystės vyriausybės prieigos prie duomenų, remiantis principais, apsaugos priemonėmis ir asmenų teisėmis, panašiomis į tas, kurios garantuojamos pagal ES teisę ir yra taikomos valstybėms narėms, sistemą. Todėl, kaip pažymėta (19) konstatuojamojoje dalyje, tokių priemonių paisymas yra ypač svarbus šio sprendimo vertinimo pagrindą sudarantis aspektas.

(121) Be to, konkrečios duomenų apsaugos priemonės ir teisės garantuojamos pagal 2018 m. DAA tais atvejais, kai duomenis tvarko valdžios institucijos, įskaitant teisėsaugos ir nacionalinio saugumo įstaigas.

(122) Visų pirma asmens duomenų tvarkymo baudžiamosios teisėsaugos srityje tvarka aprašyta 2018 m. DAA 3 dalyje, kuri buvo patvirtinta siekiant į nacionalinę teisę perkelti Direktyvą (ES) 2016/680. 2018 m. DAA 3 dalis taikoma asmens duomenų tvarkymui, kurį vykdo kompetentingos institucijos nusikalstamų veikų prevencijos, tyrimo, nustatymo ar traukimo baudžiamojon atsakomybėn už jas arba baudžiamųjų sankcijų vykdymo tikslais, įskaitant apsaugą nuo grėsmių visuomenės saugumui ir jų prevenciją ([132]).

(123) Pagal DAA 30 straipsnyje pateiktą apibrėžtį „kompetentinga institucija“ yra laikomas 2018 m. DAA 7 priede nurodytas asmuo ir bet kuris kitas asmuo, kuris vykdo įstatymuose nustatytas funkcijas bet kuriuo iš teisėsaugos tikslų ([133]). Kaip paaiškinta toliau (žr. (139) konstatuojamąją dalį), kai kurios kompetentingos institucijos (pavyzdžiui, Nacionalinė nusikaltimų agentūra) tam tikromis sąlygomis gali naudotis 2016 m. Tyrimo aktu (2016 m. TĮA) suteiktais įgaliojimais. Tokiu atveju 2016 m. TĮA numatytos apsaugos priemonės bus taikomos kartu su apsaugos priemonėmis, numatytomis 2018 m. DAA 3 dalyje. Žvalgybos tarnybos (Slaptoji žvalgybos tarnyba, Saugumo tarnyba ir Vyriausybės komunikacijos centras) nelaikomos kompetentingomis institucijomis ([134]), kurioms taikoma 2018 m. DAA 3 dalis, todėl joje nustatytos taisyklės jokiai jų veiklai netaikomos. Speciali 2018 m. DAA dalis (4 dalis) skirta žvalgybos tarnybų vykdomam asmens duomenų tvarkymui (daugiau apie tai (125) konstatuojamojoje dalyje ).

([129]) Europos Žmogaus Teisių Teismo sprendimas *Kennedy prieš Jungtinę Karalystę*, paraiškos Nr. 26839/05 (toliau – *Kennedy*), 167 ir 190 punktai.

([130]) Daugiau informacijos apie Europos žmogaus teisių konvenciją ir jos perkėlimą į Jungtinės Karalystės teisę priimant 1998 m. Žmogaus teisių aktą, taip pat apie 108-ąją konvenciją žr. (9)konstatuojamąją dalį.

([131]) Panašiai, pagal 108+ konvencijos 11 straipsnį tam tikrų konkrečių Konvencijoje nustatytų teisių ir pareigų apribojimai, susiję su nacionaliniu saugumu arba prevencija, nusikalstamų veikų tyrimu ir baudžiamuoju persekiojimu už jas bei baudžiamųjų sankcijų vykdymu, yra leistini tik jeigu toks apribojimas nustatytas įstatyme, juo paisoma esminių pagrindinių teisių ir laisvių, ir jis yra būtina ir proporcinga priemonė demokratinėje visuomenėje. Duomenų tvarkymo nacionalinio saugumo ir gynybos tikslais veiklai taip pat turi būti taikoma nepriklausoma ir veiksminga peržiūra ir priežiūra pagal atitinkamos Konvencijos susitariančiosios šalies vidaus teisės aktus.

([132]) 2018 m. DAA 31 straipsnis.

([133]) Prie 7 priede išvardytų kompetentingų institucijų priskiriamos ne tik policijos pajėgos, bet ir visi Jungtinės Karalystės vyriausybės ministerijų departamentai ir kitos tyrimų funkcijas vykdančios institucijos (pvz., Jos Didenybės mokesčių ir muitų komisaras, Velso mokesčių institucija, Konkurencijos ir rinkų institucija, Jos Didenybės žemės registras ir Nacionalinė nusikaltimų agentūra), prokuratūros tarnybos, kitos baudžiamojo teisingumo tarnybos ir kitos teisėsaugos veiklą vykdančios įstaigos ar organizacijos.

([134]) 2018 m. DAA 30 straipsnio 2 dalis.

(124) Panašiai, kaip ir Direktyvoje (ES) 2016/680, 2018 m. DAA 3 dalyje nustatyti teisėtumo ir sąžiningumo ([135]), tikslo apribojimo ([136]), duomenų kiekio mažinimo ([137]), tikslumo ([138]), saugojimo ribojimo ([139]) ir saugumo ([140]) principai. Teisės aktuose nustatyti konkretūs skaidrumo įpareigojimai ([141]) ir asmenims suteikiama teisė susipažinti su duomenimis ([142]), juos ištaisyti ir ištrinti ([143]), taip pat teisė nesutikti, kad dėl asmens nebūtų automatizuotai priimami sprendimai ([144]). Taip pat reikalaujama, kad kompetentingos institucijos įgyvendintų pritaikytąją ir standartizuotąją duomenų apsaugą, saugotų duomenų tvarkymo veiklos įrašus ir dėl tam tikrų tvarkymo operacijų atliktų poveikio duomenų apsaugai vertinimus ir iš anksto konsultuotųsi su Informacijos komisaru ([145]). Pagal 2018 m. DAA 56 straipsnį jos privalo įrodyti vidaus reikalavimų laikymąsi. Be to, kompetentingos institucijos privalo nustatyti tinkamas priemones, kad užtikrintų duomenų tvarkymo saugumą ([146]), ir joms galioja konkretūs įpareigojimai duomenų saugumo pažeidimo atveju, įskaitant informacijos komisaro ir duomenų subjektų informavimą apie tokius pažeidimus ([147]). Kaip ir Direktyvos (ES) 2016/680 atveju, duomenų valdytojas (išskyrus atvejus, kai duomenų valdytojas yra kita teisminė institucija, veikianti turėdama teisminius įgaliojimus) taip pat privalo paskirti duomenų apsaugos pareigūną (DAP) ([148]), kuris padeda duomenų valdytojui laikytis savo prievolių, taip pat stebėti, kaip šių prievolių laikomasi ([149]). Be to, teisės aktuose, siekiant užtikrinti apsaugos tęstinumą, nustatyti konkretūs tarptautinių asmens duomenų perdavimų reikalavimai, taikomi tais atvejais, kai duomenys į trečiąsias valstybes arba tarptautinėms organizacijoms perduodami teisėsaugos tikslais ([150]). Tą pačia dieną, kurią buvo priimtas šis sprendimas, Komisija, remdamasi Direktyvos (ES) 2016/680 36 straipsnio 3 dalimi, priėmė sprendimą dėl tinkamumo, kuriame padaryta išvada, kad Jungtinės Karalystės baudžiamosios teisėsaugos institucijų vykdomam duomenų tvarkymui taikoma tvarka užtikrinamas toks apsaugos lygis, kuris iš esmės yra lygiavertis Direktyva (ES) 2016/680 garantuojamam lygiui.

(125) 2018 m. DAA 4 dalis taikoma visam žvalgybos tarnybų arba jų vardu atliekamam duomenų tvarkymui. Visų pirma, joje nustatyti pagrindiniai duomenų apsaugos principai (teisėtumas, sąžiningumas ir skaidrumas ([151]), tikslo apribojimas ([152]), duomenų kiekio mažinimas ([153]), tikslumas ([154]), saugojimo ribojimas ([155]) ir saugumas ([156]), nustatytos specialių kategorijų asmens duomenų tvarkymo sąlygos ([157]), numatytos duomenų subjektų teisės ([158]),

([135]) 2018 m. DAA 35 straipsnis.
([136]) 2018 m. DAA 36 straipsnis.
([137]) 2018 m. DAA 37 straipsnis.
([138]) 2018 m. DAA 38 straipsnis.
([139]) 2018 m. DAA 39 straipsnis.
([140]) 2018 m. DAA 40 straipsnis.
([141]) 2018 m. DAA 44 straipsnis.
([142]) 2018 m. DAA 45 straipsnis.
([143]) 2018 m. DAA 46 ir 47 straipsniai.
([144]) 2018 m. DAA 49 ir 50 straipsniai.
([145]) 2018 m. DAA 56–65 straipsniai.
([146]) 2018 m. DAA 66 straipsnis.
([147]) 2018 m. DAA 67–68 straipsniai.
([148]) 2018 m. DAA 69-71 straipsniai.
([149]) 2018 m. DAA 67–68 straipsniai.
([150]) 2018 m. DAA 3 dalies 5 skyrius.
([151]) Pagal 2018 m. DAA 86 straipsnio 6 dalį, siekiant nustatyti, ar duomenys tvarkomi sąžiningai ir skaidriai, būtina atsižvelgti į jų gavimo metodą. Šia prasme sąžiningumo ir skaidrumo reikalavimas laikomas įvykdytu, jeigu duomenys gaunami iš asmens, kuris yra teisėtai įgaliotas juos teikti arba jis teisėtai tai privalo daryti.
([152]) Pagal 2018 m. DAA 87 straipsnį duomenų tvarkymo tikslai turi būti konkretūs, aiškūs ir teisėti. Duomenų negalima tvarkyti su tikslais, kuriais jie buvo surinkti, nesuderinamu būdu. Pagal 2018 m. DAA 87 straipsnio 3 dalį toliau suderintai asmens duomenis galima leisti tvarkyti tik jeigu duomenų valdytojui pagal įstatymą leidžiama tuo tikslu tvarkyti duomenis ir duomenis tvarkyti yra būtina ir proporcinga atsižvelgiant į tą kitą tikslą. Duomenų tvarkymas turėtų būti laikomas suderinamu, jeigu duomenys tvarkomi archyvavimo tikslais atsižvelgiant į viešąjį interesą, mokslinių arba istorinių tyrimų arba statistiniais tikslais ir jei tokiam tvarkymui taikomos tinkamos apsaugos priemonės (2018 m. DAA 87 straipsnio 4 dalis).
([153]) Asmens duomenys turėtų būti tinkami, aktualūs ir neperteklinai (2018 m. DAA 88 straipsnis).
([154]) Asmens duomenys turėtų būti tikslūs ir nauji (2018 m. DAA 89 straipsnis).
([155]) Asmens duomenys neturėtų būti saugomi ilgiau, nei to reikia (2018 m. DAA 90 straipsnis).
([156]) Pagal šeštąjį duomenų apsaugos principą duomenų tvarkymo metodai turi apimti tinkamas apsaugos nuo rizikos, kylančios dėl asmens duomenų tvarkymo, priemones. Rizika (be kita ko) apima atsitiktinę arba neteisėtą prieigą prie asmens duomenų, jų sunaikinimą, praradimą, naudojimą, keitimą arba atskleidimą (2018 m. DAA 91 straipsnis). Pagal 107 straipsnį taip pat reikalaujama, kad 1) kiekvienas duomenų valdytojas būtinai įgyvendintų tinkamas saugumo priemones, proporcingas rizikai, kylančiai dėl asmens duomenų tvarkymo, ir 2) automatizuoto duomenų tvarkymo atveju kiekvienas duomenų valdytojas ir kiekvienas duomenų tvarkytojas įgyvendintų rizikos vertinimu pagrįstas prevencines arba rizikos mažinimo priemones.
([157]) 2018 m. DAA 86 straipsnio 2 dalies b punktas ir 10 priedas.
([158]) 2018 m. DAA 4 dalies 3 skyrius, visų pirma: teisę susipažinti su duomenimis, juos ištaisyti ir ištrinti, teisę nesutikti, kad duomenys būtų tvarkomi, įsikišti į automatizuotą sprendimų priėmimą ir teisę būti informuotam apie sprendimų priėmimą. Be to, duomenų valdytojas privalo suteikti duomenų subjektui informacijos apie jo asmens duomenų tvarkymą. Kaip paaiškinta Informacijos komisaro gairėse dėl žvalgybos tarnybų atliekamo duomenų tvarkymo, asmenys gali naudotis visomis savo teisėmis (įskaitant prašymą ištaisyti duomenis) pateikdami skundą Informacijos komisarui arba kreipdamiesi į teismą (žr. Informacijos komisaro gairėse dėl žvalgybos tarnybų atliekamo duomenų tvarkymo, kurias galima rasti adresu https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-intelligence-services-processing/).

reikalaujama užtikrinti pritaikytąją duomenų apsaugą ([159]) ir reglamentuojami tarptautiniai asmens duomenų perdavimai ([160]). Informacijos komisaras neseniai paskelbė išsamias gaires dėl žvalgybos tarnybų vykdomo duomenų tvarkymo pagal 2018 m. DAA 4 dalį ([161]).

(126) Kartu 2018 m. DAA 110 straipsnyje nustatyta 2018 m. DAA 4 dalies numatytų nuostatų išimtis ([162]), kai tokia išimtis yra būtina siekiant užtikrinti nacionalinį saugumą. Šia išimtimi galima remtis kiekvienu atskiru atveju atlikus analizę ([163]). Kaip paaiškino Jungtinės Karalystės institucijos ir nustatyta jurisprudencijoje, „duomenų valdytojas privalo atsižvelgti į faktines pasekmes nacionaliniam saugumui arba gynybai, jeigu jis privalo laikytis konkrečios duomenų apsaugos nuostatos ir jeigu jis gali pagrįstai laikytis įprastos taisyklės nedarydamas poveikio nacionaliniam saugumui arba gynybai“ ([164]). Tai, ar išimtimi naudojamasi tinkamai, prižiūri informacijos komisaras ([165]).

(127) Be to, atsižvelgiant į galimybę „nacionalinio saugumo“ užtikrinimo tikslais apriboti pirmiau nurodytų konkrečių 2018 m. DAA 111 dalies nuostatų taikymą, duomenų valdytojas gali prašyti išduoti ministrų kabineto arba generalinio prokuroro pasirašytą sertifikatą, kuriuo patvirtinama, kad tokių teisių apribojimas yra būtina ir proporcinga priemonė nacionaliniam saugumui užtikrinti ([166]).

(128) Jungtinės Karalystės vyriausybė paskelbė gaires, kad padėtų duomenų valdytojams nuspręsti, ar prašyti išduoti saugumo sertifikatą pagal 2018 m. DAA, ir kuriose visų pirma atkreipiamas dėmesys į tai, kad bet kokie duomenų subjektų teisių apribojimai nacionalinio saugumo užtikrinimo tikslais turi būti proporcingi ir būtini ([167]). Visi nacionalinio saugumo sertifikatai turi būti skelbiami Informacijos komisaro interneto svetainėje ([168]).

---

([159]) 2018 m. DAA 103 straipsnis.

([160]) 2018 m. DAA 109 straipsnis. Asmens duomenų perdavimai tarptautinėms organizacijoms arba į valstybes už Jungtinės Karalystės ribų yra įmanomi, jeigu duomenų perdavimas yra būtina ir proporcinga priemonė duomenų valdytojui vykdant teisės aktuose nustatytas funkcijas arba kitais konkrečiuose 1989 m. Saugumo žvalgybos akto ir 1994 m. Žvalgybos tarnybų akto straipsniuose nustatytais tikslais.

([161]) Informacijos komisaro gairės, žr. 158 išnašą.
2018 m. DAA 30 straipsnis ir 7 priedas.

([162]) 2018 m. DAA 110 straipsnio 2 dalyje nurodyta, kurioms nuostatoms leidžiama taikyti išimtį. Šios nuostatos yra duomenų apsaugos principai (išskyrus teisėtumo principą), duomenų subjekto teisės, pareiga informuoti informacijos komisarą apie duomenų saugumo pažeidimą, informacijos komisaro įgaliojimai atlikti patikrinimus laikantis tarptautinių įpareigojimų, tam tikri informacijos komisaro vykdymo užtikrinimo įgaliojimai, nuostatos, kuriomis už tam tikrus duomenų apsaugos pažeidimus taikoma baudžiamoji atsakomybė, ir nuostatos, susijusios su specialiais duomenų tvarkymo tikslais, pvz., žurnalistikos, akademiniais arba meniniais tikslais.

([163]) Žr. *Baker prieš Secretary of State*, žr. 61išnašą.

([164]) Diskusijoms dėl duomenų apsaugos tinkamumo skirto Jungtinės Karalystės aiškinamojo dokumento H skirsnis Diskusijoms dėl duomenų apsaugos tinkamumo skirto Jungtinės Karalystės aiškinamojo dokumento H skirsnis „Nacionalinio saugumo duomenų apsaugos ir tyrimo įgaliojimų sistema“, , p. 15–16 (žr. 31išnašą). Taip pat žr. Sprendimą *Baker prieš Secretary of State* (žr. 61 išnašą), kuriame teismas panaikino vidaus reikalų sekretoriaus išduotą nacionalinį saugumo sertifikatą ir pritarė nacionalinio saugumo išimties taikymui, motyvuodamas tuo, kad nebuvo jokios priežasties numatyti bendrą pareigos atsakyti į prašymus leisti susipažinti su duomenimis išimtį ir kad leidimas taikyti tokią išimtį visomis aplinkybėmis, neatlikus kiekvieno atvejo analizės, viršija tai, kas būtina ir proporcinga nacionaliniam saugumui užtikrinti.

([165]) Žr. Informacijos komisaro ir Jungtinės Karalystės žvalgybos bendruomenės susitarimo memorandumą, pagal kurį „Informacijos komisaras, gavęs duomenų subjekto skundą, įsitikina, kad klausimas buvo išnagrinėtas teisingai ir, kai taikytina, kad bet kokia išimtis buvo taikoma tinkamai“. Informacijos komisaro biuro ir Jungtinės Karalystės žvalgybos bendruomenės susitarimo memorandumo 16 punktas, galima rasti šiuo adresu: https://ico.org.uk/media/about-the-ico/mou/2617438/uk-intelligence-community-ico-mou.pdf.

([166]) 2018 m. DAA panaikinta galimybė sertifikatus išduoti pagal 1998 m. Duomenų apsaugos akto 28 straipsnio 2 dalį. Tačiau galimybė išduoti sertifikatus pagal „seną tvarką“ vis dar egzistuoja, nes taikant 1998 m. aktą iškilo istorinis iššūkis (žr. 2018 m. DAA 20 priedo 5 dalies 17 punktą). Vis dėlto tokia galimybė, panašu, taikoma itin retai, tik tam tikrais atvejais: pavyzdžiui, jei duomenų subjektas užginčija nacionalinio saugumo išimties taikymą, kai duomenis tvarko valdžios institucija, tą daranti pagal 1998 m. aktą. Pažymėtina, kad tokiais atvejais bus taikomas visas 1998 m. DAA 28 straipsnis, įskaitant galimybę duomenų subjektui užginčyti sertifikato galiojimą teisme.

([167]) Jungtinės Karalystės gairės dėl nacionalinio saugumo sertifikatų pagal 2018 m. duomenų apsaugos aktą, galima rasti šiuo adresu: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf. Remiantis Jungtinės Karalystės institucijų pateiktu išaiškinimu, nors sertifikatas yra svarus įrodymas, kad dėl jame aprašytų duomenų arba duomenų tvarkymo taikoma išimtis, juo nepanaikinamas reikalavimas duomenų valdytojui išnagrinėti, ar esama poreikio kiekvienu konkrečiu atveju remtis išimtimi.

([168]) Pagal 2018 m. DAA 130 skyrių informacijos komisaras gali nuspręsti neskelbti sertifikato teksto ar jo dalies, jei tai prieštarautų nacionalinio saugumo interesams, viešajam interesui arba galėtų kelti pavojų kurio nors asmens saugumui. Tačiau tokiais atvejais informacijos komisaras paskelbia, kad sertifikatas buvo išduotas.

(129) Sertifikato galiojimo trukmė turėtų būti konkreti ir neviršyti penkerių metų, kad įstatymų vykdomoji valdžia galėtų jį nuolat peržiūrėti ([169]). Sertifikate nurodomi asmens duomenys arba asmens duomenų kategorijos, kurioms taikoma išimtis, taip pat 2018 m. DAA nuostatos, kurioms taikoma išimtis ([170]).

(130) Svarbu pažymėti, kad nacionalinio saugumo sertifikatai nesuteikia papildomo pagrindo apriboti duomenų apsaugos teises nacionalinio saugumo sumetimais. Kitaip tariant, domenų valdytojas arba duomenų tvarkytojas sertifikatu gali remtis tik kai padaro išvadą, kad būtina taikyti nacionalinio saugumo išimtį, kuri, kaip paaiškinta, turi būti taikoma kiekvienu konkrečiu atveju ([171]). Net jei nacionalinio saugumo sertifikatas sprendžiant konkretų klausimą yra taikomas, informacijos komisaras gali tirti, ar konkrečiu atveju remtis nacionalinio saugumo išimtimi buvo pagrįsta ([172]).

(131) Bet kuris asmuo, kurį sertifikato išdavimas paveikė tiesiogiai, gali pateikti skundą aukštesniajam specializuotam teismui ([173]) dėl to sertifikato ([174]) arba, jeigu sertifikate duomenys nurodomi pateikiant bendrą aprašymą, ginčyti sertifikato taikymą konkretiems duomenims ([175]). Specializuotas teismas peržiūrės sprendimą išduoti sertifikatą ir nuspręs, ar buvo pagrįstų priežasčių jį išduoti ([176]). Jis gali nagrinėti įvairius klausimus, įskaitant būtinumą, proporcingumą ir teisėtumą, ir atsižvelgti į poveikį duomenų subjektų teisėms ir suderinti poreikį užtikrinti nacionalinį saugumą. Todėl specializuotas teismas gali nuspręsti, kad tam tikriems asmens duomenims, dėl kurių pateiktas skundas, sertifikatas netaikomas ([177]).

(132) Kitą galimų apribojimų grupę sudaro apribojimai, pagal 2018 m. DAA 11 straipsnį taikomi tam tikroms 2018 m. DAA 4 dalies nuostatoms ([178]), siekiant apsaugoti kitus su bendru viešuoju interesu arba saugomais interesais susijusius svarbius tikslus, pvz., Parlamento neliečiamumą, advokato teisę neatskleisti profesinės paslapties, teismo proceso vykdymą arba ginkluotųjų pajėgų kovinį veiksmingumą ([179]). Šių nuostatų taikymo išimtis yra taikoma tam tikrų kategorijų informacijai (pagrįsta pagal kategoriją) arba ta apimtimi, kuria šių nuostatų taikymas galėtų pakenkti saugomam interesui (pagrįsta pagal žalą) ([180]). Žalos prielaida pagrįstomis išimtimis galima remtis tik tiek,

([169]) Jungtinės Karalystės gairių dėl nacionalinio saugumo sertifikatų 15 dalis, žr. 167išnašą.

([170]) Jungtinės Karalystės gairių dėl nacionalinio saugumo sertifikatų 5 dalis, žr. 167išnašą.

([171]) Žr. 164 išnašą.

([172]) 2018 m. DAA 102 straipsnyje nustatyta, kad duomenų valdytojas turi gebėti įrodyti, kad laikėsi 2018 m. DAA. Tai reiškia, kad žvalgybos tarnyba turėtų įrodyti informacijos komisarui, kad, remdamasi išimtimi, ji išnagrinėjo konkrečias bylos aplinkybes. Informacijos komisaras taip pat skelbia nacionalinio saugumo sertifikatų registrą, skelbiamas šiuo adresu: https://ico.org.uk/about-the-ico/our-information/national-security-certificates/.

([173]) Aukštesnysis specializuotas teismas turi kompetenciją nagrinėti skundus dėl žemesnės instancijos administracinių specializuotų teismų priimtų sprendimų ir specialią kompetenciją nagrinėti tiesioginius skundus dėl tam tikrų vyriausybės įstaigų sprendimų.

([174]) 2018 m. DAA 111 straipsnio 3 dalis.

([175]) 2018 m. DAA 111 straipsnio 5 dalis.

([176]) Sprendime *Baker prieš Secretary of State* (žr. 61 išnašą) specializuotas informacinis teismas panaikino vidaus reikalų sekretoriaus išduotą nacionalinį saugumo sertifikatą, motyvuodamas tuo, kad nebuvo jokios priežasties numatyti bendrą pareigos atsakyti į prašymus leisti susipažinti su duomenimis išimtį ir kad leidimas taikyti tokią išimtį visomis aplinkybėmis, neatlikus kiekvieno atvejo analizės, viršija tai, kas būtina ir proporcinga nacionaliniam saugumui užtikrinti.

([177]) Jungtinės Karalystės gairių dėl nacionalinio saugumo sertifikatų 25 dalis, žr. 167išnašą.

([178]) Tai yra: i) 4 dalies duomenų apsaugos principai, išskyrus duomenų tvarkymo teisėtumo reikalavimą pagal pirmąjį principą ir tai, kad duomenų tvarkymas turi atitikti vieną iš 9 ir 10 prieduose nustatytų sąlygų; ii) duomenų subjektų teisės ir iii) pareigos, susijusios su informacijos komisaro informavimu apie saugumo pažeidimus.

([179]) 2018 m. DAA 4 dalyje nustatyta teisinė sistema, taikoma visų rūšių žvalgybos agentūrų vykdomam asmens duomenų tvarkymui (ne tik nacionalinio saugumo užduočių vykdymui). Todėl 4 dalis taip pat taikoma tais atvejais, kai žvalgybos agentūros duomenis tvarko, pavyzdžiui, žmogiškųjų išteklių valdymo tikslais, bylinėdamosi arba vykdydamos viešuosius pirkimus. 11 priede išvardyti apribojimai iš esmės taikytini tokiomis kitomis aplinkybėmis. Pavyzdžiui, bylinėjantis su darbuotoju gali būti taikomas apribojimas „teismo proceso“ tikslais, o viešųjų pirkimų atveju gali būti taikomas apribojimas „derybų“ tikslais ir pan. Į tai atsižvelgta ir Informacijos komisaro gairėse dėl žvalgybos tarnybų vykdomo duomenų tvarkymo, kuriose pateikiamas pavyzdys, kad 11 priede nustatytus apribojimus galima taikyti žvalgybos agentūros ir buvusio darbuotojo, pateikusio su darbu susijusius reikalavimus, derybose dėl susitarimo (žr. 161 išnašą). Taip pat reikėtų pažymėti, kad tais pačiais apribojimais pagal 2018 m. DAI 2 dalies 2 priedą gali naudotis ir kitos valdžios institucijos.

([180]) Kaip nurodyta Jungtinės Karalystės aiškinamajame dokumente, pagal informacijos kategorijas taikomos šios išimtys: i) informacija apie Karališkųjų apdovanojimų ir titulų suteikimą; ii) profesinės paslapties apsauga; iii) konfidencialaus darbo, mokymo ar švietimo sąlygos ir iv) egzaminų darbai ir įvertinimai. „Žalos prielaida“ pagrįstos išimtys yra susijusios su šiais klausimais: i) nusikaltimų prevencija arba išaiškinimu; nusikaltėlių sulaikymu ir baudžiamuoju persekiojimu; ii) parlamento narių imunitetu; iii) teismo procesu; iv) Karališkųjų ginkluotųjų pajėgų kovos veiksmingumu; v) Jungtinės Karalystės ekonomine gerove; vi) derybomis su duomenų subjektu; vii) moksliniais arba istoriniais tyrimais arba statistiniais tikslais; viii) archyvavimu viešojo intereso labui. Diskusijoms dėl duomenų apsaugos tinkamumo skirto Jungtinės Karalystės aiškinamojo dokumento H skirsnis „Nacionalinis saugumas“, p. 13, žr. 31 išnašą.

kiek išvardytų duomenų apsaugos nuostatų taikymas galėtų pakenkti konkrečiam interesui. Todėl išimtis visada turi būti pagrindžiama nurodant atitinkamą žalą, kuri galėtų atsirasti konkrečiu atveju. Grupinėmis išimtimis galima remtis tik dėl mokslinės, siauriai apibrėžtos kategorijos informacijos, kuriai leidžiama taikyti išimtį. Atsižvelgiant į tikslą ir poveikį, šios išimtys yra panašios į Jungtinės Karalystės BDAR nustatytas išimtis (pagal 2018 m. DAA 2 priedą), kurios savo ruožtu atspindi BDAR 23 straipsnyje numatytas išimtis.

(133) Iš to, kas išvardyta, galima daryti išvadą, kad pagal taikytinas Jungtinės Karalystės teisines nuostatas galioja apribojimai ir sąlygos, kaip tai, be kita ko, išaiškino teismai ir Informacijos komisija, kuriais siekiama užtikrinti, kad šios išimtys ir apribojimai neviršytų to, kas yra būtina ir proporcinga nacionaliniam saugumui užtikrinti.

### 3.2. **Jungtinės Karalystės valdžios institucijų galimybė susipažinti su duomenimis ir jų naudojimas baudžiamosios teisėsaugos tikslais**

(134) Jungtinės Karalystės teisėje nustatyti įvairūs galimybės susipažinti su asmens duomenimis ir juos naudoti teisėsaugos tikslais apribojimai, ir šioje srityje numatyti priežiūros ir teisių gynimo mechanizmai, kurie atitinka šio sprendimo (113)–(115) konstatuojamosiose dalyse nurodytus reikalavimus. Sąlygos, kuriomis tokia prieiga gali būti suteikta, ir šių įgaliojimų naudojimui taikomos apsaugos priemonės išsamiai įvertinamos kituose skirsniuose.

#### 3.2.1. *Teisiniai pagrindai ir taikomi apribojimai / apsaugos priemonės*

(135) Pagal teisėtumo principą, kuris garantuojamas 2018 m. DAA 35 straipsnyje, asmens duomenų tvarkymas bet kuriuo teisėsaugos tikslu yra teisėtas tik jeigu jis grindžiamas įstatymu ir jeigu duomenų subjektas sutiko, kad jo duomenys būtų tvarkomi tuo tikslu ([181]), arba duomenis tvarkyti būtina siekiant, kad kompetentinga institucija atliktu tuo tikslu vykdomą užduotį.

##### 3.2.1.1. Kratos orderiai ir įrodymų pateikimo orderiai

(136) Jungtinės Karalystės teisinėje sistemoje asmens duomenis iš ūkio subjektų, įskaitant ūkio subjektus, kurie iš ES perduotus duomenis tvarkytų pagal dabartinį sprendimą dėl tinkamumo, rinkti baudžiamosios teisėsaugos tikslais leidžiama remiantis kratos orderiais ([182]) ir įrodymų pateikimo orderiais ([183]).

(137) Kratos orderius paprastai išduoda teismas tyrimą atliekančio pareigūno prašymu. Pagal šiuos orderius pareigūnui leidžiama patekti į patalpas ieškant tyrimui svarbių įrodymų arba asmenų ir paimti bet kurį daiktą, dėl kurio leista atlikti kratą, įskaitant bet kuriuos susijusius dokumentus arba įrodymus, kuriuose yra asmens duomenų ([184]). Pagal įrodymų pateikimo orderį, kurį taip pat turi išduoti teismas, reikalaujama, kad jame nurodytas asmuo pateiktų arba leistų susipažinti su jo

([181]) Atrodo, kad tinkamumo scenarijaus atveju sutikimo naudojimas nėra reikšmingas, nes perdavimo atveju Jungtinės Karalystės institucija tiesiogiai nerenka ES duomenų subjekto duomenų, remdamasi sutikimu.

([182]) Dėl atitinkamo teisinio pagrindo žr. 1984 m. pagal Policijos aktą priimto etikos kodekso (Anglija ir Velsas) 8 ir tolesnius straipsnius, 1989 m. Policijos ir baudžiamųjų įrodymų orderio (Šiaurės Airija) 10 ir tolesnius straipsnius, o Škotijoje jis išduodamas pagal bendrąją teisę (žr. 2016 m. Baudžiamojo teisingumo akto (Škotija) 46 straipsnį) ir Baudžiamosios teisės aktų (konsoliduoto įstatymo) 23B straipsnį (Škotija). Po arešto išduodamo kratos orderio teisinis pagrindas yra 1984 m. pagal Policijos aktą priimto etikos kodekso (Anglija ir Velsas) 18 straipsnis, 1989 m. Policijos ir baudžiamųjų įrodymų orderio 20 ir tolesni straipsniai (Šiaurės Airija), o Škotijoje jis išduodamas pagal bendrąją teisę (žr. 2016 m. Baudžiamojo teisingumo akto (Škotija) 46 straipsnį). Jungtinės Karalystės institucijos paaiškino, kad kratos orderius išduoda teismas tyrimą atliekančio pareigūno prašymu. Pagal šiuos orderius pareigūnui leidžiama patekti į patalpas ieškant tyrimui svarbių įrodymų arba asmenų; vykdant orderį dažnai prireiks policijos konsteblio pagalbos.

([183]) Jeigu tyrimas yra susijęs su pinigų plovimu (įskaitant konfiskavimo ir civilinio išieškojimo procedūras), atitinkamas teisinis pagrindas prašymui dėl įrodymų pateikimo orderio yra 2002 m. Nusikalstamu būdu įgytų pajamų akto 345 ir kt. straipsniai Anglijos, Velso ir Šiaurės Airijos atveju ir 380 ir kt. straipsniai Škotijos atveju. Jeigu tyrimas yra susijęs su kitais klausimais nei pinigų plovimas, prašymą išduoti įrodymų pateikimo orderį galima pateikti pagal 1984 m. PACE 1 priedo 9 straipsnį Anglijos ir Velso atveju ir 1989 m. Policijos ir baudžiamųjų įrodymų orderio (Šiaurės Airija) 10 ir kt. straipsnius Šiaurės Airijos atveju. Škotijoje jis gaunamas pagal bendrąją teisę (žr. 2016 m. Baudžiamosios teisėsaugos (Škotija) akto 46 straipsnį ir Baudžiamojo įstatymo (Škotija) (suvestinė redakcija) 23B straipsnį. Jungtinės Karalystės institucijos paaiškino, kad pagal įrodymų pateikimo orderį reikalaujama, kad jame nurodytas asmuo pateiktų savo turimus arba disponuojamus įrodymus arba leistų su jais susipažinti (žr. 1984 m. PACE 1 priedo 4 dalį).

([184]) Pavyzdžiui, 1984 m. PACE 8 ir 18 straipsniuose nustatyti įgaliojimai konfiskuoti ir laikyti bet kurį daiktą, dėl kurio buvo išduotas kratos orderis.

turimais arba disponuojamais įrodymais. Pareiškėjas privalo teismui įrodyti, kodėl būtinas orderis, taip pat dėl kokių priežasčių jis atitinka viešąjį interesą. Įstatymuose numatyta keletas įgaliojimų, pagal kuriuos leidžiama išduoti kratos orderius ir įrodymų pateikimo orderius. Kiekvieną nuostatą sudaro atskiros jai taikomos įstatyme nustatytos sąlygos, kurias turi atitikti išduotinas kratos orderis ([185]) arba įrodymų pateikimo orderis ([186]).

(138) Įrodymų pateikimo ir kratos orderius galima ginčyti prašant atlikti teisminę peržiūrą ([187]). Dėl apsaugos priemonių pažymėtina, kad visos baudžiamosios teisėsaugos institucijos, kurioms taikoma 2018 m. DAA 3 dalis, įskaitant policiją, gali susipažinti su asmens duomenimis, – o tai yra duomenų tvarkymo forma, – tik laikydamosi 2018 m. DAA nustatytų principų ir reikalavimų (žr.

([185]) Pavyzdžiui, PACE 8 ir 18 straipsniuose atitinkamai reglamentuojami taikos teisėjo įgaliojimai išduoti orderį ir policijos pareigūno įgaliojimai atlikti kratą namuose. Pirmuoju atveju (8 straipsnis) prieš išduodamas orderį, taikos teisėjas pirmiausia privalo įsitikinti, kad esama pagrįstų priežasčių manyti, kad: i) buvo padarytas įtariamas nusikaltimas; ii) patalpose yra įrodymų, kurie gali būti labai vertingi (patys savaime arba kartu su kitais įrodymais) tiriant nusikalstamą veiką; iii) tikėtina, kad tai bus svarbūs įrodymai; iv) jų nesudaro arba juose nėra daiktų, kuriems taikoma teisinė privilegija, nerinktinų įrodymų išimtis arba tai yra specialūs procesiniai įrodymai, ir v) be orderio patekti į patalpas nebūtų įmanoma. Antruoju atveju pagal 18 straipsnį policijos pareigūnui leidžiama atlikti kratą asmens, kuris buvo areštuotas dėl įtariamo nusikaltimo, patalpose ieškant kitų įrodymų nei tie, kuriems taikoma teisinė privilegija, jeigu policijos pareigūnai pagrįstai įtaria, kad patalpose esama įrodymų, susijusių su nusikaltimu arba kitu panašiu ar susijusiu įtariamu nusikaltimu. Atliekant tokią kratą turi būti ieškoma tik tokių įrodymų, be to, ją raštu privalo sankcionuoti ne žemesnio nei inspektoriaus rango policijos pareigūnas, išskyrus atvejus, kai tai yra būtina tiriant nusikaltimą. Tokiu atveju pareigūną, kurio rangas ne žemesnis nei inspektorius, būtina kuo greičiau ir, kai tik tai įmanoma, informuoti apie atliktą kratą. Kratos pagrindai ir ieškomų įrodymų pobūdis turi būti protokoluojami. Be to 1984 m. PACE 15 ir 16 straipsniuose nustatytos įstatymuose įtvirtintos apsaugos priemonės, kurias reikia naudoti kreipiantis dėl kratos orderio. 15 straipsnyje konkrečiai nurodyta, kad kratos orderiui taikomi reikalavimai (įskaitant konsteblio teikiamo prašymo turinį ir tai, kad orderyje, be kita ko, būtina nurodyti teisės aktą, kuriuo remiantis jis išduodamas, ir, kiek tai įmanoma, nurodomi ieškomi daiktai bei asmenys ir patalpos, kuriose turi būti atlikta krata). 16 straipsnyje reglamentuojama kratos atlikimo tvarka (pvz., 16 straipsnio 5 dalyje nustatyta, kad kratą atliekantis pareigūnas įteikia gyventojui orderio kopiją; pagal 16 straipsnio 11 dalį reikalaujama, kad įvykdytas orderis būt saugomas 12 mėnesių; 16 straipsnio 12 dalyje nustatyta gyventojo teisė per tą laikotarpį patikrinti orderį, jei jis to nori). Šie straipsniai padeda užtikrinti atitiktį EŽTK 8 straipsniui (žr., pvz., Sprendimo *Kent Pharmaceuticals prieš Director of the Serious Fraud Office* [2002] EWHC 3023 (QB) [30] punktą, Lord Woolf CJ). Jeigu šių apsaugos priemonių nepaisoma, krata gali būti paskelbta neteisėta (pvz., Sprendimas *R (Brook) prieš Preston Crown Court* [2018] EWHC 2024 (Admin), [2018] ACD 95; Sprendimas *R (Superior Import / Export Ltd) prieš Revenue and Customs Commissioners* [2017] EWHC 3172 (Admin), [2018] Lloyd's Rep FC 115, ir Sprendimas *R (F) prieš Blackfriars Crown Court* [2014] EWHC 1541 (Admin)). 1984 m. PACE 15 ir 16 straipsnius papildo PACE B kodeksas, t. y. praktikos kodeksas, kuriuo reglamentuojami policijos įgaliojimai atlikti kratą patalpose.

([186]) Pavyzdžiui, pagal 2002 m. Nusikalstamu būdu įgytų pajamų aktą išduodant įrodymų pateikimo orderį reikia nurodyti ne tik pagrįstas priežastis, kad būtų įvykdytos Nusikalstamu būdu įgytų pajamų akto 346 straipsnio 2 dalyje nustatytos sąlygos, bet ir pagrįstas priežastis, kad asmuo disponuoja konkrečiais nurodytais įrodymais arba juos kontroliuoja, ir kad tikėtina, jog tie įrodymai turės esminę vertę. Be to, kitas reikalavimas, taikomas išduodant įrodymų pateikimo orderį, yra susijęs su pagrįstomis priežastimis manyti, kad įrodymų pateikimas arba leidimas su jais susipažinti atitinka viešąjį interesą, atsižvelgiant į a) naudą tyrimui, jeigu įrodymai būtų gauti, ir b) aplinkybes, iš kurių, kaip nurodyta prašyme, matyti, kad asmuo disponuoja įrodymais, kuriuose yra jų informacija, arba juos kontroliuoja. Panašiai, teismas, kuris pagal 1984 m. PACE 1 priedą nagrinėja prašymą išduoti įrodymų pateikimo orderį, privalo įsitikinti, kad įvykdytos konkrečios sąlygos. Visų pirma PACE 1 priede nustatyti du atskiri alternatyvūs sąlygų rinkiniai ir vieno iš šių rinkinių sąlygos turi būti įvykdytos prieš teisėjui išduodant įrodymų pateikimo orderį. Pagal pirmąjį rinkinį reikalaujama, kad teismas turėtų pagrįstų priežasčių manyti, kad i) buvo padarytas įtariamas nusikaltimas; ii) įrodymų, išskyrus nerinktinus įrodymus, patalpoje ieškoma taikant specialią procedūrą; iii) tikėtina, kad jie turės esminę vertę tyrimui, nesvarbu, patys savaime ar kartu su kitais įrodymais; iv) ir tikėtina, kad tai bus svarbūs įrodymai; v) kiti įrodymų gavimo būdai buvo išbandyti arba jų nebuvo bandyta taikyti, nes jie nebūtų sėkmingi, ir, vi) įvertinus tyrimo ir aplinkybių, kuriomis asmuo disponuoja įrodymais, naudą, įrodymų pateikimas arba leidimas su jais susipažinti atitinka viešąjį interesą. Pagal antrąjį sąlygų rinkinį reikalaujama: i) kad įrodymai būtų patalpose ir kad jiems būtų taikoma speciali procedūra arba kad tai būtų nerinktini įrodymai; ii) jeigu dėl įrodymų nenustatytas draudimas atlikti kratas, remiantis teisės aktais, priimtais iki PACE, taikomais specialiai procedūrai, nerinktiniems įrodymams arba įrodymams, kuriems taikoma teisinė privilegija, dėl įrodymų būtų galima išduoti kratos orderį ir iii) taip elgtis būtų buvę tinkama.

([187]) Teisminė peržiūra – tai teisminė procedūra, kurią taikant valdžios sprendimus galima ginčyti Aukštajame Teisme. Teismai peržiūri ginčijamą sprendimą ir nusprendžia, ar galima pagrįstai teigti, kad sprendimas turi teisinių trūkumų, atsižvelgiant į viešosios teisės koncepcijas / principus. Pagrindiniai teisminės peržiūros pagrindai yra neteisėtumas, neracionalumas, procedūriniai pažeidimai, teisėti lūkesčiai ir žmogaus teisės. Po sėkmingos teisminės peržiūros teismas priima nutartį dėl skirtingų teisių gynimo priemonių; dažniausiai tai būna nutartis dėl anuliavimo (kuria panaikinamas arba anuliuojamas pradinis sprendimas, t. y. sprendimas išduoti kratos orderį), kai kuriomis aplinkybėmis taip pat gali būti priteisiama finansinė kompensacija. Papildomos informacijos apie teisminę peržiūrą Jungtinėje Karalystėje galima rasti Vyriausybės teisės departamento leidinyje „Judge Over Your Shoulder – a guide to good decision-making", skelbiama šiuo adresu: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/746170/JOYS-OCT-2018.pdf.

(122) ir (124) above konstatuojamąsias dalis). Todėl teisėsaugos institucijos pateiktas prašymas turėtų atitikti principą, pagal kurį nurodyti duomenų tvarkymo tikslai turi būti konkretūs, aiškūs ir teisėti ([188]), ir kad kompetentingos institucijos tvarkomi asmens duomenys turi derėti su tuo tikslu ir nebūti pertekliniai ([189]).

3.2.1.2. Teisėsaugos tikslais naudojami tyrimo įgaliojimai

(139) Siekdamos užkirsti kelią tik sunkiems nusikaltimams arba juos nustatyti ([190]), tam tikros teisėsaugos institucijos, pavyzdžiui, Nacionalinė nusikaltimų agentūra arba policijos vadovas ([191]), gali naudotis tiksliniais tyrimo įgaliojimais pagal 2016 m. TĮA. Tokiu atveju 2016 m. TĮA numatytos apsaugos priemonės bus taikomos kartu su apsaugos priemonėmis, numatytomis 2018 m. DAA 3 dalyje. Konkretūs tyrimo įgaliojimai, kuriais gali naudotis šios teisėsaugos institucijos, yra: tikslinis pasiklausymas (2016 m. TĮA 2 dalis), ryšio duomenų gavimas (2016 m. TĮA 3 dalis), ryšio duomenų saugojimas (2016 m. TĮA 4 dalis) ir tikslinis įrangos perėmimas (2016 m. TĮA 5 dalis). Perėmimas reiškia ryšio turinio įgijimą ([192]), o ryšio duomenų įgijimu ir saugojimu nesiekiama gauti ryšių turinio, bet veikiau sužinoti, „kas“, „kada“, „kur“ ir „kaip“ palaikė ryšį. Tai, pvz., yra ryšio laikas ir trukmė, ryšio iniciatoriaus ir adresato telefono numeris arba e. pašto adresas, o kartais prietaisų, iš kurių buvo palaikomas ryšys, buvimo vieta, telefono paslaugos abonentas arba detalizuota sąskaita ([193]). Įrangos perėmimas – tai metodų, naudojamų įvairiems duomenims iš įrangos, pvz., kompiuterių, planšetinių kompiuterių ir išmaniųjų telefonų, išgauti rinkinys, įskaitant kabelius, laidus ir saugojimo prietaisus ([194]).

(140) Tikslinio ryšių perėmimo įgaliojimai taip pat gali būti naudojami tais atvejais, kai tai „būtina siekiant taikyti ES savitarpio pagalbos priemones arba tarptautinio savitarpio pagalbos susitarimo nuostatas“ (vadinamasis savitarpio pagalbos orderis ([195])). Savitarpio pagalbos orderiai išduodami tik dėl ryšių perėmimo, o ne ryšio duomenų gavimo arba įrangos perėmimo. Šie specialūs įgaliojimai reguliuojami 2016 m. Tyrimo įgaliojimų akte (2016 m. TĮA) ([196]), kuris kartu su Anglijos, Velso ir Šiaurės Airijos 2000 m. Tyrimo įgaliojimų akto reglamentu (RIPA) ir 2000 m. Škotijos Tyrimo įgaliojimų akto reglamentu (Škotija) (RIPSA) sudaro teisinį pagrindą ir kuriame nustatyti tokių įgaliojimų naudojimui taikomi apribojimai ir apsaugos priemonės. 2016 m. TĮA taip pat nustatyta didelės apimties tyrimo įgaliojimų naudojimo tvarka, tačiau teisėsaugos institucijos jais negali pasinaudoti (šiais įgaliojimais gali naudotis tik žvalgybos agentūros) ([197]).

([188]) 2018 m. Jungtinės Karalystės DAA 36 straipsnio 1 dalis.

([189]) 2018 m. Jungtinės Karalystės DAA 37 straipsnis.

([190]) 2016 m. TĮA 263 straipsnio 1 dalyje nustatyta, kad „sunkus nusikaltimas“ – tai nusikalstama veika, už kurią suaugęs anksčiau neteistas asmuo galėtų būti pagrįstai nuteistas 3 arba daugiau metų laisvės atėmimo bausme, arba su smurto naudojimu susijusi veika, dėl kurios gaunama didelė finansinė nauda, arba veika, kurią padaro daug asmenų. Be to, gaunant ryšio duomenis pagal 2016 m. TĮA 4 dalį, pažymėtina, kad TĮA 87 straipsnio 10B dalyje nustatyta, kad „sunkus nusikaltimas“ – tai nusikaltimas, už kurį galima skirti 12 mėnesių arba ilgesnę laisvės atėmimo bausmę, arba nusikalstama veika, kurią padarė ne fizinis asmuo, arba kurios metu buvo siunčiamas pranešimas arba pažeidžiamas asmens privatumas.

([191]) Toliau išvardytos teisėsaugos institucijos gali prašyti išduoti tikslinio ryšių perėmimo orderį: Nacionalinės nusikaltimų agentūros generalinis direktorius, Metropolio policijos komisaras, Šiaurės Airijos policijos tarnybos vyriausiasis konsteblis, Škotijos policijos tarnybos vyriausiasis konsteblis, Jos Didenybės mokesčių ir muitų komisaras, Gynybos žvalgybos viršininkas ir asmuo, kuris yra valstybės arba teritorijos, esančios už Jungtinės Karalystės ribų, kompetentinga institucija pagal ES savitarpio pagalbos priemonę arba tarptautinį savitarpio pagalbos susitarimą (2016 m. TĮ 18 straipsnio 1 dalis).

([192]) Žr. 2016 m. TĮA 4 straipsnį.

([193]) Žr. 2016 m. TĮA 261 straipsnio 5 dalį ir Masinio ryšio duomenų gavimo praktikos kodeksą, su kuriuo galima rasti šiuo adresu: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf, 2,9 punktas.

([194]) Ryšių perėmimo įrangos praktikos kodeksas, galima rasti šiuo adresu: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715479/Equipment_Interference_Code_of_Practice.pdf , paragraph 2.2.

([195]) Pagal savitarpio pagalbos orderį Jungtinės Karalystės institucijai leidžiama teikti paramą už Jungtinės Karalystės teritorijos ribų esančiai institucijai siekiant perimti medžiagą ir atskleisti perimtą medžiagą tai institucijai laikantis tarptautinės savitarpio pagalbos priemonės nuostatų (2016 m. TĮA 15 straipsnio 4 dalis).

([196]) 2016 m. Tyrimo įgaliojimų įstatymas (žr. https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted) pakeitė įvairius įstatymus, susijusius su ryšių ir įrangos perėmimu ir ryšio duomenų gavimu, visų pirma 2000 m. RIPA I dalį, kurioje buvo nustatyta ankstesnė bendra teisės aktų sistema, skirta teisėsaugos ir nacionalinio saugumo institucijų tyrimo įgaliojimų naudojimui.

([197]) 2016 m. TĮA 138 straipsnio 1 dalis, 158 straipsnio 1 dalis, 178 straipsnio 1 dalis, 199 straipsnio 1 dalis.

(141) Kad galėtų pasinaudoti šiais įgaliojimais, institucijos privalo gauti orderį ([198]), kurį išduoda kompetentinga institucija ([199]) ir patvirtina nepriklausomas teismo komisaras ([200]) (vadinamoji dvigubo patikrinimo procedūra). Išduodant tokį orderį, atliekamas būtinumo ir proporcingumo patikrinimas ([201]). Kadangi šie 2016 m. TĮA numatyti tiksliniai tyrimo įgaliojimai yra tapatūs įgaliojimams, kuriais gali pasinaudoti nacionalinės saugumo agentūros, tokiems įgaliojimams taikomos sąlygos, apribojimai ir apsaugos priemonės išsamiai aptariami skirsnyje dėl Jungtinės Karalystės valdžios institucijų prieigos prie asmens duomenų ir jų naudojimo nacionalinio saugumo tikslais (žr. (177)ir tolesnes konstatuojamąsias dalis).

3.2.2. *Tolesnis surinktos informacijos naudojimas*

(142) Teisėsaugos institucijos vykdomas dalijimasis duomenimis su kita institucija kitais tikslais nei tie, dėl kurių jie iš pradžių buvo surinkti (vadinamasis tolesnis perdavimas) vykdomas laikantis tam tikrų sąlygų.

(143) Panašiai į tai, kas nustatyta Direktyvos (ES) 2016/680 4 straipsnio 2 dalyje, pagal 2018 m. DAA 36 straipsnio 3 dalį kompetentingos institucijos teisėsaugos tikslu surinktus asmens duomenis leidžiama tvarkyti toliau (tą gali daryti pradinis duomenų valdytojas arba kitas duomenų valdytojas) bet kuriuo kitu teisėsaugos tikslu, jeigu duomenų valdytojas pagal įstatymą turi įgaliojimus tvarkyti duomenis kitu tikslu ir duomenų tvarkymas yra būtinas ir proporcingas tam tikslui ([202]). Šiuo atveju gaunančiosios institucijos atliekamam duomenų tvarkymui taikomos visos 2018 m. DAA 3 dalyje numatytos apsaugos priemonės, kurios nurodytos (122) ir (124) konstatuojamosiose dalyse.

(144) Pagal Jungtinės Karalystės teisinę tvarką ir įvairius jos įstatymus toks tolesnis dalijimasis duomenimis yra leidžiamas. Visų pirma, i) pagal 2017 m. Skaitmeninės ekonomikos aktą valdžios institucijoms duomenimis leidžiama dalytis keliais tikslais, pvz., dėl bet kurio sukčiavimo viešajame sektoriuje atvejo, susijusio su valdžios institucijų nuostoliais arba nuostolių rizika ([203]), arba skolos valdžios institucijai arba Karalienei atveju ([204]), ii) pagal 2013 m. Nusikaltimų ir teismų aktą, kuriame leidžiama dalytis informacija su Nacionaline nusikaltimų agentūra (NCA) ([205]) kovos su sunkiais ir organizuotais nusikaltimais, jų tyrimo ir baudžiamojo persekiojimo tikslais; iii) pagal 2007 m. Sunkių nusikaltimų aktą, kuriame valdžios institucijoms leidžiama atskleisti informaciją kovos su sukčiavimu organizacijoms, siekiant užkirsti kelią sukčiavimui ([206]).

(145) Šiuose teisės aktuose aiškiai nustatyta, kad dalijimasis informacija turi atitikti 2018 m. DAA nustatytus principus. Be to, tam, kad policijai būtų lengviau vykdyti duomenų apsaugos pareigas pagal Jungtinės Karalystės BDAR, DAA ir 1998 m. Žmogaus teisių aktą, Policijos koledžas paskelbė Dalijimosi informacija leistinos profesinės praktikos aprašą ([207]). Dalijimosi atitiktis taikomai

([198]) 2016 m. TĮA 2 dalies 2 skyriuje pateiktas ribotas atvejų, kai ryšius galima perimti be orderio, skaičius. Tai yra: ryšių perėmimas siuntėjo arba gavėjo sutikimu, ryšių perėmimas administraciniais arba teisėsaugos tikslais, ryšių perėmimas tam tikrose institucijose (kalėjimuose, psichiatrijos ligoninėse ir imigrantų sulaikymo centruose), taip pat perėmimas, atliekamas pagal atitinkamą tarptautinį susitarimą.

([199]) Valstybės sekretorius dažniausiai yra institucija, išduodanti orderius pagal 2016 m. TĮA, o Škotijos ministrams yra suteikti įgaliojimai išduoti tikslinio ryšių perėmimo orderius, savitarpio pagalbos orderius ir tikslinio įrangos perėmimo orderius, kai perimamas asmuo arba patalpos, arba įranga, kurios turi būti klausomasi, yra Škotijoje (žr. 2016 m. TĮA 22 ir 103 straipsnius). Jeigu vykdomas tikslinis įrangos pasiklausymas, vyriausiasis teisėsaugos pareigūnas (kaip aprašyta 2016 m. TĮA 6 priedo 1 ir 2 dalyse) gali išduoti orderį laikydamasis 2016 m. TĮA 106 straipsnio sąlygų.

([200]) Teismo komisarai padeda tyrimo įgaliojimų komisarui (IPC), t. y. nepriklausomai įstaigai, kuri vykdo žvalgybos agentūrų tyrimo įgaliojimų naudojimo priežiūros funkcijas (daugiau informacijos žr. (162) konstatuojamąją dalį ir toliau).

([201]) Žr. visų pirma 2016 m. TĮA 19 ir 23 straipsnius.

([202]) 2018 m. DAA 36 straipsnio 3 dalis.

([203]) 2017 m. Skaitmeninės ekonomikos akto 56 straipsnis, galima rasti šiuo adresu: https://www.legislation.gov.uk/ukpga/2017/30/section/56.

([204]) 2017 m. Skaitmeninės ekonomikos akto 48 straipsnis.

([205]) 2013 m. Nusikaltimų ir teismų akto 7 straipsnis; galima rasti šiuo adresu: https://www.legislation.gov.uk/ukpga/2013/22/section/7.

([206]) 2007 m. Sunkių nusikaltimų akto 68 straipsnis, galima rasti šiuo adresu: https://www.legislation.gov.uk/ukpga/2007/27/contents.

([207]) Profesinė leistino dalijimosi informacija praktika, galima rasti šiuo adresu: https://www.app.college.police.uk/app-content/information-management/sharing-police-information.

duomenų apsaugos teisinei sistemai, žinoma, yra peržiūrima teismine tvarka ([208]).

(146) Be to, panašiai kaip Direktyvos (ES) 2016/680 9 straipsnyje, 2018 m. DAA nustatyta, kad bet kuriuo teisėsaugos tikslu surinkti asmens duomenys gali būti tvarkomi ne teisėsaugos tikslu, kai tai leidžiama daryti pagal įstatymą ([209]).

(147) Šios rūšies duomenimis galima dalytis dviem atvejais: 1) kai baudžiamosios teisėsaugos institucija dalijasi duomenimis su nebaudžiamosios teisėsaugos institucija, išskyrus žvalgybos agentūrą (pvz., finansų arba mokesčių institucija, konkurencijos institucija, jaunimo gerovės tarnyba ir pan.), ir 2) kai baudžiamosios teisėsaugos institucija duomenimis dalijasi su žvalgybos agentūra. Pirmuoju atveju asmens duomenų tvarkymui bus taikomas Jungtinės Karalystės BDAR, taip pat 2018 m. DAA 2 dalis. Komisija įvertino Jungtinės Karalystės BDAR ir 2018 m. DAA 2 dalies (12)–(111) konstatuojamosiose dalyse nustatytas priemones ir priėjo prie išvados, kad Jungtinė Karalystė užtikrina tinkamą asmens duomenų, perduotų pagal Reglamentą (ES) 2016/679 iš Europos Sąjungos į Jungtinę Karalystę, apsaugos lygį.

(148) Antruoju atveju dėl dalijimosi duomenimis, kuriuos surinko baudžiamosios teisėsaugos institucija su žvalgybos agentūra nacionalinio saugumo tikslais, teisinis pagrindas, kuriuo leidžiama taip dalytis, yra 2008 m. Kovos su terorizmu akto (2008 m. KTA) 19 straipsnis ([210]). Pagal šį aktą bet kuris asmuo gali teikti informaciją bet kuriai žvalgybos tarnybai, kad ta tarnyba įvykdytų bet kurią funkciją, įskaitant su nacionaliniu saugumu susijusią funkciją.

(149) Dėl sąlygų, kuriomis duomenimis galima dalytis nacionalinio saugumo tikslais, pažymėtina, kad pagal Žvalgybos tarnybų aktą ([211]) ir Saugumo tarnybų aktą ([212]) žvalgybos tarnybos gali gauti tik jų funkcijoms pagal įstatymą vykdyti būtinus duomenis. Teisėsaugos institucijos, kurios nori dalytis duomenimis su žvalgybos tarnybomis, turės įvertinti įvairius veiksnius / apribojimus ir kartu atsižvelgti į agentūrų funkcijas, nustatytas Žvalgybos tarnybų akte ir Saugumo tarnybų akte ([213]). 2008 m. KTA 20 straipsnyje aiškiai nurodyta, kad bet koks dalijimasis duomenimis pagal 19 straipsnį vis tiek turi atitikti duomenų apsaugos teisės aktus; tai reiškia, kad taikomi visi 2018 m. DAA 3 dalyje nustatyti apribojimai ir reikalavimai. Be to, kadangi kompetentingos institucijos yra valdžios institucijos 1998 m. Žmogaus teisių akto taikymo tikslais, jos privalo užtikrinti, kad jų veiksmai atitiktų Konvencijoje nustatytas teises, įskaitant EŽTK 8 straipsnį. Šiais apribojimais užtikrinama, kad teisėsaugos institucijos ir žvalgybos tarnybos visais duomenimis dalytųsi laikydamosi duomenų apsaugos teisės aktų ir EŽTK.

([208]) Žr., pvz., Sprendimą byloje *M, R prieš the Chief Constable of Sussex Police* [2019] EWHC 975 (Admin), kurioje aukštojo teismo buvo prašoma išnagrinėti dalijimosi duomenimis tarp policijos ir *Business Crime Reduction Partnership* (BCRP), t. y. organizacijos, įgaliotos valdyti pranešimo apie išimtis schemas, pagal kurias jos nariams draudžiama patekti į komercines patalpas, klausimą. Teismas įvertino dalijimąsi duomenimis, kuris buvo vykdomas remiantis susitarimu, kurio tikslas – apsaugoti visuomenę ir užkirsti kelią nusikaltimams, ir galiausiai padarė išvadą, kad dauguma dalijimosi duomenimis aspektų buvo teisėti, išskyrus aspektus, susijusius su tam tikra neskelbtina informacija, kuria dalijosi policija ir BCRP. Kitas pavyzdys – Sprendimas byloje *Cooper prieš NCA* [2019] EWCA Civ 16, kurioje apeliacinis teismas pritarė policijos ir Sunkaus organizuoto nusikalstamumo agentūros (SOCA), t. y. dabar NCA priklausančios teisėsaugos agentūros, dalijimuisi duomenimis.

([209]) 2018 m. DAA 36 straipsnio 4 dalis.

([210]) 2008 m. Kovos su terorizmu aktas, galima rasti šiuo adresu: https://www.legislation.gov.uk/ukpga/2008/28/section/19.

([211]) 1994 m. Žvalgybos tarnybų aktas, galima rasti šiuo adresu: https://www.legislation.gov.uk/ukpga/1994/13/contents.

([212]) 1989 m. Saugumo tarnybų aktas, galima rasti šiuo adresu: https://www.legislation.gov.uk/ukpga/1989/5/contents.

([213]) 1994 m. Žvalgybos tarnybos akto 2 straipsnio 2 dalyje nustatyta, kad „Vyriausioji žvalgybos tarnyba atsako už tos tarnybos veiksmingumą ir privalo užtikrinti: a) kad žvalgybos tarnyba negautų jokios kitos informacijos, išskyrus informaciją, kuri yra būtina jos funkcijoms tinkamai vykdyti, ir kad ji neatskleistų jokios informacijos, išskyrus tai, kas yra būtina i) siekiant to tikslo, ii) atsižvelgiant į nacionalinio saugumo interesus; iii) siekiant sunkių nusikaltimų prevencijos arba nustatymo, arba iv) nagrinėjant bet kokią baudžiamąją bylą, ir b) kad žvalgybos tarnyba nesiimtų jokių veiksmų, kad sustiprintų bet kurios Jungtinės Karalystės politinės partijos interesus“, o 1989 m. Saugumo žvalgybos akto 2 straipsnio 2 dalyje nustatyta, kad „generalinis direktorius atsako už žvalgybos tarnybos veiksmingumą ir privalo užtikrinti a) tvarką, kad žvalgybos tarnyba negautų jokios informacijos, išskyrus informaciją, kuri yra būtina tinkamam jos funkcijų įvykdymui, ir kad ji neatskleistų jokios informacijos, išskyrus tai, kas yra būtina siekiant sunkių nusikaltimų prevencijos arba nustatymo tikslo arba nagrinėjant bet kurią baudžiamąją bylą, ir b) kad tarnyba nesiimtų jokių veiksmų, kad sustiprintų kurios nors politinės partijos interesus, ir c) tvarką, dėl kurios susitarta su Nacionalinės nusikaltimų agentūros generaliniu direktoriumi, kuria remiantis tarnybos veikla pagal šio akto 1 straipsnio 4 dalį būtų koordinuojama su policijos pajėgomis, Nacionaline nusikaltimų agentūra ir kitomis teisėsaugos agentūromis“.

(150) Jeigu kompetentinga institucija su trečiosios valstybės teisėsaugos institucijomis ketina dalytis pagal 2018 m. DAA 3 dalį tvarkomais duomenimis, taikomi konkretūs reikalavimai ([214]). Tokie perdavimai visų pirma gali vykti, kai jie grindžiami tinkamumo taisyklėmis, kurias priėmė valstybės sekretorius arba, jeigu tokių taisyklių nėra, būtina užtikrinti tinkamas apsaugos priemones. 2018 m. DAA 75 straipsnyje nustatyta, kad tinkamos apsaugos priemonės yra tais atvejais, kai jos nustatomos teisine priemone, kurios numatytas adresatas privalo laikytis, arba kai duomenų valdytojas, įvertinęs visas aplinkybes, susijusias su tos rūšies asmens duomenų perdavimu trečiajai valstybei arba tarptautine organizacijai, padaro išvadą, kad esama tinkamų duomenų apsaugą užtikrinančių priemonių.

(151) Jeigu perdavimas nėra pagrįstas tinkamumo taisykles arba tinkamomis apsaugos priemonėmis, jis gali būti atliekamas tik tam tikromis konkrečiomis aplinkybėmis, kurios vadinamos specialiomis aplinkybėmis ([215]). Taip yra tuo atveju, kai duomenis perduoti būtina: a) kad būtų apsaugoti gyvybiniai duomenų subjekto arba kito asmens interesai; b) kad būtų apsaugoti teisėti duomenų subjekto interesai; c) kad būtų užkirstas kelias tiesioginei ir didelei grėsmei valstybės narės arba trečiosios valstybės visuomenės saugumui; d) individualiais atvejais atsižvelgiant į bet kokius teisėsaugos tikslus arba e) individualiais atvejais teisėtu tikslu (pvz., atsižvelgiant į teismo procesą arba siekiant gauti teisinę konsultaciją). Galima pažymėti, kad d ir e punktai netaikomi, jeigu duomenų subjekto teisės ir laisvės yra viršesnės už su perdavimu susijusį viešąjį interesą. Šis aplinkybių rinkinys atitinka konkrečias situacijas ir sąlygas, kurios pagal Direktyvos (ES) 2016/680 38 straipsnį laikomos „nukrypti leidžiančiomis nuostatomis“.

(152) Be to, jeigu teisėsaugos institucijų įrodymai, kuriuos jos gavo remdamosi orderiu, pagal kurį leidžiama perimti ryšius arba įrangą, perduodami į trečiąja valstybę, pagal 2016 m. TĮA taikomos privalomos papildomos apsaugos priemonės. Visų pirma toks informacijos atskleidimas, kuris apibrėžiamas kaip „informacijos atskleidimas užsienyje“, leidžiamas tik jeigu išduodančioji institucija mano, kad yra nustatytos tinkamos taisyklės, kuriomis ribojamas asmenų, kuriems atskleidžiami duomenys, skaičius, mastas, kuriuo leidžiama atskleisti arba leisti susipažinti su bet kokia medžiaga, taip pat mastas, kuriuo bet kokia medžiaga kopijuojamas, ir padarytų kopijų skaičius. Be to, išduodančioji institucija gali manyti, kad būtinos atitinkamos taisyklės, padedančios užtikrinti, kad kiekviena bet kurios medžiagos dalies padaryta kopija būtų sunaikinta iš karto, kai nebegalioja jokie atitinkami jos saugojimo pagrindai (jeigu tokios kopijos nebuvo sunaikintos anksčiau) ([216]).

(153) Galiausiai, ateityje galėtų būti taikomos specialios tolesnio duomenų perdavimo iš Jungtinės Karalystės į Jungtines Valstijas formos pagal Jungtinės Didžiosios Britanijos ir Šiaurės Airijos Karalystės vyriausybės ir Jungtinių Amerikos Valstijų vyriausybės susitarimą dėl prieigos prie elektroninių duomenų siekiant kovoti su sunkiais nusikaltimais (toliau – Jungtinės Karalystės ir JAV susitarimas arba Susitarimas) ([217]), sudarytą 2019 m. spalio mėn. ([218]) Nors šio sprendimo priėmimo metu Jungtinės Karalystės ir JAV susitarimas dar nėra įsigaliojęs, numatomas jo įsigaliojimas gali turėti įtakos tolesniam duomenų, pirmą kartą perduotų Jungtinei Karalystei pagal šį sprendimą, perdavimui į JAV. Kalbant konkrečiau, iš ES Jungtinėje Karalystėje veikiantiems paslaugų teikėjams perduodamiems duomenims galėtų būti taikomi kompetentingų JAV teisėsaugos institucijų išduoti elektroninių įrodymų pateikimo orderiai, kuriuos Jungtinėje Karalystėje būtų galima taikyti įsigaliojus šiam Susitarimui. Dėl šių priežasčių taikant šį sprendimą svarbu įvertinti sąlygas ir apsaugos priemones, kuriomis tokie orderiai gali būti išduoti ir įvykdyti.

([214]) Žr. 2018 m. DAA 3 dalies 5 skyrių.

([215]) 2018 m. DAA 76 straipsnis.

([216]) 2016 m. TĮA 54 ir 130 straipsniai. Išduodančiosios institucijos privalo išnagrinėti poreikį nustatyti konkrečias užsienio institucijoms perduotos medžiagos apsaugos priemones ir taip užtikrinti, kad duomenims būtų taikomos apsaugos priemonės, susijusios su duomenų saugojimu, sunaikinimu ir atskleidimu, kurios būtų panašios į 2016 m. TĮA 53 ir 129 straipsniuose nustatytas priemones.

([217]) Didžiosios Britanijos ir Šiaurės Airijos Jungtinės Karalystės vyriausybės ir Jungtinių Amerikos Valstijų vyriausybės susitarimas dėl prieigos prie elektroninių duomenų siekiant kovoti su sunkiais nusikaltimais, galima rasti šiuo adresu: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836969/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf.

([218]) Jungtinių Amerikos Valstijų CLOUD aktas – tai JAV federalinis įstatymas, priimtas 2018 m. kovo 23 d., kuriuo iš dalies pakeičiamas 1986 m. Saugomų ryšių aktas ir paaiškinama, kad JAV paslaugų teikėjai privalo laikytis JAV įsakymų atskleisti turinio ir su turiniu nesusijusius duomenis, nepaisant to, kur tokie duomenys yra saugomi. Pagal CLOUD aktą taip pat leidžiama sudaryti vykdomuosius susitarimus su užsienio vyriausybėmis, kuriais remdamiesi JAV paslaugų teikėjai galėtų teikti turinio duomenis tiesiogiai šioms užsienio vyriausybėms (CLPUD akto tekstą galima rasti šiuo adresu: https://www.congress.gov/115/bills/s2383/BILLS-115s2383is.pdf).

(154) Dėl šių priežasčių taikant šį sprendimą svarbu įvertinti sąlygas ir apsaugos priemones, kuriomis tokie orderiai gali būti išduoti ir įvykdyti. Šiuo klausimu reikėtų pažymėti, kad, pirma, Susitarimas, atsižvelgiant į jo materialinę taikymo sritį, taikomas tik nusikaltimams, už kuriuos skiriama maksimali ne trumpesnė kaip trejų metų laisvės atėmimo bausmė (apibrėžiama kaip „sunkus nusikaltimas“) ([219]), įskaitant teroristinę veiklą. Antra, kitoje jurisdikcijoje tvarkomi duomenys pagal šį susitarimą gali būti gauti tik vadovaujantis „orderiu, <...> kurį pagal išduodančiosios šalies vidaus teisę iki orderio vykdymo bylos arba jos metu gali peržiūrėti arba prižiūrėti teismas, teisėjas, magistratas arba kita nepriklausoma institucija“ ([220]). Trečia, bet kuris orderis turi „būti pagrįstas aiškiai ir įtikinamais faktais, visų pirma, teisėtumu, ir tiriamos veikos rimtumu“ ([221]), be to, jis turi būti skirtas konkrečioms sąskaitoms ir jame turi būti nurodyta konkretaus asmens tapatybė, sąskaita, adresas arba asmeninis prietaisas, arba bet kuris kitas konkretus identifikatorius“ ([222]). Ketvirta, pagal šį susitarimą gautiems duomenims taikomos apsaugos priemonės, kurios yra lygiavertės konkrečioms apsaugos priemonėms, numatytoms vadinamajame ES ir JAV skėtiniame susitarime ([223]), t. y. 2016 m. gruodžio mėn. ES ir JAV sudarytas išsamus susitarimas dėl duomenų apsaugos, kuriame nustatytos apsaugos priemonės ir teisės, taikomos duomenų perdavimams teisėsaugos bendradarbiavimo srityje, kurios į šį susitarimą įtraukiamos *mutatis mutandis* pagrindu, visų pirma siekiant atsižvelgti į konkretų perdavimų pobūdį (t. y. perdavimui iš privačių operatorių teisėsaugos institucijoms, užuot perdavus tarp teisėsaugos institucijų) ([224]). Jungtinės Karalystės ir JAV susitarime konkrečiai nustatyta, kad lygiavertės apsaugos priemonės, numatytos ES ir JAV skėtiniame susitarime, bus taikomos „visai asmeninei informacijai, kuri bus parengta vykdant orderius, kuriems taikomas Susitarimas, kad būtų užtikrintos lygiavertės apsaugos priemonės“ ([225]).

(155) Todėl duomenims, kurie JAV institucijoms buvo perduoti pagal ES ir JAV susitarimą, turėtų būti taikomos ES teisės akte nustatytos apsaugos priemonės, įskaitant būtinus pritaikymus, kuriais atsižvelgiama į aptariamų perdavimų pobūdį. Jungtinės Karalystės institucijos taip pat patvirtino, kad skėtiniame susitarime numatytos apsaugos priemonės bus taikomos visiems pagal Susitarimą parengtiems arba išsaugotiems asmens duomenims, nepaisant prašymą teikiančios įstaigos pobūdžio arba rūšies (pvz., JAV federalinės ir valstijos teisėsaugos institucijos), todėl lygiavertė apsauga turi būti užtikrinama visais atvejais. Tačiau Jungtinės Karalystės institucijos taip pat paaiškino, kad Jungtinė Karalystė ir JAV dar turi aptarti konkretaus duomenų apsaugos priemonių įgyvendinimo klausimus. Derybose su Europos Komisijos tarnybomis dėl šio sprendimo Jungtinės Karalystės institucijos patvirtino, kad jos Susitarimo įsigaliojimui pritars tik įsitikinusios, kad jo įgyvendinimas atitinka jame nustatytas teisines prievoles, įskaitant aiškų duomenų apsaugos standartų laikymąsi dėl bet kurių pagal šį susitarimą prašomų duomenų. Kadangi galimas Susitarimo įsigaliojimas gali daryti poveikį šiame sprendime vertinamam apsaugos lygiui, bet kurią informaciją ar būsimą paaiškinimą dėl to, kaip JAV laikysis savo pareigų pagal Susitarimą, Jungtinė Karalystė turėtų perduoti Europos Komisijai iš karto, kai tik jis bus parengtas, ir bet kuriuo atveju iki įsigaliojant Susitarimui, siekdama užtikrinti tinkamą šio sprendimo stebėseną pagal Reglamento (ES) 2016/679 45 straipsnio 4 dalį. Ypatingas dėmesys bus skirtas Skėtiniame susitarime nustatytų apsaugos priemonių taikymui ir pritaikymui atsižvelgiant į konkrečią perdavimų, kuriems taikomas Jungtinės Karalystės ir JAV susitarimas, rūšį.

(156) Konkrečiau, vykdant nuolatinę šio sprendimo stebėseną, bus atsižvelgta į bet kokį svarbų pokytį, susijusį su Susitarimo įsigaliojimu ir taikymu, be kita ko, atsižvelgiant į būtinas pasekmes, kurios turi atsirasti atsiradus bet kokiems požymiams, kad nebeužtikrinamas iš esmės lygiavertis apsaugos lygis.

3.2.3. *Priežiūra*

(157) Priklausomai nuo įgaliojimų, kuriais kompetentingos institucijos naudojasi tvarkydamos asmens duomenis teisėsaugos tikslu (pagal 2018 m. DAA arba 2016 m. TĮA), šių įgaliojimų naudojimą prižiūri įvairios įstaigos. Visų

([219]) Susitarimo 1 straipsnio 14 dalis.
([220]) Susitarimo 5 straipsnio 2 dalis.
([221]) Susitarimo 5 straipsnio 1 dalis.
([222]) Susitarimo 4 straipsnio 5 dalis. Perėmimui realiuoju laiku taikomas papildomas ir griežtesnis standartas: nutarimai turi galioti ribotą trukmę, kuri negali būti ilgesnė nei tai, kas pagrįstai būtina įsakymo tikslui pasiekti, ir jis priimamas tik jeigu tos pačios informacijos pagrįstai negalima gauti mažiau intervenciniu būdu (Susitarimo 5 straipsnio 3 dalis).
([223]) Jungtinių Amerikos Valstijų ir Europos Sąjungos susitarimas dėl su nusikalstamų veikų prevencija, tyrimu, atskleidimu ir baudžiamuoju persekiojimu susijusios asmeninio pobūdžio informacijos apsaugos, OL L 336, 2016 12 10, p. 3–13, galima rasti šiuo adresu: https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:22016A1210(01)&from=LT.
([224]) Susitarimo 9 straipsnio 1 dalis.
([225]) Susitarimo 9 straipsnio 1 dalis.

pirma informacijos komisaras prižiūri asmens duomenų tvarkymą, kuriam taikoma 2018 m. DAA 3 dalis ([226]). Nepriklausomą ir teisminę tyrimo įgaliojimų pagal 2016 m. TĮA priežiūrą užtikrina Tyrimo įgaliojimų komisaro biuras (IPCO) ([227]) (ši dalis aptarta (250)–(255) konstatuojamosiose dalyse). Be to, papildomą priežiūrą garantuoja parlamentas ir kitos įstaigos.

3.2.3.1. 2018 m. DAA 3 dalies įgyvendinimo priežiūra

(158) Bendrosios informacijos komisaro, kurio nepriklausomumas ir organizacinė struktūra paaiškinta (87) konstatuojamojoje dalyje, funkcijos, susijusios su asmens duomenų tvarkymu pagal 2018 m. DAA 3 dalį, nustatytos 2018 m. DAA 13 priede. Pagrindinė informacijos komisaro užduotis – stebėti ir užtikrinti 2018 m. DAA 3 dalies įgyvendinimą, taip pat didinti visuomenės informuotumą, patarti parlamentui, vyriausybei ir kitoms institucijoms bei įstaigoms. Siekiant išlaikyti teismų nepriklausomumą, informacijos komisarui neleidžiama vykdyti savo funkcijų tais atvejais, kai asmens duomenis tvarko teisminius įgaliojimus turintis fizinis asmuo arba teismines funkcijas vykdantis bendrosios kompetencijos arba specializuotas teismas. Šiomis aplinkybėmis priežiūros funkcijas turėtų vykdyti kitos įstaigos, kaip paaiškinta (99)–(103) konstatuojamosiose dalyse.

(159) Komisaras turi bendruosius tyrimo, taisomuosius, leidimų suteikimo ir patariamuosius įgaliojimus, susijusius su asmens duomenų tvarkymu pagal 3 dalį. Komisaras visų pirma turi įgaliojimus pranešti duomenų valdytojui arba duomenų tvarkytojui apie tariamą 2018 m. DAA 3 dalies pažeidimą, įteikti duomenų valdytojui arba duomenų tvarkytojui, kuris pažeidė akto 3 dalį, įspėjimus arba papeikimus, taip pat savo iniciatyva arba paprašius teikti nuomones parlamentui, vyriausybei ir kitoms institucijoms bei įstaigoms, taip pat visuomenei bet kuriuo su asmens duomenų apsauga susijusiu klausimu ([228]).

(160) Be to, komisaras turi įgaliojimus priimti informacinius pranešimus ([229]), vertinimo pranešimus ([230]) ir vykdymo pranešimus ([231]), taip pat įgaliojimus susipažinti su duomenų valdytojų ir duomenų tvarkytojų dokumentais, patekti į jų patalpas ([232]) ir skirti administracines baudas priimdamas pranešimus apie nuobaudą ([233]). Informacijos komisaro reguliavimo veiksmų politikoje išdėstytos aplinkybės, kuriomis jis priima informacijos, vertinimo, vykdymo pranešimus ir pranešimus apie nuobaudą ([234]) (taip pat žr. (93) konstatuojamąją dalį ir Direktyvos (ES) 2016/680 101–102 konstatuojamąsias dalis dėl sprendimo dėl tinkamumo).

(161) Remdamasis savo naujausiomis metinėmis ataskaitomis (2018–2019 m. ([235]), 2019–2020 m. ([236])), informacijos komisaras atliko įvairius tyrimus ir ėmėsi vykdymo priemonių dėl teisėsaugos institucijų vykdomo duomenų tvarkymo. Pavyzdžiui, komisaras atliko tyrimą ir 2019 m. spalio mėn. paskelbė išvadą dėl to, kaip teisėsaugos institucijos naudoja veido atpažinimo technologijas viešose vietose. Tyrime daugiausia dėmesio visų pirma skirta Pietų Velso policijos ir Metropoliteno policijos tarnybos (MPS) naudojamiems gyvo veido atpažinimo pajėgumams. Informacijos komisaras taip pat ištyrė MPS „Gangs matrix“ ([237]) ir nustatė įvairių rimtų duomenų apsaugos teisės pažeidimų, dėl kurių galėjo sumažėti visuomenės pasitikėjimas matrica ir tuo, kaip naudojami duomenys. 2018 m. lapkričio mėn. informacijos komisaras priėmė vykdymo pranešimą, o MPS paskui ėmėsi veiksmų, kurie yra būtini siekiant padidinti saugumą ir atskaitomybę ir užtikrinti, kad duomenys būtų naudojami proporcingai. Kitas vykdymo veiksmų šioje srityje pavyzdys – 325 000 GBP

([226]) 2018 m. DAA 116 straipsnis.
([227]) Žr. 2016 m. TĮA, ypač 1 skyriaus 8 dalį.
([228]) 2018 m. DAA 13 priedo 2 dalis.
([229]) Įpareigoja duomenų valdytoją ir duomenų tvarkytoją (ir tam tikrais atvejais bet kurį kitą asmenį) pateikti būtiną informaciją (2018 m. DAA 142 straipsnis).
([230]) Leidžia atlikti tyrimus ir auditą, kuriame gali būti reikalaujama, kad duomenų valdytojas arba duomenų tvarkytojas leistų komisarui patekti į konkrečias patalpas, patikrinti arba išnagrinėti dokumentus arba patikrinti ir apžiūrėti įrangą, duomenų valdytojų vardu apklausti asmens duomenis tvarkančius asmenis (2018 m. DAA 146 straipsnis).
([231]) Leidžia įgyvendinti taisomuosius įgaliojimus, pagal kuriuos reikalaujama, kad duomenų valdytojai / duomenų tvarkytojai imtųsi konkrečių veiksmų arba jų nesiimtų (2018 m. DAA 149 straipsnis).
([232]) 2018 m. DAA 154 straipsnis.
([233]) 2018 m. DAA 155 straipsnis.
([234]) Reguliavimo veiksmų politika, žr. 96 išnašą.
([235]) Informacijos komisaro 2018–2019 m. metinė ataskaita ir finansinės ataskaitos, žr. 101 išnašą.
([236]) Informacijos komisaro 2019–2020 m. metinė ataskaita ir finansinės ataskaitos, žr. 82 išnašą.
([237]) Duomenų bazė, kurioje registruojami žvalgybos duomenys, susiję su įtariamais gaujų nariais ir gaujų padarytų nusikaltimų aukomis.

bauda, kurią 2018 m. gegužės mėn. komisaras skyrė Karalienės prokuratūrai už tai, kad pastaroji pametė neužšifruotus kompaktinius diskus su policijos apklausų įrašais. Informacijos komisaras taip pat atliko tyrimus platesnėmis temomis, pvz., per pirmąjį 2020 m. pusmetį atliko tyrimą dėl mobiliųjų telefonų duomenų išgavimo policijos veiklos tikslais ir dėl to, kaip policija tvarko aukų duomenis. Be to, komisaras dabar tiria bylą dėl teisėsaugos institucijų prieigos prie privataus sektoriaus subjekto „Clearview AI Inc." turimų duomenų ([238]).

(162) Be informacijos komisarui suteiktų vykdymo įgaliojimų, kurie aprašyti (160) ir (161) konstatuojamosiose dalyse, tam tikri duomenų apsaugos teisės aktų pažeidimai laikomi nusikalstamomis veikomis, todėl už jų padarymą gali būti skiriamos baudžiamosios sankcijos (2018 m. DAA 196 straipsnis). Pavyzdžiui, baudžiamosios sankcijos gali būti skirtos už tai, kad asmens duomenys buvo gauti, atskleisti arba saugomi be duomenų valdytojo sutikimo, už tarpininkavimą asmens duomenis atskleidžiant kitam asmeniui be duomenų valdytojo sutikimo ([239]), į informaciją, kurią sudaro nuasmeninti asmens duomenys, vėl įtraukiant tapatybės duomenis be duomenų valdytojo, atsakingo už asmens duomenų nuasmeninimą, sutikimo ([240]), tyčia trukdant komisarui vykdyti savo įgaliojimus, susijusius su asmens duomenų patikrinimu pagal tarptautinius įsipareigojimus ([241]) ir jeigu atsakant į informacinį pranešimą pateikiami klaidingi pareiškimai arba sunaikinama su informaciniu pranešimu arba vertinimo pranešimu susijusi informacija ([242]).

3.2.3.2. Kitos įstaigos, vykdančios priežiūrą baudžiamosios teisėsaugos srityje

(163) Be informacijos komisaro, baudžiamosios teisėsaugos srityje veikia keletas priežiūros institucijų, turinčių konkrečius įgaliojimus, susijusius su duomenų apsaugos klausimais. Tai, pvz., yra biometrinės medžiagos saugojimo ir naudojimo komisaras (toliau – biometrinių duomenų komisaras) ([243]) ir stebėjimo kamerų komisaras ([244]).

3.2.3.3. Parlamentinė priežiūra baudžiamosios teisėsaugos srityje

(164) Vidaus reikalų atskirasis komitetas (HASC) užtikrina parlamentinę priežiūrą baudžiamosios teisenos srityje. Šį komitetą sudaro 11 parlamento narių, atrinktų iš trijų didžiausių politinių partijų. Komiteto užduotis – analizuoti Vidaus reikalų ministerijos ir susijusių valdžios įstaigų, įskaitant policiją ir NCA, kurių darbą komitetas gali tikrinti atidžiai, išlaidas, administravimą ir politiką ([245]).

([238]) Žr. Informacijos komisaro pareiškimą, kurį galima rasti šiuo adresu: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/07/oaic-and-ico-open-joint-investigation-into-clearview-ai-inc/.

([239]) 2018 m. DAA 170 straipsnis.

([240]) 2018 m. DAA 171 straipsnis.

([241]) 2018 m. DAA 119 straipsnio 6 dalis.

([242]) 2019 m. balandžio 1 d. – 2020 m. kovo 31 d. laikotarpio finansiniais metais atliktų informacijos komisaro tyrimų rezultatas: keturi perspėjimai ir aštuoni baudžiamieji persekiojimai. Šiose bylose baudžiamasis persekiojimas buvo vykdomas pagal 1998 m. Duomenų apsaugos akto 55 straipsnį, 2000 m. Informacijos laisvės akto 77 straipsnį ir 2018 m. Duomenų apsaugos akto 170 straipsnį. 75 proc. bylų atsakovai pripažino kaltę, todėl neprireikė tęsti teismo procesų, kuriuose patiriama papildomų išlaidų. (Informacijos komisaro 2019–2020 m. metinė ataskaita ir finansinės ataskaitos, žr. 87 išnašą, p. 40).

([243]) Biometrinių duomenų komisaro pareigybė buvo įsteigta 2012 m. Laisvės apsaugos aktu (angl. PoFA) (žr. https://www.legislation.gov.uk/ukpga/2012/9/contents). Bet kitų funkcijų, biometrinių duomenų komisaras nusprendžia, kada policija gali, o kada negali saugoti DNR profilio įrašų ir pirštų antspaudų, kurie buvo paimti iš areštuotų, tačiau padarius kvalifikuotą nusikaltimą neapkaltintų asmenų (pagal Policijos aktą priimto 1984 m. etikos kodekso 63G straipsnis). Biometrinių duomenų komisaras taip pat yra bendrai atsakingas už DNR ir pirštų antspaudų saugojimą ir naudojimą bei jų saugojimą siekiant užtikrinti nacionalinį saugumą (2012 m. Laisvių apsaugos akto 20 straipsnio 2 dalis). Biometrinių duomenų komisaras skiriamas pagal Valstybės pareigūnų skyrimo kodeksą (kodeksas pateikiamas adresu: Https://www.gov.uk/government/publications/governance-code-for-public-appointments,, o jo paskyrimo sąlygose aiškiai pasakyta, kad tik Vidaus reikalų sekretorius ir tik griežtai apibrėžtomis aplinkybėmis gali jį atleisti iš pareigų; tai, be kita ko, pareigų nevykdymas tris mėnesius, apkaltinamasis nuosprendis dėl nusikalstamos veikos arba paskyrimo sąlygų nesilaikymas.

([244]) Stebėjimo kamerų komisaro pareigybė buvo įsteigta 2012 m. Laisvių apsaugos aktu ir jo pareiga – skatinti laikytis stebėjimo kamerų praktikos kodekso; peržiūrėti, kaip šis kodeksas taikomas ir konsultuoti ministrus būtinybės pakeisti šį kodeksą klausimais. Komisaras skiriamas pagal tas pačias taisykles kaip ir už biometrinius rodiklius atsakingi komisarai; jis turi panašius įgaliojimus, išteklius ir apsaugą nuo atleidimo iš pareigų.

([245]) Žr. https://committees.parliament.uk/committee/83/home-affairs-committee/news/100537/work-of-the-national-crime-agency-scrutinised/.

(165) Komitetas per savo nustatytus terminus gali pats nustatyti tyrimo temą, įskaitant konkrečių atvejų tyrimą, jeigu klausimas nepriklauso teismo kompetencijai. Komitetas taip pat gali prašyti įvairių atitinkamų grupių ir asmenų pateikti rašytinius ir žodinius įrodymus. Jis rengia savo išvadų ataskaitas ir teikia vyriausybei rekomendacijas ([246]). Tikimasi, kad vyriausybė kiekvieną ataskaitos rekomendaciją įgyvendins ir tai padarys per 60 dienų ([247]).

(166) Stebėjimo srityje komitetas taip pat parengė ataskaitą dėl 2000 m. Tyrimo įgaliojimų akto reglamento (2000 m. RIPA) ([248]), kurioje priėjo prie išvados, kad 2000 m. RIPA neatitiko tikslo. Į jo ataskaitą buvo atsižvelgta svarbias 2000 m. RIPA dalis pakeičiant 2016 m. TĮA. Išsamų tyrimų sąrašą galima rasti komiteto svetainėje ([249]).

(167) HASC užduotis Škotijoje vykdo Policijos veiklos teisingumo pakomitetis, i Šiaurės Airijoje jas vykdo Teisingumo komitetas ([250]).

3.2.4. *Teisių gynimas*

(168) Dėl teisėsaugos institucijų tvarkomų asmens duomenų, pažymėtina, kad pagal 2018 m. DAA 3 dalį ir 2016 m. TĮA, taip pat pagal 1998 m. Žmogaus teisių aktą galima pasinaudoti teisių gynimo mechanizmais.

(169) Šiais įvairiais mechanizmais duomenų subjektams suteikiamos veiksmingos administracinės ir teisminės teisių gynimo priemonės, kuriomis jiems sudaromos sąlygos visų pirma užtikrinti savo teises, įskaitant teisę susipažinti su savo asmens duomenimis arba ištaisyti ar ištrinti tokius duomenis.

(170) Pirma, pagal 2018 m. DAA 165 straipsnį duomenų subjektas turi teisę pateikti skundą informacijos komisarui, jeigu mano, kad, atsižvelgiant į jo asmens duomenis, buvo padarytas 2018 m. DAA 3 dalies pažeidimas. Informacijos komisaras turi įgaliojimus įvertinti, ar duomenų valdytojas ir duomenų tvarkytojas laikosi 2018 m. DAA, reikalauti, kad jie imtųsi būtinų veiksmų reikalavimų nesilaikymo atveju, ir skirti baudas ([251]). Informacijos komisaras turi įgaliojimus įvertinti, ar duomenų valdytojas ir duomenų tvarkytojas laikosi 2018 m. DAA, reikalauti, kad jie imtųsi būtinų veiksmų reikalavimų nesilaikymo atveju, ir skirti baudas.

([246]) Atrankos komitetai, įskaitant Vidaus reikalų atrankos komitetą, privalo laikytis Bendruomenių rūmų darbo tvarkos taisyklių. Darbo tvarkos taisyklės – tai taisyklės, dėl kurių susitarė Bendruomenių rūmai ir kuriose nustatyta parlamento veikimo tvarka. Atrankos komitetų kompetencija yra plati, o darbo tvarkos taisyklių 152 straipsnio 1 dalyje nustatyta, kad „[a]trankos komitetai skiriami pagrindinių vyriausybės departamentų, kaip nustatyta šių taisyklių 2 dalyje, ir susijusių valdžios įstaigų išlaidų, administravimo ir politikos klausimams nagrinėti“. Taip sudaromos sąlygos Vidaus reikalų atrankos komitetui nagrinėti bet kurią Vidaus reikalų ministerijos politiką, kurioje, be kita ko, reglamentuojami su tyrimo įgaliojimais susiję politiniai klausimai (ir atitinkami teisės aktai). Be to, darbo tvarkos taisyklių 152 straipsnio 4 dalyje aiškiai nurodyta, kad komitetai turi įvairius įgaliojimus, įskaitant gebėjimą prašyti asmenų pateikti įrodymus arba dokumentus konkrečiu klausimu ir pateikti ataskaitas. Su einamasiais ir ankstesniais komiteto tyrimais galima susipažinti adresu https://committees.parliament.uk/committee/83/home-affairs-committee/.

([247]) Anglijos ir Velso vidaus reikalų atrankos komiteto įgaliojimai nustatyti Bendruomenių rūmų darbo tvarkos taisyklėse, kurias galima rasti šiuo adresu: https://www.parliament.uk/business/publications/commons/standing-orders-public11/.

([248]) Galima rasti šiuo adresu: https://publications.parliament.uk/pa/cm201415/cmselect/cmhaff/711/71103.htm

([249]) Galima rasti šiuo adresu: https://committees.parliament.uk/committee/83/home-affairs-committee

([250]) Škotijos teisingumo pakomitečio policijos veiklos klausimais taisykles galima rasti šiuo adresu: https://www.parliament.scot/parliamentarybusiness/CurrentCommittees/justice-committee.aspx, o Šiaurės Airijos teisingumo komiteto taisykles galima rasti šiuo adresu: http://www.niassembly.gov.uk/assembly-business/standing-orders/ ]

([251]) Paskutinėje informacijos komisaro ataskaitoje gauti ir išnagrinėti skundai suskirstyti pagal skundo pobūdį. Visų pirma gautų skundų dėl „policijos įrašai ir informacija apie teistumą“ skaičius sudaro 6 proc. viso gautų skundų skaičiaus (t. y. 1 proc. daugiau, palyginti su ankstesniais finansiniais metais). Iš metinės ataskaitos taip pat matyti, kad skundai dėl subjektų prašymų leisti susipažinti su duomenimis sudaro didžiausią dalį (46 proc. viso skundų skaičiaus, t. y. 8 proc. daugiau, palyginti su ankstesniais finansiniais metais) (Informacijos komisaro 2019–2020 m. metinė ataskaita, p. 55; žr. 88 išnašą).

(171) Antra, 2018 m. DAA nustatyta teisė į teisinę gynybą prieš informacijos komisarą, jeigu jis tinkamai neišnagrinėja duomenų subjekto skundo. Konkrečiau, jeigu komisaras nesugeba „pasistūmėti į priekį“ ([252]) nagrinėdamas duomenų subjekto pateiktą skundą, skundo pateikėjas turi teisę imtis teisminių teisių gynimo priemonių, nes gali kreiptis į pirmosios instancijos specializuotą teismą ([253]) ir prašyti, kad komisaras būtų įpareigotas imtis nagrinėti skundą arba informuoti skundo pateikėją apie padarytą pažangą ([254]). Be to, bet kuris asmuo, kuris iš komisaro gauna bet kurį iš minėtų pranešimų (informacinį, vertinimo ar vykdymo pranešimą arba pranešimą apie nuobaudą), gali skųstis specializuotam pirmosios instancijos teismui. Jeigu specializuotas teismas mano, kad komisaro sprendimas neatitinka įstatymo arba kad informacijos komisaras turėjo kitaip pasinaudoti savo diskrecija, specializuotas teismas privalo priimti skundą arba pakeisti kitą pranešimą arba sprendimą, kurį pateikė arba priėmė informacijos komisaras ([255]).

(172) Trečia, asmenys tiesiogiai teismuose gali pasinaudoti teisminėmis teisių gynimo priemonėmis prieš duomenų valdytojus ir duomenų tvarkytojus. Visų pirma pagal 2018 m. DAA 167 straipsnį duomenų subjektas gali pateikti prašymą teismui dėl jo teisių pažeidimo pagal duomenų apsaugos teisės aktus ir teismas, priimdamas nutartį, gali prašyti, kad duomenų valdytojas imtųsi bet kokių veiksmų (arba jų nesiimtų), susijusių su duomenų tvarkymu, kad laikytųsi 2018 m. DAA. Be to, pagal 2018 m. DAA 169 straipsnį bet kuris asmuo, kuris dėl duomenų teisės akte (įskaitant 2018 m. DAA 3 dalį), išskyrus Jungtinės Karalystės BDAR, nustatyto reikalavimo pažeidimo patyrė žalos, turi teisę, kad duomenų valdytojas arba duomenų tvarkytojas kompensuotų jam tą žalą, išskyrus atvejus, kai duomenų valdytojas arba duomenų tvarkytojas įrodo, kad jis bet kuriuo atveju neatsako už įvykį, dėl kurio atsirado žala. Žalą sudaro finansiniai nuostoliai ir su jais nesusijusi žala, pvz., stresas.

(173) Galiausiai bet kuris asmuo, kuris mano, kad bet kuri valdžios institucija pažeidė jo teises, įskaitant teises į privatumą ir duomenų apsaugą, Jungtinės Karalystės teismuose pagal 1998 m. Žmogaus teisių aktą ([256]) gali pasinaudoti teisių gynimo priemonėmis ir, išnaudojęs visas nacionalines teisių gynimo priemones, asmuo, nevyriausybinė organizacija ir asmenų grupės Europos Žmogaus Teisių Teisme gali pasinaudoti teisių gynimo priemonėmis dėl Europos žmogaus teisių konvencijoje garantuojamų teisių pažeidimų ([257]) (žr. (111)konstatuojamojoje dalyje).

3.2.4.1. Pagal 2016 m. TĮA galimi teisių gynimo mechanizmai

(174) Asmenys nuo 2016 m. TĮA pažeidimų savo teises gali ginti specializuotame tyrimo įgaliojimų teisme. Pagal 2016 m. TĮA galimi teisių gynimo būdai aprašyti (263)–(269) konstatuojamosiose dalyse.

([252]) 2018 m. DAA 166 straipsnyje konkrečiai nurodyti šie atvejai: a) komisaras nesiima tinkamų veiksmų, kad reaguotų į skundą, b) komisaras nepateikia skundo pateikėjui informacijos apie skundo nagrinėjimo eigą arba rezultatą prieš pasibaigiant 3 mėnesių terminui, kuris pradedamas skaičiuoti nuo dienos, kurią komisaras gavo skundą, arba c) jeigu komisaras, per tą terminą nebaigęs nagrinėti skundo, nepateikia skundo pateikėjui tokios informacijos per paskesnį 3 mėnesių terminą.

([253]) Specializuotas pirmosios instancijos teismas turi kompetenciją nagrinėti skundus dėl vyriausybės reguliavimo įstaigų priimtų sprendimų. Jeigu sprendimą priėmė informacijos komisaras, kompetentinga kolegija yra „Bendroji reguliavimo kolegija“, kuri turi jurisdikciją visoje Jungtinėje Karalystėje.

([254]) 2018 m. DAA 166 straipsnis. Sėkmingų ieškinių informacijos komisarui specializuotame teisme pavyzdžiai: byla, kurioje informacijos komisaras pripažino gavęs duomenų subjekto skundą, tačiau nenurodė, kokių veiksmų jis ketino imtis, todėl buvo įpareigotas per 21 kalendorinę dieną patvirtinti, ar jis ketino tirti skundus ir, jei taip, ne rečiau kaip kas 21 dieną po to informuoti skundo pateikėją apie padarytą pažangą (sprendimas dar nepaskelbtas), ir byla, kurioje pirmosios instancijos specializuotas teismas konstatavo, kad nebuvo aišku, ar informacijos komisaro atsakymas skundo pateikėjui buvo tinkamas skundo „rezultatas“ (žr. Sprendimą *Susan Milne prieš The Information Commissioner* [2020], sprendimą galima rasti šiuo adresu: https://informationrights.decisions.tribunals.gov.uk/DBFiles/Decision/i2730/Milne,%20S%20-%20QJ2020-0296-GDPR-V,%20051220%20Section%20166%20DPA%20-DECISION.pdf).

([255]) 2018 m. DAA 162 ir 163 straipsniai.

([256]) Žr., pvz., Sprendimą *Brown prieš Commissioner of Police of the Metropolis & Anor* [2019] EWCA Civ 1724, kuriame pagal 1998 m. DAA ir 1998 m. Žmogaus teisių aktą buvo priteista 9 000 GBP už neteisėtą asmeninės informacijos gavimą ir netinkamą panaudojimą, ir Sprendimą *R (on the application of Bridges) prieš Chief Constable of South Wales* [2020] EWCA Civ 1058, kuriame apeliacinis teismas paskelbė, kad Velso policija neteisėtai naudojo veido atpažinimo sistemą, nes taip buvo pažeistas EŽTK 8 straipsnis, o duomenų valdytojo pateiktas poveikio duomenų apsaugai vertinimas neatitiko 2018 m. DAA.

([257]) Europos žmogaus teisių konvencijos 34 straipsnyje nustatyta, kad „Kiekvienas fizinis asmuo, nevyriausybinės organizacijos ar grupės asmenų, teigiantys, kad jie yra vienos iš Aukštųjų Susitariančių Šalių padaryto Konvencijoje ir jos protokoluose įtvirtintų teisių pažeidimo auka, gali pateikti Teismui individualią peticiją. Aukštosios Susitariančios Šalys įsipareigoja niekaip netrukdyti veiksmingai pasinaudoti šia teise“. Aukštosios Susitariančios Šalys įsipareigoja niekaip netrukdyti veiksmingai pasinaudoti šia teise“.

### 3.3. **Jungtinės Karalystės valdžios institucijų galimybė susipažinti su duomenimis ir jų naudojimas nacionalinio saugumo tikslais**

(175) Pagal Jungtinės Karalystės teisinę tvarką žvalgybos tarnybos, turinčios įgaliojimus rinkti elektroninę informaciją, kurią turi duomenų valdytojai arba duomenų tvarkytojai, remdamosi nacionalinio saugumo pagrindais, situacijose, kurios atitinka tinkamumo scenarijų, yra Žvalgybos tarnyba ([258]) (MI5), Slaptoji žvalgybos tarnyba ([259]) (SIS) ir Vyriausybės ryšių būstinė ([260]) (GCHQ) ([261]).

#### 3.3.1. *Teisiniai pagrindai, apribojimai ir apsaugos priemonės*

(176) Jungtinėje Karalystėje žvalgybos tarnybų įgaliojimai yra išdėstyti 2016 m. TĮA ir 2000 m. RIPA, kuriuose, įskaitant 2018 m. DAA, nustatyta šių įgaliojimų materialinė ir individualioji taikymo sritis bei jiems taikomi apribojimai ir apsaugos priemonės. Šie įgaliojimai, taip pat jiems taikomi apribojimai ir apsaugos priemonės išsamiai įvertinti kituose skirsniuose.

##### 3.3.1.1. Tyrimo įgaliojimai, kuriais naudojamasi nacionalinio saugumo srityje

(177) 2016 m. TĮA nustatyta tyrimo įgaliojimų teisinė sistema, t. y. įgaliojimai perimti ryšio duomenis ir su jais susipažinti ir perimti įrangą. 2016 m. TĮA nustatytas bendras draudimas, o metodų, kuriais sudaromos sąlygos susipažinti su ryšių turiniu, gauti prieigą prie ryšio duomenų arba perimti įrangą be teisėto pagrindo, naudojimas laikomas nusikalstama veika ([262]). Taip yra todėl, kad šių tyrimo įgaliojimų naudojimas yra teisėtas tik kai vykdomas remiantis orderiu arba leidimu ([263]).

(178) 2016 m. TĮA nustatytos išsamios taisyklės, kuriomis reglamentuojama kiekvieno tyrimo įgaliojimų taikymo sritis ir taikymo tvarka, taip pat konkretūs jų apribojimai ir apsaugos priemonės. Priklausomai nuo tyrimo

([258]) MI5 yra pavaldi vidaus reikalų sekretoriui. MI5 funkcijos nustatytos 1989 m. Saugumo tarnybų akte: saugoti nacionalinį saugumą (įskaitant apsaugą nuo šnipinėjimo, terorizmo ir sabotažo, nuo užsienio valstybių agentų veiklos ir nuo veiksmų, kuriais siekiama sunaikinti arba sutrikdyti parlamentinę demokratiją politinėmis, pramoninėmis ar smurtinėmis priemonėmis), apsaugoti Jungtinės Karalystės ekonominę gerovę nuo išorės grėsmių ir remti policijos pajėgų ir kitų teisėsaugos agentūrų veiklą vykdant sunkių nusikaltimų prevenciją ir nustatymą.

([259]) SIS yra pavaldi užsienio reikalų sekretoriui ir jo funkcijos išdėstytos 1994 m. Žvalgybos tarnybų akte. Jos funkcijos – gauti ir teikti informaciją, susijusią su asmenų, nesančių Didžiosios Britanijos salose, veiksmais ir ketinimais, ir vykdyti kitas užduotis, susijusias su tokių asmenų veiksmais arba ketinimais. Šias funkcijas galima vykdyti tik nacionalinio saugumo, Jungtinės Karalystės ekonominės gerovės labui arba remiant sunkių nusikaltimų prevenciją arba nustatymą.

([260]) GCHQ pavaldi užsienio reikalų sekretoriui ir jo funkcijos išdėstytos 1994 m. Žvalgybos tarnybų akte. Tai yra: a) stebėti, naudoti arba perimti elektromagnetinę ir kitokią spinduliuotę ir įrangą, gaminančią tokią spinduliuotę, gauti ir teikti informaciją, gautą iš tokios spinduliuotės arba įrangos arba su ja susijusią, ir iš užšifruotos medžiagos; b) teikti konsultacijas ir paramą vyriausybei arba, kai tinkama, kitoms organizacijoms ar asmenims apie kalbas, įskaitant techniniais klausimais naudojamą terminiją ir kriptografiją, ir kitais klausimais, susijusiais su ginkluotosioms pajėgoms teikiamos informacijos apsauga. Šias funkcijas galima vykdyti tik nacionalinio saugumo, Jungtinės Karalystės ekonominės gerovės labui, atsižvelgiant į asmenų, nesančių Didžiosios Britanijos salose, veiksmus arba ketinimus, arba remiant sunkių nusikaltimų prevenciją arba nustatymą.

([261]) Kitos valdžios įstaigos, vykdančios su nacionaliniu saugumu susijusias funkcijas, yra Gynybos žvalgyba (DI), Nacionalinio saugumo taryba ir sekretoriatas, Bendra žvalgybos organizaciją ir Bendras žvalgybos komitetas. Tačiau nei JIC, nei JIO negali pasinaudoti tyrimo įgaliojimais pagal 2016 m. TĮA, o DI galimybės pasinaudoti savo įgaliojimais yra ribotos.

([262]) Draudimas taikomas viešiems ir privatiems ryšio tinklams, taip pat valstybinei pašto tarnybai, kai perėmimas atliekamas Jungtinėje Karalystėje. Draudimas netaikomas privataus tinklo duomenų valdytojui, jeigu duomenų valdytojas davė aiškų arba numanomą sutikimą imtis perėmimo veiksmų (2016 m. TĮA 3 straipsnis).

([263]) Konkrečiais ribotais atvejais perėmimas įmanomas be orderio, t. y. kai perimama su siuntėjo arba gavėjo sutikimu (2016 m. TĮ 44 straipsnis), ribotais administraciniais arba vykdymo užtikrinimo tikslais (TĮA 45–48 straipsniai), tam tikrose specialiose institucijose (2016 m. TĮA 49–51 straipsniai) ir atsižvelgiant į prašymus iš užsienio (2016 m. TĮA 52 straipsnis).

įgaliojimų (ryšių perėmimas, ryšio duomenų įgijimas ir saugojimas ir įrangos perėmimas) ([264]), taip pat nuo to, ar įgaliojimais naudojamasi dėl konkretaus taikinio, ar masiškai, taikomos skirtingos taisyklės. Išsami informacija apie kiekvienos 2016 m. TĮA numatytos priemonės taikymo sritį, apsaugos priemones ir apribojimus pateikta specialiuose skyriuose toliau.

(179) Be to, 2016 m. TĮA papildo įvairūs teisės aktuose nustatyti praktikos kodeksai, kuriuos paskelbė valstybės sekretorius ir patvirtino abeji parlamento rūmai ([265]) ir kurie taikomi visoje šalyje. Šiuose praktikos kodeksuose pateikiamos naudojimosi šiais įgaliojimais gairės ([266]). Nors duomenų subjektai, norėdami pasinaudoti savo teisėmis, gali tiesiogiai remtis 2016 m. TĮA nuostatomis, 2016 m. TĮA 7 priedo 5 dalyje nurodyta, kad Praktikos kodeksai laikomi priimtinais įrodymais civilinėse ir baudžiamosiose bylose, o bendrosios kompetencijos teismas, specializuotas teismas arba priežiūros institucija, teisminio proceso metu spręsdami atitinkamą klausimą, gali atsižvelgti į tai, kad kodeksų nebuvo laikomasi ([267]). Vertindama ankstesnio Jungtinės Karalystės teisės aktą stebėjimo srityje – 2000 m. Tyrimo įgaliojimų reguliavimo akto – teisinę kokybę, Europos Žmogaus Teisių Teismo didžioji kolegija aiškiai pripažino Jungtinės Karalystės praktikos kodeksų svarbą ir konstatavo, kad vertinant teisės aktų, kuriais leidžiama stebėti, numatomumą galima atsižvelgti į jų nuostatas ([268]).

(180) Reikia pažymėti, kad tiksliniai įgaliojimai (tikslinis perėmimas ([269]), ryšių duomenų gavimas ([270]), ryšių duomenų saugojimas ([271]) ir tikslinis įrangos perėmimas ([272])) gali būti suteikti nacionalinio saugumo tarnyboms ir tam tikroms teisėsaugos institucijoms ([273]), tačiau su masiniais duomenimis susiję įgaliojimai (t. y. masinis perėmimas ([274]), masinis ryšio duomenų gavimas ([275]), masinis įrangos perėmimas ([276]) ir masinių asmens duomenų rinkiniai ([277])) suteikiami išskirtinai žvalgybos tarnyboms.

(181) Nuspręsdama, kuriais tyrimo įgaliojimais pasinaudoti, žvalgybos agentūra privalo laikytis 2016 m. TĮA 2 straipsnio 2 dalies a punkte išvardytų „bendrųjų su privatumu susijusių pareigų“, tarp kurių yra būtinumo ir proporcingumo patikrinimas. Konkrečiau, pagal šią nuostatą valdžios institucija, ketinanti pasinaudoti tyrimo įgaliojimais, privalo įvertinti, i) ar tai, ko siekiama orderiu, leidimu arba pranešimu, galima pasiekti kitomis, mažiau

([264]) Pavyzdžiui, kalbant apie tokių priemonių taikymo sritį, pagal 3 ir 4 dalis (ryšių duomenų saugojimas ir gavimas) priemonės taikymo sritis yra griežtai susieta su telekomunikacijų operatorių, kurių naudotojų duomenims taikoma priemonė, apibrėžtimi. Kitas pavyzdys gali būti susijęs su „masinių“ įgaliojimų naudojimu. Šiuo atveju šie įgaliojimai apima tik „ryšių duomenis, kuriuos asmenys siunčia arba gauna už Didžiosios Britanijos salų ribų“.

([265]) 2016 m. TĮA 7 priede nustatyta kodeksų taikymo sritis, procedūra, kuria reikia vadovautis juos priimant, jų peržiūros taisyklės ir galiojimas. Praktikos kodeksus, priimtais pagal 2016 m. TĮA, galima rasti šiuo adresu:

([266]) Pagal 2016 m. TĮA priimti praktikos kodeksai skelbiami šiuo adresu: https://www.gov.uk/government/publications/investigatory-powers-act-2016-codes-of-practice.

([267]) Bendrosios kompetencijos ir specializuoti teismai naudoja praktikos kodeksus, kad įvertintų institucijų elgesio teisėtumą. Žr., pvz., Sprendimą *Dias prieš Cleveland Police*, [2017] UKIPTrib15_586-CH, kuriame specializuotas Tyrimo įgaliojimų teismas pateikė nuorodą į konkrečias praktikos kodekso dėl ryšio duomenų nuostatas, padedančias suprasti „nusikaltimo prevencijos ar nustatymo arba neramumų prevencijos“ pagrindo, naudojamo prašant gauti ryšio duomenis, apibrėžtį. Kodeksas motyvuojamojoje dalyje buvo nurodytas siekiant išsiaiškinti, ar tas pagrindas buvo panaudotas neteisingai. Teismas padarė išvadą, ginčijamas elgesys buvo neteisėtas. Teismai taip pat įvertino kodeksuose nustatytų apsaugos priemonių lygį, žr., pvz., Sprendimą *Just for Law Kids prieš Secretary of State for the Home Department* [2019] EWHC 1772 (Admin), kuriame Aukštasis teismas nusprendė, kad pirminiuose ir antriniuose teisės aktuose kartu su vidaus gairėmis nustatytos pakankamos apsaugos priemonės, arba Sprendimą *R (National Council for Civil Liberties) prieš Secretary of State for the Home Department & Others* [2019] EWHC 2057 (Admin), kuriame jis nustatė, kad 2016 m. TĮA ir praktikos kodekse dėl įrangos perėmimo buvo pakankamai nuostatų, susijusių su poreikiu orderiuose pateikti konkrečią sistemą.

([268]) Byloje *Big Brother Watch* Europos Žmogaus Teisių Teismo didžioji kolegija pažymėjo, kad „Informacijos komisaro kodeksas yra abiejų parlamento rūmų patvirtintas viešas dokumentas, kurį vyriausybė skelbia internete ir spausdintine versija ir į kurį turi atsižvelgti tiek perėmimo pareigas vykdantys asmenys, tiek teismai (žr. šio sprendimo 93–94 punktus). Taigi šis teismas pripažino, kad į jo nuostatas galima atsižvelgti vertinant Tyrimo įgaliojimų reguliavimo akto nuspėjamumą (žr. Pirmiau minėto sprendimo *Kennedy* 157 punktą). Taigi teismas pripažino, kad vidaus teisės akto nuspėjamumas yra tinkamas“ (žr. Europos Žmogaus Teisių Teismo (didžiosios kolegijos) sprendimą *Big Brother Watch ir kt. prieš Jungtinę Karalystę*, paraiškų Nr. 58170/13, 62322/14 ir 24960/15 (toliau – *Big Brother Watch ir kt.*), 2021 m. gegužės 25 d., 366 punktas).

([269]) 2016 m. TĮA 2 dalis.

([270]) 2016 m. TĮA 3 dalis.

([271]) 2016 m. TĮA 4 dalis.

([272]) 2016 m. TĮA 5 dalis.

([273]) Atitinkamų teisėsaugos institucijų, galinčių pasinaudoti tyrimo įgaliojimais pagal 2016 m. TĮA, sąrašas minimas (139) išnašoje.

([274]) 2016 m. TĮA 136 straipsnis.

([275]) 2016 m. TĮA 158 straipsnis.

([276]) 2016 m. TĮA 176 straipsnis.

([277]) 2016 m. TĮA 199 straipsnis.

intervencinėmis priemonėmis; ii) ar apsaugos lygis, kuris turi būti taikomas bet kokiam informacijos gavimui pagal orderį, leidimą arba pranešimą, yra didesnis būtent dėl tos informacijos slaptumo; iii) viešąjį interesą, atsižvelgdama į telekomunikacijų sistemų ir pašto tarnybų vientisumą ir saugumą ir iv) bet kuriuos kitus viešojo intereso, susijusio su privatumo apsauga, aspektus ([278]).

(182) Šių kriterijų taikymo būdas išsamiau apibūdintas atitinkamuose praktikos kodeksuose, o tai, kaip jų laikomasi, įvertina valstybės sekretorius ir nepriklausomi teismų komisarai, išduodami leidimą naudotis tokiais įgaliojimais. Visų pirma bet kurių iš šių tyrimo įgaliojimų naudojimas visada turi būti „proporcingas siekiamam tikslui, kurį nustatant derinamas privatumo (iki kitų 2 straipsnio 2 dalyje išvardytų aspektų) ribojimo mastas ir poreikis imtis veiksmų atsižvelgiant į tyrimo, operatyvinius ar pajėgumų aspektus“. Tai visų pirma reiškia, kad tokiu atveju „turėtų būti numatoma reali galimybė gauti tikėtiną naudą, kuri neturėtų būti neproporcinga arba savavališka“ ir „[j]oks privatumo apribojimas neturėtų būti laikomas proporcingu, jeigu informaciją, kurią norima gauti, galima gauti mažiau intervencinėmis priemonėmis“ ([279]). Konkrečiau, proporcingumo principo laikymasis turi būti vertinamas atsižvelgiant į šiuos kriterijus: „i) siūlomo privatumo ribojimo mastas, palyginti su siekiamu tikslu; ii) kaip ir kodėl patvirtintini metodai padės užtikrinti kuo mažesnį kišimąsi į asmens ir kitų reikalus; iii) ar vykdant veiklą tinkamai naudojamasi ir protingai naudojamasi aktu, atsižvelgiant į visas pagrįstas alternatyvas, susijusias su siektinu tikslu; iv) kokie kiti metodai, kai tinkama, buvo neįgyvendinti arba buvo naudojami, tačiau yra vertinami kaip nepakankami, siekiant įgyvendinti operatyvinius uždavinius nenaudojant siūlomų tyrimo įgaliojimų“ ([280]).

(183) Kaip paaiškino Jungtinės Karalystės institucijos, taip praktiškai užtikrinama, kad žvalgybos tarnyba, pirma, nustatytų operatyvinį tikslą (taip nustatydama duomenų rinkimo ribas, pvz., tarptautinės kovos su terorizmu tikslo siekiama konkrečioje geografinėje teritorijoje), ir, antra, remdamasi operatyviniu tikslu, žvalgybos agentūra turės įvertinti, kuri techninė galimybė (pvz., tikslinis arba masinis perėmimas, įrangos perėmimas, ryšio duomenų gavimas) yra tinkamiausia (t. y. mažiausiai pažeidžianti privatumą, plg. TĮA 2 straipsnio 2 dalį), atsižvelgiant į siekiamą tikslą, todėl jis yra leistinas, remiantis vienu iš teisės aktuose nustatytų pagrindų.

(184) Verta pažymėti, kad į šį rėmimąsi būtinumo ir proporcingumo standartais dėmesį taip pat atkreipė ir jį teigiamai įvertino Jungtinių Tautų specialusis pranešėjas teisės į privatumą klausimais Josephas Cannataci, kuris dėl 2016 m. TĮA nustatytos sistemos nurodė, kad „atrodo, jog pagal žvalgybos tarnybose ir teisėsaugos institucijose galiojančias procedūras sistemiškai reikalaujama atsižvelgti į stebėjimo priemonės arba operacijos būtinumą ir proporcingumą ir tik tuomet teikti rekomendaciją dėl leidimo, taip pat ją peržiūrėti tais pačiais pagrindais“ ([281]). Jis taip pat pažymėjo, kad, susitikęs su teisėsaugos ir nacionalinių saugumo agentūrų atstovais, „[jis] sulaukė pritarimo dėl to, kad teisė į privatumą yra svarbiausia aplinkybė, į kurią reikia atsižvelgti priimant bet kokį sprendimą dėl stebėjimo priemonių. Visi suprato ir pripažino, kad būtinumas ir proporcingumas yra pagrindiniai principai, į kuriuos reikia atsižvelgti“.

([278]) Ryšių perėmimo kodekse nustatyta, kad kiti proporcingumo patikrinimo elementai yra: „i) siūlomo privatumo ribojimo mastas, palyginti su siekiamu tikslu; ii) kaip ir kodėl patvirtintini metodai padės užtikrinti kuo mažesnį kišimąsi į asmens ir kitų reikalus; iii) ar vykdant veiklą tinkamai naudojamasi ir protingai naudojamasi aktu, atsižvelgiant į visas pagrįstas alternatyvas, susijusias su siektinu tikslu; iv) kokie kiti metodai, kai tinkama, buvo neįgyvendinti arba buvo naudojami, tačiau yra vertinami kaip nepakankami, siekiant įgyvendinti operatyvinius uždavinius nenaudojant siūlomų tyrimo įgaliojimų“. Ryšių perėmimo praktikos kodekso 4.16 punktas, galima rasti šiuo adresu: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf .

([279]) Žr. Ryšių perėmimo praktikos kodekso 4.12 ir 4.15 straipsnius, galima rasti šiuo adresu: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf .

([280]) Žr. Ryšių perėmimo praktikos kodekso 4.16 dalį.

([281]) Specialiojo pranešėjo teisės į privatumą klausimais misijos pabaigos pareiškimas, padarytas įvykdžius misiją Jungtinėje Didžiosios Britanijos ir Šiaurės Airijos Karalystėje, galima rasti šiuo adresu: https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23296&LangID=E, para 1.a.

(185) Konkretūs įvairių orderių priėmimo kriterijai, taip pat 2016 m. TĮA nustatyti apribojimai ir apsaugos priemonės dėl kiekvieno tyrimo įgaliojimo išsamiai aprašyti (186)–(243) konstatuojamosiose dalyse.

3.3.1.1.1. Tikslinis perėmimas ir tyrimas

(186) Tikslinio perėmimo orderiai būna trijų rūšių: tikslinio perėmimo orderis ([282]), tikslinio tyrimo orderis ir savitarpio pagalbos orderis ([283]). Šių orderių gavimo sąlygos ir atitinkamos apsaugos priemonės išdėstytos 2016 m. TĮA 1 skyriaus 2 dalyje.

(187) Pagal tikslinio perėmimo orderį leidžiama perimti orderyje aprašytus ryšius juos perduodant ir gaunant kitus duomenis, susijusius su tais ryšiais ([284]), įskaitant antrinius duomenis ([285]). Pagal tikslinio tyrimo orderį asmeniui leidžiama atrinkti tirti perimtą turinį, kuris buvo gautas remiantis masinio perėmimo orderiu ([286]).

(188) Valstybės sekretorius gali priimti bet kurį orderį pagal 2016 m. TĮA 2 dalį ([287]), kurį patvirtina teismo komisaras ([288]). Visais atvejais bet kurios rūšies tikslinio orderio galiojimo trukmė yra šeši mėnesiai ([289]) ir orderio pakeitimui ([290]) ir galiojimo pratęsimui ([291]) taikomos konkrečios taisyklės.

(189) Prieš išduodamas orderį, valstybės sekretorius privalo atlikti būtinumo ir proporcingumo vertinimą ([292]). Konkrečiau, tikslinio perėmimo orderio ir tikslinio tyrimo orderio atveju valstybės sekretorius turėtų patikrinti, ar priemonė yra būtina atsižvelgiant į vieną iš šių pagrindų: nacionalinio saugumo interesą; nusikaltimų prevencija arba išaiškinimą arba Jungtinės Karalystės ekonominės gerovės interesus ([293]) tiek, kiek jie taip pat yra svarbūs nacionalinio saugumo interesams ([294]). Kita vertus, savitarpio pagalbos orderis (žr. (139) above konstatuojamąją dalį) gali būti išduodamas tik jeigu valstybės sekretorius mano, kad esama aplinkybių, kurios yra lygiavertės aplinkybėms, kuriomis jis būtų išdavęs orderį, siekdamas užkirsti kelią sunkiam nusikaltimui arba jį nustatyti ([295]).

(190) Be to, valstybės sekretorius turėtų įvertinti, ar priemonė proporcinga atsižvelgiant į tai, ko ja siekiama ([296]). Vertinant prašomų priemonių proporcingumą, būtina atsižvelgti į bendrąsias privatumo pareigas, nustatytas 2016 m. TĮA 2 straipsnio 2 dalyje, visų pirma į poreikį įvertinti, ar tai, ko siekiama orderiu, leidimu arba pranešimu, būtų galima

([282]) 2016 m. TĮA 15 straipsnio 2 dalis.
([283]) 2016 m. TĮA 15 straipsnio 4 dalis.
([284]) 2016 m. TĮA 15 straipsnio 2 dalis.
([285]) Antriniai duomenys – perimtiems ryšiams priskirti arba su jais logiškai susieti duomenys; duomenys, kuriuos galima logiškai atskirti nuo perimtų ryšių, ir, jeigu jie taip buvo atskirti, jais neatskleidžiama jokia informacija, kuri pagrįstai gali būti laikoma ryšių prasme (jeigu ji yra). Kai kurie antrinių duomenų pavyzdžiai: maršruto parinktuvo konfigūracija arba ugniasienės, arba laikotarpis, kurį veikė maršruto parinktuvas, kuris yra tinklo dalis, prie jo prijungtas arba logiškai susietas su perimtais ryšiais. Daugiau informacijos galima rasti 2016 m. TĮA 16 straipsnyje ir Ryšių perėmimo praktikos kodekso 2.19 straipsnyje, žr. 278išnašą.
([286]) Šis nagrinėjimas atliekamas kaip 2016 m. TĮA 152 straipsnio 4 dalies išimtis, kurioje numatytas draudimas siekti nustatyti asmenų, esančių Didžiosios Britanijos salose, ryšių tapatybę. Žr. (229)konstatuojamąją dalį.
([287]) Škotijos ministras leidžia išduoti orderį tais atvejais, kai jis susijęs su sunkia nusikalstama veika Škotijoje (žr. 2016 m. TĮA 21 ir 22 skirsnius), o valstybės sekretorius gali paskirti vyresnįjį pareigūną, kuris išduoda savitarpio pagalbos orderį, kai manoma, kad perėmimas bus susijęs su asmeniu arba patalpomis, esančiais už Jungtinės Karalystės ribų (2016 m. TĮA 40 straipsnis).
([288]) 2016 m. TĮA 19 ir 23 straipsniai.
([289]) 2016 m. TĮA 32 straipsnis.
([290]) 2016 m. TĮA 39 straipsnis. Nurodyti asmenys gali atlikti ribotus orderių pakeitimus pagal 2016 m. TĮA nustatytas sąlygas. Orderį išdavęs asmuo jį gali anuliuoti bet kuriuo metu. Jis privalo tai padaryti, jeigu orderis tampa nebereikalingas remiantis bet kuriais atitinkamais pagrindais arba veika, dėl kurios išduotas orderis, nebėra proporcinga siekiamam tikslui.
([291]) 2016 m. TĮA 33 straipsnis. Sprendimą atnaujinti orderį privalo patvirtinti teismo komisaras.
([292]) 2016 m. TĮA 19 straipsnis.
([293]) Dėl sąvokos „ekonominės gerovės interesai“, kai šie interesai taip pat svarbūs nacionaliniam saugumui, Europos Žmogaus Teisių Teismo didžioji kolegija sprendimo *Big Brother Watch ir kt. prieš Jungtinę Karalystę* (žr. 268 išnašą) 371 punkte nustatė, kad tokia sąvoka yra pakankamai aiškiai pagrįsta nacionalinio saugumo sumetimais. Nors teismo išvada šiuo atveju buvo susijusi su sąvokos vartojimu 2000 m. Tyrimo įgaliojimų reguliavimo akte, ta pati sąvoka vartojama ir 2016 m. TĮA.
([294]) 2016 m. TĮA 20 straipsnio 2 dalis.
([295]) 2016 m. TĮA 20 straipsnio 3 dalis.
([296]) 2016 m. TĮA 19 straipsnio 1 dalies b punktas, 19 straipsnio 2 dalies b punktas ir 19 straipsnio 3 dalies b punktas.

pagrįstai pasiekti kitomis, mažiau intervencinėmis priemonėmis, ir ar apsaugos lygis, taikomas bet kuriuo būdu gaunant informaciją pagal orderį, yra didesnis dėl konkretaus tos informacijos slaptumo (žr. (181) konstatuojamąją dalį).

(191) Šiuo tikslu valstybės sekretorius turės atsižvelgti į visus prašančiosios institucijos pateikto prašymo aspektus, visų pirma susijusius su asmenimis, kurių duomenys perimami, ir priemonės reikšme tyrimui. Tokie aspektai išvardyti Ryšių perėmimo praktikos kodekse ir jų aprašymas turi atitikti tam tikrą konkretumo lygį ([297]). Be to, 2016 m. TĮA 17 straipsnyje reikalaujama, kad bet kokiame pagal 2 skyrių išduotame orderyje turi būti nurodytas arba apibūdintas konkretus asmuo arba asmenų grupė, organizacija arba perimtinos patalpos („taikinys“). Tikslinio perėmimo orderis arba tikslinio tyrimo orderis taip pat gali būti susiję su asmenų grupėmis, daugiau nei vienu asmeniu arba organizacija, arba daugiau nei viena patalpa (taip pat vadinami teminiais orderiais) ([298]). Šiais atvejais orderyje taip pat turėtų būti aprašytas bendras tikslas arba veikla, kurią bendrai vykdo asmenų grupė arba operacija / tyrimai ir įvardijama arba apibūdinama kuo daugiau tų asmenų / organizacijų arba patalpų, kai tai praktiškai įmanoma ([299]). Galiausiai visuose pagal 2016 m. TĮA 2 dalį išduotuose orderiuose turi būti nurodyti adresai, numeriai, aparatūra, veiksniai arba veiksnių derinys, kurie turi būti naudojami nustatant ryšius ([300]). Šiuo atžvilgiu Ryšių perėmimo praktikos kodekse nustatyta, kad tikslinio perėmimo orderio ir tikslinio tyrimo orderio atveju „orderyje turi būti nurodyti (arba aprašyti) veiksniai arba veiksnių deriniai, kurie turi būti naudojami nustatant ryšių tapatybę. Jeigu ryšiai turi būti nustatomi pateikiant telefono numerį, jame, pvz., turi būti nurodomi visi skaičiai. Tačiau tais atvejais, kai ryšio tapatybei identifikuoti turi būti naudojami labai sudėtingi arba nuolat kintantys internetiniai selektoriai, tie selektoriai turėtų būti kuo išsamiau aprašyti“ ([301]).

(192) Šiomis aplinkybėmis svarbi apsaugos priemonė yra ta, kad valstybės sekretoriaus atliekamą vertinimą siekiant išduoti orderį turi patvirtinti nepriklausomas teismo komisaras ([302]), kuris visų pirma patikrins, ar sprendimas išduoti orderį atitinka būtinumo ir proporcingumo principus ([303]) (dėl teismo komisarų statuso ir vaidmens žr. (251)–(256) below konstatuojamąsias dalis). 2016 m. TĮA taip pat paaiškinta, kad, atlikdamas tokį patikrinimą, teismo komisaras privalo taikyti tuos pačius principus, kuriuos teismas taikytų atlikdamas teisminę peržiūrą ([304]). Taip užtikrinama, kad kiekvienu atveju ir prieš susipažįstant su duomenimis nepriklausoma įstaiga sistemiškai patikrintų būtinumo ir proporcingumo principų laikymąsi.

(193) 2016 m. TĮA numatytos kelios konkrečios ir siauros išimtys, kai tikslinį informacijos perėmimą galima vykdyti be orderio. Šie išimtiniai atvejai išsamiai aprašyti teisės aktuose ([305]) ir, išskyrus atvejus, kai gautas siuntėjo (gavėjo) sutikimas, juos atlieka asmenys (privačios arba viešosios įstaigos), kurie nėra nacionalinės saugumo agentūros. Be to, tokio tipo informacijos perėmimas vykdomas kitais, ne žvalgybos, tikslais ([306]) ir kai kuriais iš jų atveju labai mažai tikėtina, kad duomenys gali būti renkami pagal perdavimo scenarijų (pavyzdžiui, perėmimo psichiatrijos

([297]) Prašoma informacija apima duomenis apie aplinkybes (asmenų / organizacijų / patalpų, perimtinų ryšių) ir kaip šios informacijos gavimas prisidės prie tyrimo, taip pat leistinų veiksmų aprašymas. Jeigu asmenų / organizacijų / patalpų neįmanoma apibūdinti, būtina pateikti paaiškinimą, kodėl to padaryti neįmanoma, arba kodėl buvo pateiktas tik bendras apibūdinimas (Ryšių perėmimo praktikos kodekso 5.32 ir 5.34 dalys, žr. 278 išnašą).

([298]) 2016 m. TĮA 17 straipsnio 2 dalis. Taip pat žr. Ryšių perėmimo praktikos kodekso 5.11 ir kt. straipsnius, žr. 278 išnašą.

([299]) 2016 m. TĮA 31 straipsnio 4 ir 5 dalys.

([300]) 2016 m. TĮA 31 straipsnio 8 dalis.

([301]) Ryšių perėmimo praktikos kodekso 5.37 ir 5.38 straipsniai, žr. 278 išnašą.

([302]) Teismo komisaro patvirtinimas nereikalingas, jeigu valstybės sekretorius mano, kad būtina skubiai išduoti orderį (žr. TĮA 19 straipsnio 1 dalį). Tačiau teismo komisarą būtina informuoti per trumpą terminą ir jis privalo nuspręsti, ar patvirtinti orderį. Jei jis to nepadaro, orderis nustoja galioti (2016 m. TĮA 24 ir 25 straipsniai).

([303]) 2016 m. TĮA 23 straipsnio 1 dalis.

([304]) 2016 m. TĮA 23 straipsnio 2 dalis.

([305]) Žr. 2016 m. TĮA 44–51 straipsnius ir Komunikato dėl informacijos perėmimo praktikos kodekso 12 skirsnį (žr. 278 išnašą).

([306]) Taip yra, pavyzdžiui, kai reikia perimti informaciją kalėjime arba psichiatrinėje ligoninėje (siekiant patikrinti sulaikyto asmens ar paciento elgesį) arba pašto ar telekomunikacijų operatoriaus, pavyzdžiui, siekiant nustatyti neteisėtą turinį.

ligoninėje arba kalėjime atveju). Atsižvelgiant į įstaigos, kuri taiko šias konkrečias išimtis (jei ji nėra nacionalinė saugumo agentūra), pobūdį, taikomos visos 2018 m. DAA 2 dalyje ir Jungtinės Karalystės BDAR numatytos apsaugos priemonės, įskaitant Informacijos komisaro vykdomą priežiūrą ir visus esamus teisių gynimo mechanizmus. Be to, tam tikrais atvejais, be 2018 m. DAA numatytų apsaugos priemonių, 2016 m. TĮA taip pat numatyta Tyrimų įgaliojimų komisaro biuro *ex post* priežiūra ([307]).

(194) Kai vykdomas informacijos perėmimas, taikomi papildomi apribojimai ir apsaugos priemonės, atsižvelgiant į konkretų asmens (-ų), kurio (-ių) atžvilgiu vykdomas perėmimas, statusą ([308]). Teisę perimti daiktus, kuriems taikoma teisinė paslaptis, leidžiama tik esant išimtinėms ir įtikinamoms aplinkybėms: orderį išduodantis asmuo turi atsižvelgti į viešąjį interesą, susijusį su objektų, kuriems taikoma teisinė paslaptis, konfidencialumu ir į tai, kad yra nustatyti konkretūs tokios medžiagos tvarkymo, saugojimo ir atskleidimo reikalavimai ([309]).

(195) Be to, 2016 m. TĮA numatytos konkrečios apsaugos priemonės, susijusios su saugumu, saugojimu ir informacijos atskleidimu, į kurias valstybės sekretorius turėtų atsižvelgti prieš išduodamas tikslinį orderį ([310]). Visų pirma 2016 m. TĮA 53 straipsnio 5 dalyje reikalaujama, kad kiekviena bet kurios tos medžiagos, surinktos remiantis orderiu, kopija būtų saugoma saugiai ir sunaikinama kuo greičiau, kai nebelieka jos saugojimą pateisinančių pagrindų, o 2016 m. TĮA 53 straipsnio 2 dalyje reikalaujama, kad asmenų, kuriems atskleidžiama medžiaga, skaičius ir mastas, kuriuo atskleidžiama bet kokia medžiaga, būtų prieinama arba kopijuojama tik tiek, kiek tai yra būtina teisės aktuose nustatytais tikslais.

(196) Galiausiai tais atvejais, kai medžiaga, perimta remiantis tikslinio perėmimo orderiu arba savitarpio pagalbos orderiu, turi būti perduota trečiajai valstybei („informacijos atskleidimas užsienyje“), 2016 m. TĮA nustatyta, kad valstybės sekretorius privalo užtikrinti, kad būtų nustatytos tinkamos priemonės, siekiant užtikrinti, kad toje trečiojoje šalyje būtų panašios informacijos saugumo, saugojimo ir atskleidimo priemonės ([311]). Be to, 2018 m. DAA 109 straipsnio 2 dalyje nustatyta, kad asmens duomenis žvalgybos tarnybos gali perduoti už Jungtinės Karalystės teritorijos ribų tik tuomet, kai tai būtina arba proporcinga duomenų valdytojui siekiant įvykdyti teisės akte nustatytas funkcijas arba kitais 1989 m. Saugumo tarnybų akto 2 straipsnio 2 dalies a punkte arba 1994 m. Žvalgybos tarnybų akto 2 straipsnio 2 dalies a punkte ir 4 straipsnio 2 dalies a punkte nustatytais tikslais ([312]). Svarbu pažymėti, kad šie reikalavimai galioja ir tais atvejais, kai taikoma nacionalinio saugumo išimtis pagal 2018 m. DAA 110 straipsnį, nes 2018 m. DAI 110 straipsnyje šio akto 109 straipsnis nenurodytas kaip viena iš nuostatų, kurios gali būti netaikomos, jei nacionalinio saugumo užtikrinimo tikslais reikia išimties tvarka netaikyti tam tikrų nuostatų.

3.3.1.1.2. Tikslinis ryšio duomenų gavimas ir saugojimas

(197) Pagal 2016 m. TĮA valstybės sekretoriui leidžiama reikalauti, kad telekomunikacijų operatoriai saugotų ryšio duomenis, kad su jais tikslingai galėtų susipažinti įvairios valdžios institucijos, įskaitant teisėsaugos ir žvalgybos agentūras. 2016 m. TĮA 4 dalyje numatyta ryšio duomenų saugojimo tvarka, o 3 dalyje numatyta galimybė tikslingai perimti ryšio duomenis. 2016 m. TĮA 3 ir 4 dalyse taip pat nustatyti konkretūs šių įgaliojimų naudojimo apribojimai ir numatytos konkrečios apsaugos priemonės.

([307]) Žr. *a contrario* TĮA 229 straipsnio 4 dalį.

([308]) 2016 m. TĮA 26–29 straipsniuose nustatyti apribojimai, taikomi tikslinio perėmimo ir tikslinio tyrimo orderiams, susijusiems su ryšių, kuriuos siuntė parlamento narys arba kurie buvo išsiųsti parlamento nariui, perėmimu (tai pasakytina apie bet kuriuos Jungtinės Karalystės parlamento rūmus), daiktų, kuriems taikoma teisinė privilegija, perėmimui, ryšių perėmimui, kai perimančioji institucija mano, kad ryšiuose bus konfidencialios žurnalistinės medžiagos, ir kai orderio tikslas yra nustatyti arba patvirtinti žurnalistinės informacijos šaltinį.

([309]) 2016 m. TĮA 26 straipsnis.

([310]) 2016 m. TĮA 19 straipsnio 1 dalis.

([311]) 2016 m. TĮA 54 straipsnis. Su medžiagos atskleidimu užsienio institucijoms susijusios apsaugos priemonės išsamiau apibrėžtos praktikos kodeksuose: žr., be kita ko, Ryšių perėmimo praktikos kodekso 9.26 ir paskesnius punktus bei 9.87 punktą ir Įrangos perėmimo praktikos kodekso 9.33 ir paskesnius bei 9.41 punktą (žr. 278 išnašą).

([312]) Tai yra šie tikslai: saugumo tarnybos atveju – sunkių nusikaltimų prevencija arba nustatymas arba bet kokia baudžiamoji byla (1989 m. Saugumo tarnybų akto 2 straipsnio 2 dalies a punktas), žvalgybos tarnybos atveju – nacionalinio saugumo interesai, sunkaus nusikaltimo prevencija arba nustatymas, arba bet kuri baudžiamoji byla (1994 m. Žvalgybos tarnybų akto 2 straipsnio 2 dalies a punktas) ir GCHQ atveju – bet kuri baudžiamoji byla (1994 m. Žvalgybos tarnybų akto 4 straipsnio 2 dalies a punktas). Taip pat žr. 2018 m. DAA aiškinamąsias pastabas, kurias galima rasti adresu https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.

(198) Sąvoka „ryšio duomenys“ reiškia „kas“, „kada“, „kur“ ir „kaip“ siuntė ryšius, o ne turinį, t. y. kas buvo pasakyta arba užrašyta. Kitaip nei perėmimo atveju, gaunant ir saugant ryšio duomenis siekiama ne gauti ryšio turinį, bet informaciją, tokią kaip telefono paslaugų abonentas arba išsami sąskaita. Tai galėtų būti ryšio laikas ir trukmė, siuntėjo ir gavėjo numeris arba e. pašto adresas ir kartais prietaisų, kuriuos naudojant buvo siunčiamas telekomunikacinis ryšys, buvimo vieta ([313]).

(199) Reikėtų pažymėti, kad ryšių duomenų saugojimas ir rinkimas paprastai nėra susijęs su ES duomenų subjektų asmens duomenimis, pagal šį sprendimą perduotais į Jungtinę Karalystę. Pareiga saugoti arba atskleisti ryšio duomenis pagal 2016 m. TĮA 3 ir 4 dalis taikoma duomenims, kuriuos Jungtinės Karalystės telekomunikacijų operatoriai tiesiogiai surinko iš telekomunikacijų paslaugų naudotojų ([314]). Šios rūšies bendravimas su klientais tvarkant jų duomenis paprastai nėra susijęs su perdavimu, remiantis šiuo sprendimu, t. y. perdavimas iš ES duomenų valdytojo / tvarkytojo, Jungtinės Karalystės duomenų valdytojui / tvarkytojui.

(200) Tačiau siekiant išsamumo, sąlygos ir apsaugos priemonės, kuriomis reglamentuojama ši gavimo ir saugojimo tvarka, aptartos tolesnėse konstatuojamosiose dalyse.

(201) Reikia pažymėti, kad ryšių duomenų saugojimą ir tikslinį gavimą gali vykdyti tiek nacionalinės saugumo tarnybos, tiek tam tikros teisėsaugos institucijos ([315]). Sąlygos, kuriomis pagrindžiamas poreikis saugoti ir (arba) gauti ryšių duomenis, gali skirtis priklausomai nuo prašymo taikyti priemonę pagrindo, t. y. nacionalinio saugumo ar teisėsaugos tikslo.

(202) Visų pirma, nors pagal naująją tvarką nustatytas bendras reikalavimas gauti nepriklausomos įstaigos *ex ante* leidimą, kuris bus taikomas visais atvejais, kai ryšių duomenys saugomi ir (arba) gaunami (teisėsaugos arba nacionalinio saugumo tikslais), remiantis Europos Teisingumo Teismo sprendimu *Tele2/Watson* ([316]) buvo nustatytos specialios apsaugos priemonės, privalomos prašant taikyti šią priemonę teisėsaugos tikslais. Svarbu pažymėti, kad tais atvejais, kai ryšių duomenų saugojimo arba gavimo prašoma teisėsaugos tikslais, *ex ante* leidimą visada turi išduoti tyrimo įgaliojimų komisaras. Taip yra ne visada, jei priemonės prašoma nacionalinio saugumo tikslais, nes, kaip aprašyta toliau, tam tikrais atvejais tokios rūšies priemones gali leisti taikyti kitas „leidimą išduodantis asmuo“. Be to, pagal naująją tvarką pakelta riba, nuo kurios gali būti leidžiama saugoti ir gauti ryšių duomenis – tai „sunkūs nusikaltimai“ ([317]).

([313]) Ryšių duomenys apibrėžti 2016 m. TĮA 261 straipsnio 5 dalyje. Ryšių duomenys skirstomi į „įvykių duomenis“ (bet kurie duomenys, kuriais identifikuojamas arba apibūdinamas įvykis, nurodant jo vietą arba jos nenurodant, kuris įvyko telekomunikacijų sistemoje arba ją naudojant, ir įvykyje dalyvauja vienas arba daugiau subjektų, konkrečiu metu vykdančių konkrečią veiklą) ir „duomenys apie subjektą“ (bet kurie duomenys, kurie a) yra apie i) subjektą, ii) telekomunikacijų paslaugos ir subjekto ryšį arba iii) bet kurios telekomunikacijų sistemos dalies ir subjekto ryšį, b) kuriuos sudaro arba kurie apima duomenis, kuriais nustatoma subjekto tapatybė arba jis aprašomas (nesvarbu, ar nurodoma subjekto buvimo vieta), ir c) nėra duomenys apie įvykius).

([314]) Tokią išvadą galima daryti remiantis ryšio duomenų apibrėžtimi, pateikta 2016 m. TĮA 261 straipsnio 5 dalyje, pagal kurią ryšio duomenis saugo arba gauna telekomunikacijų operatorius ir šie duomenys yra apie telekomunikacijų paslaugos naudotoją ir susiję su šios paslaugos teikimu, arba tai yra ryšio turinio duomenys, duomenys, kurie yra ryšio sudedamoji dalis, prie ryšio pridėti arba su juo logiškai susieti duomenys (taip pat žr. Ryšio duomenų praktikos kodeksą, galima rasti šiuo adresu: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/757850/Communications_Data_Code_of_Practice.pdf, 2.22–2.33 dalys). Be to, pagal telekomunikacijų operatoriaus apibrėžtį, pateiktą 2016 m. TĮA 261 straipsnio 10 dalyje, reikalaujama, kad telekomunikacijų operatorius būtų asmuo, siūlantis arba teikiantis telekomunikacijų paslaugą asmenims Jungtinėje Karalystėje arba eksploatuojantis telekomunikacijų sistemą, kuri (visa arba jos dalis) kontroliuojama Jungtinėje Karalystėje. Iš šių apibrėžčių aiškiai matyti, kad 2016 m. TĮA pareigų negalima nustatyti telekomunikacijų operatoriams, kurių įranga nėra Jungtinėje Karalystėje arba nėra joje kontroliuojama ir kurie nesiūlo arba neteikia paslaugų asmenims Jungtinėje Karalystėje (taip pat žr. Ryšio duomenų praktikos kodekso 2.1 dalį). Jeigu ES abonentai (nesvarbu, ar jie yra ES, ar Jungtinėje Karalystėje) naudojasi paslaugomis Jungtinėje Karalystėje, bet kokius ryšius, susijusius su šios paslaugos teikimu, tiesiogiai rinktų Jungtinės Karalystės paslaugų teikėjas, užuot juos perdavus iš ES.

([315]) Atitinkamos institucijos išvardytos 2016 m. TĮA 4 priede ir tai gali būti policijos pajėgos, žvalgybos tarnybos, kai kurios ministerijos ir vyriausybės departamentai, Nacionalinė nusikalstamumo prevencijos agentūra, Jos Didenybės mokesčių ir muitų inspekcija, Konkurencijos ir rinkų institucija, informacijos komisaras, greitosios medicinos pagalbos, ugniagesių ir pagalbos tarnybos ir institucijos, kurios, pvz., veikia sveikatos ir maisto saugos srityje.

([316]) Sprendimas *Tele2/Watson*, sujungtos bylos C-203/15 ir C-698/15, ECLI:EU:C:2016:970).

([317]) Žr. 61.7 skirsnio b punktą dėl ryšių duomenų įgijimo ir 87.10A skirsnį dėl ryšių duomenų saugojimo.

i) *Leidimas gauti ryšio duomenis*

(203) Pagal 2016 m. TĮA 3 dalį atitinkamos valdžios institucijos turi įgaliojimus gauti ryšio duomenis iš telekomunikacijų operatoriaus arba bet kurio asmens, galinčio gauti ir atskleisti tokius duomenis. Pagal leidimą gali būti neleidžiama perimti ryšių turinio ([318]) ir jis nustoja galioti pasibaigus vieno mėnesio terminui ([319]), įskaitant galimybę pratęsti galiojimo terminą išduodant papildomą leidimą ([320]). Norint gauti ryšių duomenis, reikalingas Tyrimo įgaliojimų komisaro leidimas ([321]) (dėl Tyrimo įgaliojimų komisaro (IPC) statuso ir įgaliojimų žr. (250)–(251) konstatuojamąsias dalis). Taip taikoma visais atvejais, kai atitinkama teisėsaugos institucija paprašo gauti ryšių duomenis. Tačiau 2016 m. TĮA 61 straipsnyje nustatyta, kad tais atvejais, kai duomenys gaunami atsižvelgiant į nacionalinio saugumo arba Jungtinės Karalystės ekonominės gerovės interesus, ir jeigu jie yra svarbūs nacionaliniam saugumui arba kai prašymą pateikia žvalgybos agentūros narys pagal 61 straipsnio 7 dalies b punktą ([322]), leidimą gauti duomenis taip pat gali išduoti ([323]) Tyrimo įgaliojimų komisaras arba paskirtasis vyresnysis pareigūnas ([324]). Paskirtasis pareigūnas turi būti nepriklausomas nuo atitinkamo tyrimo ar operacijos ir turėti praktinių žinių apie žmogaus teisių principus ir teisės aktus, kuriais visų pirma reglamentuojamas būtinumas ir proporcingumas ([325]). Paskirtojo pareigūno priimto sprendimo atžvilgiu vykdoma Tyrimo įgaliojimų komisaro *ex post* priežiūra (daugiau informacijos apie Tyrimo įgaliojimų komisaro *ex post* priežiūros funkcijas pateikta (254) below konstatuojamojoje dalyje).

(204) Leidimas gauti ryšio duomenis yra grindžiamas priemonės būtinumo ir proporcingumo vertinimu. Konkrečiau kalbant, priemonės būtinumas vertinamas atsižvelgiant į teisės aktuose išvardytus pagrindus ([326]). Atsižvelgiant į šios priemonės tikslinį pobūdį, ji taip pat turi būti reikalinga konkrečiam tyrimui ar operacijai ([327]). Kiti reikalavimai dėl priemonių būtinumo vertinimo nustatyti Ryšių duomenų praktikos kodekse ([328]). Šiame kodekse visų pirma nustatyta, kad prašančiosios institucijos pateiktame prašyme turėtų būti nustatyti trys būtiniausi elementai, kuriais pagrindžiamas tokio prašymo būtinumas: i) tiriamas įvykis, pvz., nusikaltimas arba pažeidžiamo dingusio asmens buvimo vieta; ii) asmuo, kurio duomenis siekiama gauti, pvz., įtariamasis, liudytojas arba dingęs asmuo, ir informacija apie tai, kaip jie yra susiję su įvykiu; ir iii) ryšio duomenys, kuriuos siekiama gauti, pvz., telefono numeris arba IP adresas, ir informacija apie tai, kaip šie duomenys yra susiję su asmeniu ir įvykiu ([329]).

(205) Be to, ryšio duomenų gavimas turi būti proporcingas atsižvelgiant į tai, ko juo siekiama ([330]). Ryšio duomenų praktikos kodekse paaiškinama, kad leidimą išduodantis asmuo, atlikdamas tokį vertinimą, turėtų stengtis suderinti „asmens teisių ir laisvių ribojimą su konkrečia tyrimo arba operacijos, kurią viešojo intereso labui vykdo atitinkama valdžios institucija, nauda“ ir kad, atsižvelgiant į visas konkrečios bylos aplinkybes, „asmens teisių ribojimas vis tiek negali būti pateisinamas dėl per didelio neigiamo poveikio kito asmens arba asmenų grupės teisėms“. Be to, siekiant konkrečiai įvertinti priemonės proporcingumą, kodekse išvardijami įvairūs aspektai, kuriuos savo prašyme turėtų

([318]) 2016 m. TĮA 60A straipsnio 6 dalis.

([319]) Šis laikotarpis sutrumpinamas iki trijų dienų, kai leidimas išduodamas skubos tvarka (2016 m. TĮA 65 straipsnio 3A dalį).

([320]) Pagal 2016 m. TĮA 65 straipsnį atnaujinti leidimai galios vieną mėnesį, kuris pradedamas skaičiuoti nuo dabartinio leidimo galiojimo pabaigos. Leidimą išdavęs asmuo jo galiojimą gali atšaukti bet kuriuo metu, jei mano, kad reikalavimai nebevykdomi.

([321]) 2016 m. TĮA 60A straipsnio 1 dalis. Šią funkciją IPC vardu atlieka Ryšių duomenų leidimų biuras (žr. Ryšių duomenų praktikos kodekso 5.6 punktą).

([322]) Paraiška pagal 2016 m. TĮA 61 straipsnio 7 dalies b punktą teikiama dėl taikytino „su nusikaltimu susijusio tikslo“, t. y. pagal 2016 m. TĮA 61 straipsnio 7 dalies A punktą: „kai ryšio duomenys visiškai arba iš dalies yra įvykio duomenys ir jais siekiama užkirsti kelią sunkiam nusikaltimui arba jį nustatyti; bet kuriuo kitu atveju siekiama užkirsti kelią nusikaltimui arba jį nustatyti arba užkirsti kelią neramumams“.

([323]) Ryšių duomenų praktikos kodekse nurodyta, kad „jeigu prašymas, susijęs su nacionaliniu saugumu, gali būti pateikiamas pagal 60A arba 61 straipsnį, sprendimą dėl tinkamiausio leidimo išdavimo būdo atitinkamu atveju priima pavienės valdžios institucijos. Valdžios institucijos, kurios nori pasinaudoti paskirtojo vyresniojo pareigūno būdu, turėtų būti nustačiusios aiškias gaires dėl to, kada šis leidimo išdavimo būdas yra tinkamas“ (Ryšio duomenų praktikos kodekso 5.19 dalis, galima rasti šiuo adresu: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/822817/Communications_Data_Code_of_Practice.pdf).

([324]) 2016 m. TĮA 70 straipsnio 3 dalyje pateikta „paskirtojo pareigūno“ apibrėžtis, kuri įvairuoja priklausomai nuo atitinkamos valdžios institucijos (kaip nustatyta 2016 m. TĮA 4 priede).

([325]) Išsamesnė informacija apie paskirto vyresniojo pareigūno nepriklausomumą pateikta Ryšio duomenų praktikos kodekse (Ryšių duomenų praktikos kodeksas, 4,12–4,17 punktai, žr. 323 išnašą).

([326]) Tai yra šie pagrindai: i) nacionalinis saugumas; ii) nusikaltimo prevencija arba nustatymas arba neramumų prevencija („įvykių duomenys“ apima tik sunkaus nusikaltimo duomenis); iii) Jungtinės Karalystės ekonominės gerovės interesai tiek, kiek jie taip pat yra svarbūs nacionalinio saugumo interesams; iv) atsižvelgiant į visuomenės saugumo interesus; v) siekiant užkirsti kelią mirčiai arba sužalojimui, arba bet kokiai žalai asmens fizinei arba psichinei sveikatai, arba sumažinti bet kokį sužalojimą arba žalą asmens fizinei arba psichinei sveikatai; vi) siekiant padėti atlikti netinkamo teisingumo vykdymo atvejų tyrimus arba vii) nustatyti mirusio asmens tapatybę arba asmens, kuris dėl tam tikros būklės negali savęs atpažinti, tapatybę (2016 m. TĮA 61 straipsnio 7 dalis).

([327]) 2016 m. TĮA 60A straipsnio 1 dalies b punktas.

([328]) Ryšio duomenų praktikos kodekso 3.3 ir kt. dalys, žr. 323 išnašą.

([329]) Ryšio duomenų praktikos kodekso 3.13 dalis, žr. 323išnašą.

([330]) 2016 m. TĮA 60 straipsnio 1 dalies c punktas.

aptarti prašančioji institucija ([331]). Be to, reikia labai atkreipti dėmesį į gautinų ryšių duomenų rūšį (ar tai duomenys apie subjektą, ar įvykį ([332])); pirmenybė turi būti teikiama mažiau intervencinės kategorijos duomenų naudojimui ([333]). Ryšio duomenų praktikos kodekse taip pat pateikta konkrečių nurodymų dėl leidimų, susijusių su konkrečių profesijų (pvz., gydytojų, advokatų, žurnalistų, parlamento narių arba dvasininkų) ([334]) asmenų ryšio duomenimis, kuriems taikomos papildomos apsaugos priemonės ([335]).

ii) *Pranešimas, kuriame reikalaujama saugoti ryšio duomenis*

(206) 2016 m. TĮA 4 dalyje nustatytos ryšio duomenų saugojimo taisyklės, visų pirma kriterijai, kuriais remiantis valstybės sekretoriui leidžiama paskelbti pranešimą apie duomenų saugojimą ([336]). TĮA nustatytos apsaugos priemonės taikomos saugant duomenis tiek teisėsaugos, tiek nacionalinio saugumo tikslais.

(207) Išduodant tokius pranešimus apie duomenų saugojimą siekiama užtikrinti, kad telekomunikacijų operatoriai ne ilgiau nei 12 mėnesių saugotų atitinkamus ryšio duomenis, kurie kitu atveju būtų ištrinti po to, kai tampa nereikalingi veiklos tikslais ([337]). Su saugomais duomenimis galima susipažinti reikalaujamą laikotarpį, jeigu jie paskui tampa reikalingi valdžios institucijai, remiantis leidimu dėl tikslinio ryšio duomenų gavimo, kaip numatyta 2016 m. TĮA 3 dalyje ir aprašyta (203)–(205) konstatuojamosiose dalyse.

(208) Įgaliojimams reikalauti saugoti tam tikrus duomenis taikomi įvairūs apribojimai ir apsaugos priemonės. Valstybės sekretorius pranešimą apie duomenų saugojimą vienam ar keliams operatoriams ([338]) gali išduoti tik tais atvejais, kai mano, kad reikalavimas saugoti duomenis yra būtinas, remiantis vienu iš teisės aktuose nustatytų pagrindų ([339]), ir jis yra proporcingas siekiamam tikslui ([340]). Kaip paaiškinta

([331]) Nurodant šią informaciją, būtina: i) aprašyti, kokią naudą gauti duomenys turės tyrimui arba operacijai; ii) paaiškinti prašomų terminų svarbą, įskaitant paaiškinimą, ar šie terminai yra proporcingi tiriamam įvykiui; iii) paaiškinti ribojimų lygmens pagrindimą, atsižvelgiant į naudą, kurią duomenys duos tyrimui (šis pagrindimas turėtų apimti informaciją apie tai, ar, siekiant tikslo, būtų galima atlikti mažiau intervencinio pobūdžio tyrimus); iv) aptarti asmens teises (visų pirma teisę į privatumą ir atitinkamais atvejais žodžio laisvę) ir suderinti šias teises su tyrimo nauda; v) pateikti išsamią informaciją apie galimus papildomus ribojimus ir tai, kokį poveikį prašomi terminai daro papildomiems ribojimams (Ryšio duomenų praktikos kodekso 3.22–3.26 dalys, žr. 323 išnašą).

([332]) Žr. 313 išnašą.

([333]) Jeigu norima gauti labiau intervencinio pobūdžio ryšio duomenų (t. y. įvykio duomenys), kodekse konkrečiai nurodyta, kad pirmiausia būtų labiau tinkama gauti duomenis apie subjektą arba tiesiogiai gauti duomenis apie įvykius tam tikrais skubiais atvejais (Ryšio duomenų praktikos kodekso 6.10–6.14 dalys, žr. 323 išnašą).

([334]) Ryšio duomenų praktikos kodekso 8.8–8.44 dalys, žr. 323 išnašą.

([335]) Praktikos kodekse konkrečiai nustatyta, kad „leidimą išduodantis asmuo, nagrinėdamas tokius prašymus, turi būti ypač atidus ir skirti papildomą dėmesį aplinkybėms, susijusios su tuo, ar toks prašymas gali sukelti nenumatytų pasekmių ir ar prašymas visiškai atitinka viešąjį interesą“ (Ryšio duomenų praktikos kodekso 8.8 dalis). Be to, būtina saugoti šios rūšies prašymų įrašus, o kito patikrinimo metu tokie prašymai turėtų būti pateikti IPC susipažinti (Ryšio duomenų praktikos kodekso 8.10 dalis, žr. 323 išnašą).

([336]) 2016 m. TĮA 87–89 straipsniai.

([337]) Pagal 2016 m. TĮA 90 straipsnį telekomunikacijų operatorius, kuriam įteikiamas pranešimas apie duomenų saugojimą, gali prašyti, kad jį išdavęs valstybės sekretorius atliktų peržiūrą.

([338]) Pagal 2016 m. TĮA 87 straipsnio 2 dalies a punktą pranešimas apie duomenų saugojimą gali būti susijęs su „konkrečiu veiklos vykdytoju arba bet kokiu operatorių aprašymu“.

([339]) Tai šie pagrindai: i) nacionalinio saugumo interesai; ii) taikytinas su nusikaltimu susijęs tikslas (kaip apibrėžta 2016 m. TĮA 87 straipsnio 10A dalyje; iii) Jungtinės Karalystės ekonominės gerovės interesai tiek, kiek jie taip pat yra svarbūs nacionalinio saugumo interesams; iv) visuomenės saugumo interesai; v) siekiant užkirsti kelią mirčiai arba sužalojimui, arba bet kokiai žalai asmens fizinei arba psichikos sveikatai, arba sumažinti bet kokį sužalojimą arba žalą asmens fizinei arba psichikos sveikatai, arba vi) padėti atlikti netinkamo teisingumo vykdymo atvejų tyrimus (TĮA 87 straipsnis).

([340]) 2016 m. TĮA 87 straipsnis. Be to, pagal atitinkamą praktikos kodeksą, siekiant įvertinti pranešimo apie duomenų saugojimą proporcingumą, taikomi 2016 m. TĮA 2 straipsnio 2 dalyje nustatyti kriterijai, visų pirma reikalavimas įvertinti, ar pranešimu siekiamą tikslą būtų galima pagrįstai pasiekti mažiau intervencinėmis priemonėmis. Panašiai, kaip ir gautų ryšio duomenų proporcingumo vertinimo atveju, Ryšio duomenų praktikos kodekse paaiškinta, kad tokio vertinimo metu „ribojimo mastas derinamas su asmens teise į jo privataus gyvenimo gerbimą ir konkrečia tyrimo nauda (Ryšio duomenų praktikos kodekso 16.3 dalis, žr. 323 išnašą).

pačiame 2016 m. TĮA ([341]), prieš įteikdamas pranešimą apie duomenų saugojimą, valstybės sekretorius privalo atsižvelgti į: tikėtiną pranešimo naudą ([342]); telekomunikacijų paslaugų aprašymą; saugotinų duomenų ribojimo tinkamumą nurodant vietą arba apibūdinant asmenis, kuriems teikiamos telekomunikacijų paslaugos ([343]); tikėtiną bet kokių telekomunikacijų paslaugos naudotojų (jei žinomi), su kuriais yra susijęs pranešimas, skaičių ([344]); technines galimybes laikytis pranešimo; tikėtinas pranešimo laikymosi išlaidas ir bet kurį kitą pranešimo poveikį telekomunikacijų operatoriui (arba operatorių aprašymą), su kuriuo jis yra susijęs ([345]). Kaip išsamiau aprašyta Ryšio duomenų praktikos kodekso 17 skyriuje, visuose pranešimuose dėl duomenų saugojimo turi būti nurodyta kiekviena duomenų, kuriuos reikia saugoti, rūšis ir tai, kaip ta duomenų rūšis dera su saugojimo būtinumo patikrinimais.

(209) Visais atvejais (tiek nacionalinio saugumo, tiek teisėsaugos tikslais) Valstybės sekretoriaus sprendimą paskelbti pranešimą apie duomenų saugojimą turi patvirtinti nepriklausomas teismo komisaras pagal vadinamąją dvigubo patvirtinimo procedūrą: jis visų pirma turi patikrinti, ar nurodymas saugoti atitinkamus ryšių duomenis yra būtinas ir proporcingas vienam ar keliems teisės aktuose nustatytiems tikslams ([346]).

3.3.1.1.3. Įrangos perėmimas

(210) Įrangos perėmimas – tai tam tikri metodai, naudojami siekiant gauti įvairius duomenis iš įrangos ([347]), įskaitant kompiuterius, planšetinius kompiuterius ir išmaniuosius telefonus, taip pat kabelius, laidus ir kaupiklius ([348]). Įrangos perėmimas sudaro sąlygas gauti ryšio ir įrangos turinio duomenis ([349]).

(211) Pagal 2016 m. TĮA 13 straipsnio 1 dalį tam, kad žvalgybos tarnyba galėtų perimti įrangą, reikalingas pagal „dvigubo patvirtinimo“ procedūrą, nustatytą 2016 m. TĮA, išduotas orderis, ir jeigu yra „ryšys su Didžiosios Britanijos salomis“ ([350]). Remiantis Jungtinės Karalystės institucijų pateiktais paaiškinimais, tais atvejais, kai duomenys

([341]) Žr. 2016 m. TĮA 88 straipsnį.

([342]) Nauda gali būti esama arba numatoma ir turi būti susijusi su teisės aktuose nustatytais tikslais, kuriais galima saugoti duomenis (Ryšio duomenų praktikos kodekso 17.17 dalis, žr. 323 išnašą).

([343]) Šiomis aplinkybėmis reikės nuspręsti, ar būtina ir proporcinga nustatyti visapusišką pranešimo apie duomenų saugojimą geografinę apimtį ir ar būtina ir proporcinga įtraukti arba išbraukti kokių nors konkrečių asmenų apibūdinimą (Ryšio duomenų praktikos kodekso 17.17 dalis, žr. 323 išnašą).

([344]) Tai padės valstybės sekretoriui įvertinti klientų ribojimo lygį ir tikėtiną saugotinų duomenų naudą (Ryšio duomenų praktikos kodekso 17.17 dalis, žr. 323 išnašą).

([345]) 2016 m. TĮA 88 straipsnis.

([346]) 2016 m. TĮA 89 straipsnis.

([347]) Pagal 2016 m. TĮA 135 straipsnio 1 dalį ir 198 straipsnio 1 dalį „įranga“ reiškia įrangą, gaminančią elektromagnetinę, akustinę arba kitą spinduliuotę, ir bet kurį prietaisą, kuris gali būti naudojamas kartu su tokia įranga.

([348]) Ryšių perėmimo įrangos praktikos kodeksas, galima rasti šiuo adresu: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715479/Equipment_Interference_Code_of_Practice.pdf , paragraph 2.2.

([349]) Įrangos duomenys 2016 m. TĮA 100 straipsnyje apibrėžiami kaip sistemos duomenys ir duomenys, kurie a) yra ryšio (siuntėjo ar pan.) sudedamoji dalis, prie ryšio pridėti arba su juo logiškai susieti duomenys, arba bet kuris kitas informacijos elementas; b) gali būti logiškai atskirti nuo likusios ryšio dalies arba informacijos elemento ir c) jei atskirti, neatskleistų jokios informacijos, kuri pagrįstai galėtų būti laikoma ryšių arba informacijos elemento prasme (jeigu ji yra).

([350]) Kad orderio reikalavimas būtų privalomas, pagal 2016 m. TĮA 13 straipsnio 1 dalį taip pat reikalaujama, kad žvalgybos tarnybos veika atitiktų vieno ar daugiau nusikaltimų pagal 1990 m. Netinkamo kompiuterių panaudojimo akto 1–3A straipsnius sudėtį. Tą būtų galima pasakyti apie didžiąją daugumą aplinkybių, žr. Įrangos perėmimo praktikos kodekso 3.32 ir 3.6–3.9 dalis. Pagal 2016 m. TĮA 13 straipsnio 2 dalį esama „ryšio su Didžiosios Britanijos salomis“, jeigu a) bet kuri veika būtų padaryta Didžiosios Britanijos salose (nepaisant įrangos, kuri būtų perimta arba kurią būtų galima perimti, buvimo vietos), b) žvalgybos tarnyba mano, kad bet kuri įranga, kuri būtų perimta arba kurią būtų galima perimti, galėtų būti arba gali būti Didžiosios Britanijos salose kuriuo nors perėmimo momentu, arba c) perėmimo tikslas yra gauti i) ryšius, išsiųstus asmens arba asmeniui, kuris tuo metu yra arba, žvalgybos tarnybos manymu, turi būti Didžiosios Britanijos salose, ii) privačią informaciją, susijusią su asmeniu, kuris tuo metu yra arba, žvalgybos tarnybos manymu, turi būti Didžiosios Britanijos salose, arba iii) įrangos duomenis, kurie yra ryšių arba informacijos, kuriems taikomas i arba ii papunktis, sudedamoji dalis arba su ja susiję.

perduodami iš Europos Sąjungos Jungtinei Karalystei pagal šį sprendimą, „ryšys su Didžiosios Britanijos salomis“ visada bus, todėl bet koks įrangos perėmimas, susijęs su tokiais duomenimis, turės būti atliekamas laikantis privalomo orderio reikalavimo, nustatyto 2016 m. TĮA 13 straipsnio 1 dalyje ([351]).

(212) Taisyklės dėl tikslinio įrangos perėmimo išdėstytos 2016 m. TĮA 5 dalyje. Panašiai, kaip ir tikslinis perėmimas, tikslinis įrangos perėmimas turi būti susijęs su konkrečiu „taikiniu“, kuris turi būti apibūdintas orderyje ([352]). Išsami informacija apie tai, kaip turi būti nustatomas „taikinys“, priklauso nuo dalyko ir perimamos įrangos rūšies.. TĮA 115 straipsnio 3 dalyje nurodyta informacija, kuri turi būti pateikta orderyje (pvz., asmens vardas ir pavardė arba organizacijos pavadinimas, vietos aprašymas), priklausomai, pvz., nuo to, ar perėmimas yra susijęs su įranga, kuri priklauso konkrečiam asmeniui, organizacijai arba grupei asmenų, yra jo naudojama ar disponuojama konkrečioje vietoje ir pan. ([353]). Tikslas, kuriuo remiantis galima išduoti tikslinio įrangos perėmimo orderius, priklauso nuo jį prašančios išduoti valdžios institucijos ([354]).

(213) Panašiai, kaip ir tikslinio perėmimo atveju, išduodančioji institucija turi išnagrinėti, ar priemonė yra būtina siekiant konkretaus tikslo ir ar ji yra proporcinga siekiamam tikslui ([355]). Be to, taip pat reikėtų atsižvelgti į tai, ar esama informacijos saugumą, saugojimą ir atskleidimą užtikrinančių priemonių, įskaitant „atskleidimo užsienyje“ atvejus ([356]) (žr. (196) konstatuojamąją dalį).

(214) Orderį turi patvirtinti teismo komisaras, išskyrus skubius atvejus ([357]). Pastaruoju atveju teismo komisarą reikia informuoti apie išduotą orderį ir jį privaloma patvirtinti per tris darbo dienas. Jeigu teismo komisaras atsisako jį patvirtinti, orderis nustoja galioti ir negali būti atnaujintas ([358]). Be to, teismo komisaras turi teisę reikalauti, kad visi pagal orderį gauti duomenys būtų ištrinti ([359]). Tai, kad orderis buvo išduotas skubos tvarka, nereiškia, kad jam netaikoma *ex post* priežiūra (žr. (244)–(255)konstatuojamąsias dalis) ar tai, kad jis negali būti asmens apskųstas teisme (žr. (260)–(270)konstatuojamąsias dalis). Asmenys gali pateikti skundą ICO arba dėl bet kokio įtariamo elgesio įprasta tvarka kreiptis į Tyrimo įgaliojimų teismą. Visais atvejais komisaras atlieka būtinumo ir proporcingumo patikrinimą, taikytiną tikslinio perėmimo prašymų atvejais ([360]) (žr. (192) konstatuojamąją dalį).

([351]) Didesnio išsamumo dėlei reikėtų pažymėti, kad net ir situacijose, kuriose nėra „ryšio su Didžiosios Britanijos salomis“, todėl įrangos perėmimui netaikomas privalomas orderio reikalavimas pagal 2016 m. TĮA 13 straipsnio 1 dalį, žvalgybos tarnyba, kuri planuoja užsiimti veikla, dėl kurios ji gali gauti masinio įrangos perėmimo orderį, turėtų gauti tokį orderį politiniu požiūriu (Įrangos perėmimo praktikos kodekso 3.24 dalis). Net jeigu pagal 2016 m. TĮA teisiškai nereikalaujama gauti įrangos perėmimo orderį ir jis nereikalaujamas politiniu požiūriu, žvalgybos tarnybų veiksmams taikomos įvairios sąlygos ir ribojimai pagal 1994 m. Žvalgybos tarnybų akto 7 straipsnį. Tai visų pirma yra reikalavimas gauti valstybės sekretoriaus leidimą – jis turi įsitikinti, kad bet koks veiksmas neviršija to, kas yra būtina siekiant tinkamai įvykdyti žvalgybos tarnybos funkcijas.

([352]) 2016 m. TĮA 115 straipsnyje reglamentuojamas orderio turinys, nurodant, kad jame turi būti nurodyti asmenų, organizacijų, vietos arba grupės asmenų, kurie yra „taikinys“, vardai ir pavardės ar pavadinimai arba apibūdinimai, tyrimo pobūdžio apibūdinimas ir veiklos, kuriai naudojama įranga, apibūdinimas. Jame taip pat turi būti aprašyta įrangos rūšis ir veiksmai, kuriuos turi teisę atlikti asmuo, kuriam skirtas orderis.

([353]) Taip pat žr. Įrangos perėmimo praktikos kodekso 5.7 dalį, žr. 348 išnašą.

([354]) Nacionalinio saugumo agentūros gali prašyti išduoti įrangos perėmimo orderį, kai tai yra būtina nacionalinio saugumo tikslais, siekiant nustatyti sunkų nusikaltimą ir (arba) atsižvelgiant į Jungtinės Karalystės ekonominės gerovės interesus tiek, kiek tokie interesai taip pat yra svarbūs užtikrinant nacionalinio saugumo interesus (2016 m. TĮA 102–103 straipsniai). Priklausomai nuo agentūros, įrangos perėmimo orderį gali būti prašoma išduoti teisėsaugos tikslu, kai tai yra būtina sunkaus nusikaltimo nustatymo arba prevencijos tikslais arba siekiant užkirsti kelią mirčiai arba bet kokiam asmens fizinės arba psichikos sveikatos sutrikdymui, arba siekiant sumažinti žalą asmens fizinei arba psichikos sveikatai (žr. 2016 m. TĮA 106 straipsnio 1 ir 3 dalys).

([355]) 2016 m. TĮA 102 straipsnio 1 dalis.

([356]) 2016 m. TĮA 129–131 straipsniai.

([357]) 2016 m. TĮA 109 straipsnis.

([358]) 2016 m. TĮA 109 straipsnio 4 dalis.

([359]) 2016 m. TĮA 110 straipsnio 3 dalies b punktas. Pagal Įrangos perėmimo praktikos kodekso 5.67 punktą skubumą lemia tai, ar būtų pagrįstai įmanoma prašyti teismo komisaro sutikimo išduoti orderį per laiką, turimą operatyviniam ar tyrimo veiksmui. Skubos tvarka išduodami orderiai turėtų atitikti vieną ar abi šias kategorijas: i) neišvengiama grėsmė gyvybei ar didelė žala, pavyzdžiui, jeigu asmuo buvo pagrobtas ir nustatyta, kad jo gyvybei gresia neišvengiamas pavojus; arba ii) žvalgybinės informacijos rinkimo arba tyrimo galimybė ribotą laiką, pavyzdžiui, A klasės narkotikų siunta netrukus bus įvežta į Jungtinę Karalystę, o teisėsaugos institucijoms reikia informacijos apie sunkių nusikaltimų vykdytojus, kad galėtų juos sulaikyti. Žr. 348 išnašą.

([360]) 2016 m. TĮA 108 straipsnis.

(215) Galiausiai konkrečios apsaugos priemonės, taikomos tiksliniam perėmimui, taip pat galioja įrangos perėmimui, atsižvelgiant į orderio galiojimo trukmę, pratęsimus ir pakeitimus, taip pat į parlamento narių pasiklausymą, daiktų, kuriems taikoma teisinė privilegija, ir žurnalistų medžiagos perėmimą (žr. išsamesnę informaciją 193 konstatuojamojoje dalyje).

3.3.1.1.4. Naudojimasis masiniais įgaliojimais

(216) Masiniai įgaliojimai reglamentuojami 2016 m. TĮA 6 dalyje. Be to, praktikos kodeksuose pateikta išsamesnė informacija apie masinių įgaliojimų naudojimą. Nors Jungtinės Karalystės teisėje sąvoka „masiniai įgaliojimai“ neapibrėžta, 2016 m. TĮA jie apibūdinti kaip didelio kiekio duomenų, kuriuos įvairiomis priemonėmis gavo vyriausybė, rinkimas ir saugojimas (t. y. masinio perėmimo įgaliojimai, masinis gavimas, masinis įrangos perėmimas ir masinių asmens duomenų rinkiniai), su kuriais paskui gali susipažinti institucijos. Šis apibūdinimas patikslinamas paaiškinant, kas nelaikoma „masiniais įgaliojimais“: tai nėra vadinamasis masinis sekimas nenustačius apribojimų ar apsaugos priemonių. Priešingai, kaip paaiškinta toliau, masiniai įgaliojimai apima apribojimus ir apsaugos priemones, skirtas užtikrinti, kad prieiga prie duomenų nebūtų suteikta be atrankos arba nepagrįstai ([361]). Visų pirma masiniai įgaliojimai gali būti naudojami, jeigu nustatomas techninės priemonės, kurią ketina naudoti nacionalinė žvalgybos agentūra, ir veiklos tikslo, kuriam prašoma taikyti tokią priemonę, ryšys.

(217) Be to, žvalgybos tarnybos masiniais įgaliojimais gali pasinaudoti tik gavusios valstybės sekretoriaus išduotą ir teismo komisaro patvirtintą orderį. Pasirenkant priemones žvalgybos duomenims rinkti, būtina atsižvelgti į tai, ar atitinkamą tikslą galima pasiekti „mažiau intervencinėmis priemonėmis“ ([362]). Šis požiūris grindžiamas teisės aktų sistema, kurios pagrindą sudaro proporcingumo principas, todėl pirmenybė teikiama tiksliniam, o ne masiniam duomenų rinkimui.

3.3.1.1.4.1. Masinis perėmimas ir masinis įrangos perėmimas

(218) Masinio perėmimo tvarka nustatyta 2016 m. TĮA 1 skyriaus 6 dalyje, o tos pačios dalies 3 skyriuje reglamentuojama masinio įrangos perėmimo tvarka. Abi šios tvarkos rūšys iš esmės yra vienodos, todėl tiems orderiams taikomos sąlygos ir papildomos apsaugos priemonės bus analizuojamos kartu.

i) *Orderio išdavimo sąlygos ir kriterijai*

(219) Masinio perėmimo orderis apima tik ryšių perėmimą tuo metu, kai juos perdavimo metu siunčia arba gauna už Didžiosios Britanijos salų esantys asmenys ([363]), vadinamieji ryšiai užjūrio teritorijoje ([364]), taip pat kitus

([361]) Remiantis lordo Davido Andersono, nepriklausomo terorizmo teisės aktų kritiko, ataskaita dėl masinių įgaliojimų, pateikta iki 2016 m. patvirtinimo, „turėtų būti aišku, kad masinis duomenų rinkimas ir saugojimas neprilygsta vadinamajam masiniam sekimui. *Bet kurioje savo pavadinimo vertoje teisinėje sistemoje bus nustatyti apribojimai ir apsaugos priemonės, skirti užtikrinti, kad prieiga prie saugomų neskelbtinų duomenų <...> nebūtų suteikta be atrankos arba nepagrįstai. Tokie įgaliojimai ir apsaugos priemonės iš tiesų yra nustatyti įstatyme*. Lord David Anderson, Report of the bulk power review (Masinių įgaliojimų peržiūros ataskaita), 2016 m. rugpjūčio mėn, 1.9 dalis (išskirta autoriaus), galima rasti šiuo adresu: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/546925/56730_Cm9326_WEB.PDF.

([362]) 2016 m. TĮA 2,2 straipsnis. Žr., pvz., Masinio ryšio duomenų gavimo praktikos kodekso 4.11 dalį, galima rasti šiuo adresu: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf.

([363]) Didžiosios Britanijos salos – tai Jungtinė Karalystė, Normandijos salos ir Meno sala ir jos apibrėžiamos 1978 m. Aiškinimo akto 1 priede, kurį galima rasti šiuo adresu: https://www.legislation.gov.uk/ukpga/1978/30/schedule/1.

([364]) Pagal 2016 m. TĮA 136 straipsnį „ryšiai užjūrio teritorijose“ reiškia: i) asmenų, esančių už Didžiosios Britanijos salų ribų, išsiųstus pranešimus, arba ii) asmenų, esančių už Didžiosios Britanijos salų ribų, gautus pranešimus. Ši tvarka, kurią patvirtino Jungtinės Karalystės institucijos, taip pat taikoma dviejų asmenų, esančių už Didžiosios Britanijos salų ribų, ryšiams. Europos Žmogaus Teisių Teismo didžioji kolegija byloje *Big Brother Watch ir kt. prieš Jungtinę Karalystę* (žr. 279 išnašą), 376 punkte, išnagrinėjusi panašų ryšių apribojimą (kalbant apie „išorės ryšius“), kurį galima užfiksuoti masiniu perėmimu pagal 2000 m. Tyrimo įgaliojimų reguliavimo aktą, nusprendė, kad jis buvo pakankamai apibrėžtas ir numatomas.

susijusius duomenis ir paskesnę perimtos medžiagos atranką ir nagrinėjimą ([365]). Pagal masinio įrangos perėmimo orderį ([366]) adresatui leidžiama saugiai perimti bet kokią įrangą, siekiant pasiklausyti užjūrio ryšių (įskaitant bet kokius ryšius, kuriuose kalbama, skamba muzika, garsai, pateikiami vaizdai arba užšifruoti duomenys), įrangos duomenis (duomenis, kurie sudaro sąlygas arba palengvina pašto tarnybos darbą, telekomunikacijos sistemos veikimą, telekomunikacijų paslaugų teikimą) arba bet kurią kitą informaciją ([367]).

(220) Valstybės sekretorius gali išduoti masinį orderį tik dėl paraiškos, kurią pateikė žvalgybos tarnybos vadovas ([368]). Orderis, kuriuo leidžiamas masinis perėmimas arba masinis įrangos perėmimas, gali būti išduodamas tik jeigu tai būtina atsižvelgiant į nacionalinio saugumo interesą ir siekiant užkirsti kelią sunkiam nusikaltimui arba jį nustatyti, arba atsižvelgiant į Jungtinės Karalystės ekonominės gerovės interesus, kai tai yra susiję su nacionaliniu saugumu ([369]). Be to, pagal 2016 m. TĮA 142 straipsnio 7 dalį reikalaujama, kad masinio perėmimo orderyje būtų pateikta išsamesnė informacija, užuot pateikus paprasčiausią nuorodą į „nacionalinio saugumo interesus“, „Jungtinės Karalystės ekonominę gerovę“ ir sunkių nusikaltimų prevenciją ir nustatymą“. Vis dėlto, turi būti nustatytas ryšys tarp prašomos priemonės ir vieno arba kelių operatyvinių tikslų, kurie turi būti nurodyti orderyje.

(221) Operatyvinio tikslo pasirinkimas yra daugiasluoksnio proceso rezultatas. 142 straipsnio 4 dalyje nustatyta, kad orderyje nurodyti operatyviniai tikslai turi būti įtraukti į žvalgybos tarnybų vadovų tvarkomą sąrašą, nes tikslai, kuriais jie pagrįsti, yra operatyviniai tikslai, kurių siekiant perimtas turinys arba antriniai duomenys, gauti remiantis masinio perėmimo orderiais, gali būti atrinkti tyrimui atlikti. Operatyvinių tikslų sąrašą turi patvirtinti valstybės sekretorius. Valstybės sekretorius tokį patvirtinimą gali duoti tik jei įsitikina, kad operatyvinis tikslas yra apibūdintas išsamiau, palyginti su bendraisiais orderį pateisinančiais pagrindais (nacionalinis saugumas arba nacionalinis saugumas ir ekonominė gerovė arba sunkių nusikaltimų prevencija) ([370]). Kiekvieno atitinkamo trijų mėnesių laikotarpio pabaigoje valstybės sekretorius privalo pateikti parlamento žvalgybų tarnybų komitetui operatyvinių tikslų sąrašą. Galiausiai operatyvinių tikslų sąrašą ne rečiau kaip kartą per metus privalo peržiūrėti ministras pirmininkas ([371]). Kaip pažymėjo Aukštasis teismas „jų nereikėtų sumenkinti iki nereikšmingų apsaugos priemonių, nes jie kartu sudaro sudėtingą atskaitomybės modelį, kuriame aukščiausiu lygmeniu dalyvauja parlamentas ir vyriausybės nariai“ ([372]).

(222) Tokiais operatyviniais tikslais taip pat ribojamas nagrinėjimo etape perimamos medžiagos atrankos mastas. Bet kurios remiantis masiniu orderiu surinktos medžiagos atranka tyrimui atlikti turi būti pagrįsta atsižvelgiant į operatyvinį (-ius) tikslą (-us). Kaip paaiškino Jungtinės Karalystės institucijos, tai reiškia, kad praktines tyrimo taisykles valstybės sekretorius privalo įvertinti jau orderio išdavimo etape, pateikdamas pakankamai informacijos, kad būtų įvykdytos 2016 m. TĮA 152–193 straipsniuose nustatytos pareigos ([373]). Valstybės sekretoriui pateikiama išsami informacija apie tas taisykles turėtų apimti, pvz., informaciją (jei taikytina) apie tai, kaip filtravimo taisyklės gali keistis orderio galiojimo metu ([374]). Daugiau informacijos apie procesą ir apsaugos priemones, taikomas filtravimo ir nagrinėjimo etapais, žr. (229) below konstatuojamąją dalį.

([365]) 2016 m. TĮA 136 straipsnio 4 dalis. Remiantis iš Jungtinės Karalystės vyriausybės gautais paaiškinimais, masinis perėmimas gali būti naudojamas, pvz., siekiant nustatyti anksčiau nežinomas grėsmes Jungtinės Karalystės nacionaliniam saugumui, filtruojant ir analizuojant perimtą medžiagą, ir taip išaiškinti žvalgybinę vertę turinčius ryšius (JK aiškinamojo dokumento H skirsnis „Nacionalinis saugumas“, p. 27–28, žr. 29 išnašą). Kaip paaiškino Jungtinės Karalystės institucijos, tokios priemonės gali būti naudojamos siekiant nustatyti ryšius tarp žinomų dominančių subjektų, taip pat siekiant ieškoti asmenų, kurie dar gali būti nežinomi, tačiau paaiškėti tyrimo metu, veiklos pėdsakų ir išsiaiškinti veiklos, kuri gali kelti grėsmę Jungtinei Karalystei, būdus.

([366]) Pagal 2016 m. TĮA 13 straipsnio 1 dalį tam, kad žvalgybos tarnyba galėtų perimti įrangą, reikalingas pagal 2016 m. TĮA, išduotas orderis, ir jeigu yra „ryšys su Didžiosios Britanijos salomis“, žr. (211) konstatuojamąją dalį.

([367]) 2016 m. TĮA 176 straipsnis. Masinio įrangos perėmimo orderyje negali būti leidžiami veiksmai, kurie (išskyrus atvejus, kai jie atliekami remiantis teisėtais įgaliojimais) yra neteisėtas perėmimas (išskyrus saugomų ryšių perėmimą). Remiantis JK aiškinamuoju dokumentu, gauta informacija gali būti reikalinga siekiant nustatyti dominančius subjektus ir ji paprastai būtų susijusi su didelio masto operacijomis (Aiškinamojo dokumento H skirsnis „Nacionalinis saugumas“, p. 28, žr. 29 išnašą).

([368]) 2016 m. TĮA 138 straipsnio 1 dalis ir 178 straipsnio 1 dalis.

([369]) 2016 m. TĮA 138 straipsnio 2 dalis ir 178 straipsnio 2 dalis.

([370]) Remiantis Jungtinės Karalystės institucijų pateiktais paaiškinimais, dėl operatyvinio tikslo, pvz., gali būti ribojama priemonės taikymo sritis atsižvelgiant į grėsmę konkrečioje geografinėje teritorijoje.

([371]) 2016 m. TĮA 142 straipsnio 4–10 dalys.

([372]) Aukštojo teisingumo teismo sprendimo *Liberty*, [2019] EWHC 2057 (Admin), 167 punktas.

([373]) Pagal 2016 m. TĮA 152 ir 193 straipsnius reikalaujama, kad: a) medžiaga tyrimui atlikti būtų atrenkama tik orderyje nurodytais operatyviniais tikslais, b) atrinkti medžiagą tyrimui atlikti yra būtina ir proporcinga visomis aplinkybėmis ir c) atrenkant medžiagą tyrimui atlikti nepažeidžiamas draudimas atrinkti medžiagą ir nustatyti ryšius, kuriuos išsiuntė asmenys, kurie turimomis žiniomis tuo metu yra Didžiosios Britanijos salose, arba kurie yra skirti tiems asmenims.

([374]) Žr. Ryšių perėmimo praktikos kodekso 6.6 straipsnį, žr. 278 išnašą.

(223) Masinius įgaliojimus galima leisti naudoti tik jeigu jie yra proporcingi siekiamam tikslui ([375]). Kaip nurodyta Perėmimo praktikos kodekse, atliekant bet kurį proporcingumo vertinimą, reikia „suderinti privatumo ribojimo mastą (ir kitus 2 straipsnio 2 dalyje išvardytus aspektus) su poreikiu imtis veiklos atsižvelgiant į tyrimą, operacijas ar pajėgumus. Veiksmais, kuriuos leista atlikti, turėtų būti suteiktos realios galimybės gauti tikėtiną naudą ir jie neturėtų būti neproporcingi arba savavališki“ ([376]). Kaip minėta, tai praktiškai reiškia, kad proporcingumo patikrinimas yra grindžiamas pusiausvyros tarp siekiamo tikslo („operatyvinis (-iai) tikslas (-ai)“) ir turimų techninių galimybių (pvz., tikslinis arba masinis perėmimas, įrangos perėmimas, ryšio duomenų gavimas) nustatymu, pirmenybę teikiant mažiausiai intervencinėmis priemonėms (žr. (181) ir (182) above konstatuojamąsias dalis). Jeigu tikslą atitinka daugiau nei viena priemonė, pirmenybę reikia teikti mažiau intervencinei priemonei.

(224) Papildoma apsaugos priemonė, susijusi su prašomos priemonės proporcingumo vertinimu, užtikrinama atsižvelgiant į tai, kad valstybės sekretorius privalo gauti atitinkamą informaciją, kuri yra reikalinga tam, kad jis galėtų tinkamai atlikti savo vertinimą. Perėmimo praktikos kodekse ir Įrangos perėmimo praktikos kodekse visų pirma reikalaujama, kad atitinkamos institucijos pateiktame prašyme būtų paminėtos prašymo aplinkybės, aprašyti perimtini ryšiai, o iš telekomunikacijų operatorių būtų reikalaujama teikti pagalbą, aprašyti leistini veiksmai, operatyviniai tikslai ir paaiškinama, kodėl veiksmai yra būtini ir proporcingi ([377]).

(225) Galiausiai svarbiausia tai, kad valstybės sekretoriaus sprendimą išduoti orderį privalo patvirtinti nepriklausomas teismo komisaras, kuris pasiūlytos priemonės būtinumą ir proporcingumą įvertina naudodamas tuos pačius principus, kuriuos naudotų teismas nagrinėdamas prašymą dėl teisminės peržiūros ([378]). Konkrečiau, teismo komisaras gaus valstybės sekretoriaus išvadas, ar orderis yra būtinas ir ar veiksmai yra proporcingi atsižvelgiant į 2016 m. TĮA 2 straipsnio 2 dalies principus (su privatumu susijusios bendrosios pareigos). Teismo komisaras taip pat peržiūrės valstybės sekretoriaus išvadas dėl to, ar kiekvienas iš orderyje nurodytų operatyvinių tikslų yra tikslas, dėl kurio būtina arba gali prireikti atrinkti medžiagą. Jeigu teismo komisaras atsisako patvirtinti sprendimą išduoti orderį, valstybės sekretorius gali: i) sutikti su sprendimu ir orderio neišduoti arba ii) perduoti klausimą spręsti tyrimo įgaliojimų komisarui, kad šis priimtų sprendimą (išskyrus atvejus, kai tyrimų įgaliojimų komisaras priėmė pradinį sprendimą) ([379]).

ii) *Papildomos apsaugos priemonės*

(226) 2016 m. TĮA nustatyti papildomi apribojimai dėl masinio orderio trukmės, galiojimo pratęsimo ir pakeitimo. Orderio galiojimo trukmė turi būti ne ilgesnė nei šeši mėnesiai ir bet kurį sprendimą pratęsti orderio galiojimą arba jį pakeisti (išskyrus nedidelius pakeitimus) turi patvirtinti teismo komisaras ([380]). Perėmimo praktikos kodekse ir Įrangos perėmimo praktikos kodekse nustatyta, kad orderio operatyvinių tikslų pakeitimas laikomas esminiu orderio pakeitimu ([381]).

([375]) 2016 m. TĮA 138 straipsnio 1 dalies b ir c punktai ir 178 straipsnio b ir c punktai.

([376]) Ryšių perėmimo praktikos kodekso 4.10 straipsnis, žr. 278 išnašą.

([377]) Ryšių perėmimo praktikos kodekso 6.20 straipsnis, žr. 278 išnašą, ir Įrangos perėmimo praktikos kodekso 6.13 straipsnis, žr. 348 išnašą.

([378]) 2016 m. TĮA 138 straipsnio 1 dalies g punktas ir 178 straipsnio 1 dalies f punktas. Europos Žmogaus Teisių Teismas visų pirma nurodė, kad išankstinis nepriklausomos įstaigos leidimas yra svarbi apsaugos nuo piktnaudžiavimo priemonė masinio perėmimo atveju. Europos Žmogaus Teisių Teismas (didžioji kolegija), *Big Brother Watch ir kt. prieš Jungtinę Karalystę* (žr. 269 išnašą), 351 ir 352 punktai Svarbu nepamiršti, kad šis sprendimas buvo susijęs su ankstesne teisine sistema (2000 m. Tyrimo įgaliojimų reguliavimo aktą), kurioje nebuvo kai kurių apsaugos priemonių (įskaitant išankstinį nepriklausomo teisminių institucijų komisaro leidimą), nustatytų 2016 m. TĮA.

([379]) 2016 m. TĮA 159 straipsnio 3 ir 4 dalys.

([380]) 2016 m. TĮA 143–146 ir 184–188 straipsniai. Skubaus pakeitimo atveju valstybės sekretorius pakeitimus gali atlikti be patvirtinimo, tačiau privalo informuoti komisarą, kuris tuomet privalo priimti sprendimą dėl pakeitimo patvirtinimo arba atsisakymo jį patvirtinti (2016 m. TĮA 147 straipsnis). Orderis turi būti panaikintas, jeigu jis nebebūtinas arba nebeproporcingas, arba pagal orderį perimto turinio, metaduomenų arba kitų gautų duomenų nebereikia tirti atsižvelgiant į bet kurį orderyje nurodytą operatyvinį tikslą (2016 m. TĮA 148 ir 189 straipsniai).

([381]) Ryšių perėmimo praktikos kodekso 6.44–-6.47 straipsnis, žr. 278 išnašą, ir Įrangos perėmimo praktikos kodekso 6.48 straipsnis, žr. 348 išnašą.

(227) Panašiai, kaip ir tikslinio perėmimo atveju, 2016 m. TĮA 6 dalyje nustatyta, kad valstybės sekretorius privalo užtikrinti taisyklių galiojimą, kad būtų suteiktos remiantis orderiu gautos medžiagos saugojimas ir atskleidimas ([382]), tą patį galima pasakyti apie medžiagos atskleidimą užsienyje ([383]). Visų pirma 2016 m. TĮA 150 straipsnio 5 dalyje ir 191 straipsnio 5 dalyje reikalaujama, kad kiekviena bet kurios tos medžiagos, surinktos remiantis orderiu, kopija būtų saugoma saugiai ir sunaikinama kuo greičiau, kai nebelieka jos saugojimą pateisinančių pagrindų, o 2016 m. TĮA 150 straipsnio 2 dalyje ir 191 straipsnio 2 dalyje reikalaujama, kad asmenų, kuriems atskleidžiama medžiaga, skaičius ir mastas, kuriuo atskleidžiama bet kokia medžiaga, būtų prieinama arba kopijuojama tik tiek, kiek tai yra būtina teisės aktuose nustatytais tikslais ([384]).

(228) Galiausiai tais atvejais, kai medžiaga, perimta atliekant masinį perėmimą arba masinį įrangos perėmimą, turi būti perduota trečiajai valstybei („informacijos atskleidimas užsienyje“), 2016 m. TĮA nustatyta, kad valstybės sekretorius privalo užtikrinti, kad būtų nustatytos tinkamos priemonės, siekiant užtikrinti, kad toje trečiojoje šalyje būtų panašios informacijos saugumo, saugojimo ir atskleidimo priemonės ([385]). Be to, 2018 m. DAA 109 straipsnyje nustatyti konkretūs reikalavimai dėl žvalgybos tarnybų vykdomo tarpvalstybinio asmens duomenų perdavimo į trečiąsias valstybes arba tarptautinėms organizacijoms: duomenų neleidžiama perduoti į valstybę arba teritoriją, esančią už Jungtinės Karalystės ribų, arba tarptautinei organizacijai, išskyrus atvejus, kai duomenis perduoti yra būtina arba proporcinga duomenų valdytojui siekiant įvykdyti teisės akte nustatytas funkcijas arba kitais 1989 m. Saugumo tarnybų akto 2 straipsnio 2 dalies a punkte arba 1994 m. Žvalgybos tarnybų akto 2 straipsnio 2 dalies a punkte ir 4 straipsnio 2 dalies a punkte nustatytais tikslais ([386]). Svarbu pažymėti, kad šie reikalavimai galioja ir tais atvejais, kai taikoma nacionalinio saugumo išimtis pagal 2018 m. DAA 110 straipsnį, nes 2018 m. DAI 110 straipsnyje šio akto 109 straipsnis nenurodytas kaip viena iš nuostatų, kurios gali būti netaikomos, jei nacionalinio saugumo užtikrinimo tikslais reikia išimties tvarka netaikyti tam tikrų nuostatų.

(229) Patvirtinus orderį ir surinkus masinius duomenis, duomenys prieš juos tiriant bus atrenkami. Atrankos ir turimo etape taikomas papildomas proporcingumo patikrinimas – jį atlieka analitikas, kuris, remdamasis orderyje nurodytais operatyviniais tikslais (ir galbūt esamomis filtravimo taisyklėmis), apibrėžia atrankos kriterijus. Kaip nustatyta TĮA 152 ir 193 straipsniuose, išduodamas orderį, valstybės sekretorius privalo užtikrinti, kad būtų nustatytos taisyklės, kuriomis garantuojama, kad medžiaga būtų atrenkama tik siekiant konkrečių operatyvinių tikslų ir kad medžiaga būtų būtina ir proporcinga visomis aplinkybėmis. Šiuo atžvilgiu Jungtinės Karalystės institucijos paaiškino, kad perimta masinė medžiaga pirmiausia atrenkama taikant automatinį filtravimą, siekiant atmesti duomenis, kurie vargu ar yra susiję su nacionalinio saugumo interesu. Filtrai ilgainiui keičiasi (kartu su interneto srauto modelių, tipų ir protokolų pokyčiais) ir priklausys nuo technologijos bei operatyvinių aplinkybių. Po šio etapo duomenis galima atrinkti tyrimui atlikti tik jeigu jie yra svarbūs atsižvelgiant į orderyje nustatytus konkrečius operatyvinius tikslus ([387]). 2016 m. TĮA numatytos apsaugos priemonės, susijusios su surinktos medžiagos nagrinėjimu, taikomos visų rūšių duomenims (ir perimtiems, ir antriniams) ([388]). 2016 m. TĮA 152 ir 193 straipsniuose taip pat nustatytas bendras draudimas atrinkti tyrimui atlikti medžiagą, kurioje nurodomi pokalbiai, kuriuos išsiuntė Didžiosios Britanijos salose esantys asmenys arba kurie skirti šiose salose esantiems asmenims. Jeigu institucijos nori nagrinėti tokią medžiagą, jos pagal 2016 m. TĮA 2 ir 4 dalis turėtų pateikti prašymą dėl tikslinio tyrimo orderio, kurį išdavė valstybės sekretorius ir patvirtino teismo komisaras ([389]). Jeigu asmuo tyrimui atlikti sąmoningai atrenka perimtą turinį pažeisdamas teisės aktuose nustatytus reikalavimus ([390]), jis padaro nusikalstamą veiką ([391]).

---

([382]) 2016 m. TĮA 156 straipsnis.

([383]) 2016 m. TĮA 150 ir 191 straipsniai.

([384]) Europos Žmogaus Teisių Teismo didžioji kolegija byloje *Big Brother Watch ir kt. prieš Jungtinę Karalystę* (žr. 268 išnašą) patvirtino pagal 2000 m. Tyrimo įgaliojimų reguliavimo aktą nustatytą papildomų apsaugos priemonių, susijusių su saugojimu, prieiga ir atskleidimu, sistemą, žr. 392–394 ir 402–405 punktus. Ta pati apsaugos priemonių sistema nustatyta ir 2016 m. TĮA.

([385]) 2016 m. TĮA 151 ir 192 straipsniai.

([386]) Daugiau informacijos apie šiuos tikslus pateikiama 312 išnašoje.

([387]) Ryšių perėmimo kodeksuose šiuo atžvilgiu nurodyta: „šios duomenų tvarkymo sistemos tvarko ryšių kanalų arba signalų, kuriuos nusprendė perimti perimančioji institucija, duomenis. Tuomet tų kanalų ir signalų srautui taikomi filtrai, pritaikyti taip, kad būtų atrinkti potencialią žvalgybinę vertę turinčių rūšių ryšiai kartu atmetant duomenis, kurie, tikėtina, turi mažiausią žvalgybinę vertę. Dėl šio filtravimo, kuris įvairiose duomenų tvarkymo sistemose bus labai skirtingas, didelė šių kanalų ir signalų ryšių dalis bus automatiškai atmesta. Paskui gali būti atliekamos papildomos sudėtingos paieškos, siekiant gauti papildomus ryšius, kurie, labiausiai tikėtina, turės didžiausią žvalgybinę vertę ir bus susiję su teisės aktuose nustatytomis agentūros funkcijomis. Tuomet šie ryšiai gali būti atrinkti įvertinimui dėl vieno ar kelių operatyvinių tikslų, nurodytų orderyje, su sąlyga, kad tenkinamos būtinumo ir proporcingumo sąlygos. Tik tie ryšių elementai, kurie nebuvo atmesti, gali būti teikiami įvertinti įgaliotiems pareigūnams“ (Ryšių perėmimo kodekso 6.6 dalis, žr. 278 išnašą).

([388]) Žr. 2016 m. TĮA 152 straipsnio 1 dalies a ir b punktus, pagal kuriuos abiejų rūšių duomenų (perimtų ir antrinių) nagrinėjimas turi būti atliekamas tik nurodytu tikslu ir visomis aplinkybėmis turi būti būtinas bei proporcingas.

([389]) Šios rūšies orderio nereikalaujama, jei duomenys, susiję su asmenimis, esančiais Britanijos salose, yra antriniai duomenys (žr. 2016 m. TĮA 152 straipsnio 1 dalies c punktą).

([390]) 2016 m. TĮA 152 ir 193 straipsniai.

([391]) 2016 m. TĮA 155 ir 196 straipsniai.

(230) Analitiko atliktą atrinktos medžiagos *ex post* vertinimą prižiūri IPC, kuris įvertina vertinimo atitiktį konkrečioms 2016 m. TĮA nustatytoms apsaugos priemonėms, taikomomis per tyrimo etapą ([392]) (taip pat žr. (229) konstatuojamąją dalį). IPC privalo nuolat peržiūrėti (įskaitant audito, patikrinimų ir tyrimų atlikimą), kaip valdžios institucijos naudojasi 2016 m. TĮA nustatytais tyrimo įgaliojimais ([393]). Šiuo atžvilgiu Perėmimo praktikos kodekse ir Įrangos perėmimo praktikos kodekse paaiškinta, kad agentūra privalo saugoti įrašus atsižvelgdama į paskesnį tyrimą ir auditus, ir šiuose įrašuose būtina išdėstyti, kodėl prieiga prie medžiagos įgaliotiems asmenims yra būtina ir proporcinga, taip pat turi būti nurodyti taikomi operatyviniai tikslai ([394]). Pavyzdžiui, savo 2018 m. metinėje ataskaitoje tyrimo įgaliojimų komisaro biuras (IPCO) ([395]) padarė išvadą, kad analitiko nustatyti pagrindimai, susiję su tam tikros masiškai surinktos medžiagos tyrimu, atitiko reikalaujamą proporcingumo standartą, nes juose buvo pakankamai duomenų apie analitikų užklausų motyvus, susijusius su siekiamu tikslu ([396]). 2019 m. ataskaitoje IPCO, kalbėdamas apie su masiniais duomenimis susijusius įgaliojimus, aiškiai pasakė ketinantis toliau tikrinti masinio duomenų perėmimo atvejus, be kita ko, išsamiai įvertinti taikomus selektorius ir paieškos kriterijus ([397]). Jis taip pat toliau atidžiai, kiekvienu konkrečiu atveju nagrinėdamas prašymus išduoti orderius pagal dvigubo patikrinimo principą ir atlikdamas vertinimą, atidžiai tikrins stebėjimo (tikslingo ar masinio) priemonių pasirinkimą ([398]). Į šią papildomą stebėseną bus deramai atsižvelgta Komisijai vykdant stebėseną, kaip nurodyta(281)–(284) konstatuojamosiose dalyse.

3.3.1.1.4.2. Masinis ryšio duomenų gavimas

(231) 2016 m. TĮA 6 dalies 2 skyriuje reglamentuojami masinio gavimo orderiai, kuriais adresatui leidžiama reikalauti, kad telekomunikacijų operatorius atskleistų bet kuriuos ryšio duomenis, kuriuos turi operatorius, arba gauti tuos duomenis. Šiais orderiais taip pat leidžiama prašančiajai institucijai atrinkti duomenis tolesniam tyrimo etapui. Kaip ir tikslinio ryšio duomenų saugojimo ir gavimo atveju (žr. (199) konstatuojamąją dalį), masinis ryšio duomenų gavimas paprastai nėra susijęs su ES duomenų subjektų asmens duomenimis, kurie pagal šį sprendimą perduodami į Jungtinę Karalystę. Pareiga atskleisti ryšio duomenis pagal 2016 m. TĮA 6 dalies 2 skyrių taikoma duomenims, kuriuos Jungtinės Karalystės telekomunikacijų operatoriai tiesiogiai surinko iš telekomunikacijų paslaugų naudotojų ([399]). Šios rūšies bendravimas su klientais tvarkant jų duomenis paprastai nėra susijęs su perdavimu, remiantis šiuo sprendimu, t. y. perdavimas iš ES duomenų valdytojo / tvarkytojo, Jungtinės Karalystės duomenų valdytojui / tvarkytojui.

(232) Tačiau siekiant išsamumo, sąlygos ir apsaugos priemonės, kuriomis reglamentuojama masinio ryšio duomenų gavimo tvarka, aprašyta toliau.

([392]) 2016 m. TĮA 152 ir 193 straipsniai.

([393]) 2016 m. TĮA 229 straipsnis.

([394]) Ryšių perėmimo praktikos kodekso 6.74 straipsnis, žr. 278 išnašą, ir Įrangos perėmimo praktikos kodekso 6.78 straipsnis, žr. 348 išnašą.

([395]) IPCO įsteigtas pagal 2016 m. TĮA 238 straipsnį, kad teiktų informacijos komisarui būtinus darbuotojus, patalpas, įrangą ir kitas priemones bei paslaugas, kurios yra būtinos jo funkcijoms vykdyti (žr. (251) konstatuojamąją dalį).

([396]) IPCO 2018 m. metinėje ataskaitoje konkrečiai nurodyta, kad GCHQ analitikų pateikti pagrindimai „atitiko keliamus standartus ir analitikai pateikė pakankamai informacijos pagrįsdami savo užklausų dėl masinių duomenų proporcingumą“. Tyrimo įgaliojimų komisaro 2018 m. metinės ataskaitos 6.22 dalis, žr. 464 išnašą.

([397]) Tyrimo įgaliojimų komisaro 2019 m. metinės ataskaitos 7.6 dalis, žr. 463 išnašą.

([398]) Tyrimo įgaliojimų komisaro 2019 m. metinės ataskaitos 10.22 dalis, žr. 463 išnašą.

([399]) Tokią išvadą galima daryti iš ryšio duomenų apibrėžties, pateiktos 2016 m. TĮA 261 straipsnio 5 dalyje, pagal kurią ryšio duomenis saugo arba gauna telekomunikacijų operatorius ir šie duomenys yra apie telekomunikacijos paslaugos naudotoją ir susiję su šios paslaugos teikimu, arba tai yra ryšio turinio duomenys, duomenys, kurie yra ryšio sudedamoji dalis, prie ryšio pridėti arba su juo logiškai susieti duomenys (taip pat žr. Masinio ryšio duomenų gavimo praktikos kodeksą, galima rasti šiuo adresu: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf 2.15–2.22 dalys). Be to, pagal telekomunikacijų operatoriaus apibrėžtį, pateiktą 2016 m. TĮA 261 straipsnio 10 dalyje, reikalaujama, kad telekomunikacijų operatorius būtų asmuo, siūlantis arba teikiantis telekomunikacijos paslaugą asmenims Jungtinėje Karalystėje arba eksploatuojantis telekomunikacijų sistemą, kuri (visa arba jos dalis) kontroliuojama Jungtinėje Karalystėje. Iš šių apibrėžčių aiškiai matyti, kad 2016 m. TĮA pareigų negalima nustatyti telekomunikacijų operatoriams, kurių įranga nėra Jungtinėje Karalystėje arba nėra joje kontroliuojama ir kurie nesiūlo arba neteikia paslaugų asmenims Jungtinėje Karalystėje (taip pat žr. Masinio ryšio duomenų gavimo praktikos kodekso 2.2 dalį). Jeigu ES abonentai (nesvarbu, ar jie yra ES, ar Jungtinėje Karalystėje) naudojasi paslaugomis Jungtinėje Karalystėje, bet kokius ryšius, susijusius su šios paslaugos teikimu, tiesiogiai rinktų Jungtinės Karalystės paslaugų teikėjas, užuot juos perdavus iš ES.

(233) 2016 m. TĮA pakeičia teisės aktus, susijusius su masinių ryšio duomenų gavimu, kuriam buvo taikomas ESTT sprendimas *Privacy International*. Toje byloje nagrinėjami teisės aktai buvo panaikinti, o pagal naują tvarką nustatytos konkrečios sąlygos ir apsaugos priemonės, kuriomis galima taikyti tokią priemonę.

(234) Visų pirma, kitaip nei pagal ankstesnę tvarką, kai valstybės sekretorius turėjo visišką diskreciją leisti naudoti priemonę ([400]), 2016 m. TĮA reikalaujama, kad valstybės sekretorius orderį išduotų tik jeigu priemonė yra būtina ir proporcinga. Tai praktiškai reiškia, kad šiuo atveju turėtų būti ryšys tarp prieigos prie duomenų ir siekiamo tikslo ([401]). Konkrečiau, valstybės sekretorius turės įvertinti, ar esama ryšio tarp prašomos priemonės ir vieno arba daugiau orderyje nurodyto (-ų) „operatyvinio (-ių) tikslo (-ų)“ (žr. (219) konstatuojamąją dalį). Dėl proporcingumo vertinimo atitinkamame praktikos kodekse nurodyta, kad „valstybės sekretorius privalo atsižvelgti į tai, ar tikslas, kuris turi būti pasiektas orderiu, galėtų pagrįstai būti pasiektas kitomis mažiau intervencinėmis priemonėmis (žr. akto 2 straipsnio 2 dalies a punktą). Pavyzdžiui, ar reikiamą informaciją galima gauti naudojantis mažiau intervencinėmis galiomis, pavyzdžiui, tiksliniu ryšių duomenų gavimu“ ([402]).

(235) Pavyzdžiui, reikalingos informacijos gavimas naudojant mažiau intervencinius įgaliojimus, pvz., tikslinį ryšio duomenų gavimą. Kad atliktų tokį vertinimą, valstybės sekretorius remsis informacija, kurią savo prašyme turi pateikti žvalgybos tarnybų vadovai ([403]), pvz., dėl kokių priežasčių priemonė laikoma būtina atsižvelgiant į vieną iš teisės aktuose nurodytų pagrindų ir kodėl siekiamo tikslo nebūtų galima pagrįstai pasiekti kitomis, mažiau intervencinėmis priemonėmis ([404]). Be to, operatyviniais tikslais ribojamas tyrimui atlikti atrenkamų pagal orderį gautų duomenų mastas ([405]). Kaip nurodyta atitinkamame praktikos kodekse, operatyviniuose tiksluose turi būti aprašytas aiškus reikalavimas ir jame turi būti pakankamai išsamios informacijos, kad valstybės sekretorius įsitikintų, jog atrinkti gautus duomenis tyrimui atlikti galima tik atsižvelgiant į konkrečias priežastis ([406]). Iš tiesų, valstybės sekretorius prieš leisdamas išduoti orderį turės užtikrinti, kad būtų nustatytos konkrečios taisyklės, kuriomis garantuojama, kad medžiaga, kurią būtina išnagrinėti siekiant operatyvinio ir teisės aktuose nustatyto tikslo, būtų atrinkta tyrimui atlikti ir kad ji visomis aplinkybėmis turėtų būti proporcinga ir būtina. Šis konkretus reikalavimas, kuris atsispindi 2016 m. TĮA 158 ir 172 straipsniuose ([407]) ir yra susijęs su išankstiniu atrankos tikslais naudojamų kriterijų būtinumu ir proporcingumu, yra kita svarbi 2016 m. TĮA nustatytos tvarkos naujovė, palyginti su anksčiau galiojusia tvarka.

(236) 2016 m. TĮA taip pat nustatyta valstybės sekretoriaus pareiga užtikrinti, kad prieš išduodant orderį dėl masinio ryšio duomenų gavimo būtų nustatyti konkretūs apribojimai dėl surinktų asmens duomenų saugumo, saugojimo ir atskleidimo ([408]). Kalbant apie duomenų atskleidimą užsienyje, šiame kontekste taip pat taikomos (227) konstatuojamojoje dalyje aprašytos apsaugos priemonės, taikomos masiniam perėmimui ir masiniam įrangos perėmimui ([409]). Papildomi apribojimai teisėje nustatyti dėl masinio orderio galiojimo termino ([410]), galiojimo pratęsimo ([411]) ir pakeitimo ([412]).

(237) Svarbu tai, kad kaip ir kitų su masiniais duomenimis susijusių įgaliojimų atveju, prieš išduodamas orderį Valstybės sekretorius turi gauti teismo komisaro patvirtinimą ([413]). Tai pagrindinė 2016 m. TĮA nustatytos tvarkos nuostata.

---

([400]) 1984 m. Telekomunikacijų akto 94 straipsnio 1 dalyje buvo nustatyta, kad valstybės sekretorius galėjo pateikti „bendro pobūdžio nurodymus, kurie, valstybės sekretoriaus manymu, yra būtini arba tikslingi atsižvelgiant į nacionalinio saugumo interesus <...>“ (žr. 451 išnašą).

([401]) Žr. Sprendimo *Privacy International* 78 punktą.

([402]) Žr. Masinio ryšio duomenų gavimo praktikos kodekso 4.11 dalį (žr. 399414 išnašą).

([403]) Masinio duomenų gavimo orderį gali prašyti išduoti tik žvalgybos tarnybų vadovai, t. y.: i) Saugumo tarnybos generalinis direktorius; ii) Slaptosios žvalgybos tarnybos direktorius arba iii) GCHQ direktorius (žr. 2016 m. TĮA 158 ir 263 straipsnius).

([404]) Masinio ryšio duomenų gavimo praktikos kodekso 4.5 dalis (žr. 399 išnašą).

([405]) Pagal 2016 m. TĮA 161 straipsnį orderyje nurodyti operatyviniai tikslai turi būti įtraukti į žvalgybos tarnybų vadovų tvarkomą sąrašą („operatyvinių tikslų sąrašas“), nes tikslai, kuriais jie remiasi, yra operatyviniai tikslai, kurių siekiant ryšio duomenys, gauti remiantis masinio duomenų gavimo orderiais, gali būti atrinkti tyrimui atlikti.

([406]) Masinio ryšio duomenų gavimo praktikos kodekso 6.6 dalis (žr. 399 išnašą).

([407]) Pagal 2016 m. TĮA 172 straipsnį reikalaujama nustatyti konkrečias apsaugos priemones, kurios būtų taikomos tyrimui atlikti atrenkant gautus masinius ryšius. Be to, sąmoningas tyrimas pažeidžiant šias apsaugos priemones taip pat laikomas nusikalstama veika (žr. 2016 m. TĮA 173 straipsnį).

([408]) 2016 m. TĮA 171 straipsnis.

([409]) 2016 m. TĮA 171 straipsnio 9 dalis.

([410]) 2016 m. TĮA 162 straipsnis.

([411]) 2016 m. TĮA 163 straipsnis.

([412]) 2016 m. TĮA 164–166 straipsniai.

([413]) 2016 m. TĮA 159 straipsnis.

(238) IPC vykdo masiniu būdu surinktų materialinių (ryšių duomenų) nagrinėjimo procedūros *ex post* priežiūrą (žr. (254) below konstatuojamąją dalį). Šiuo atžvilgiu 2016 m. TĮA nustatytas reikalavimas, kad tyrimą atliekantis žvalgybos ekspertas, prieš atrinkdamas nagrinėtinus duomenis, turi nurodyti priežastį, kodėl siūlomas duomenų nagrinėjimas yra būtinas ir proporcingas atsižvelgiant į konkretų veiklos tikslą ([414]). IPCO 2019 m. metinėje ataskaitoje dėl GCHQ ir MI5 praktikos buvo nustatyta, kad „ypač svarbus masinių ryšio duomenų vaidmuo, atsižvelgiant į GCHQ vykdomos veiklos įvairovę, buvo tinkamai aptartas mūsų išnagrinėtose bylose. Išnagrinėjome prašomų duomenų pobūdį ir nurodytus žvalgybos reikalavimus ir įsitikinome, kad dokumentuose buvo pateikti įrodymai, iš kurių matyti, kad jų metodas buvo būtinas ir proporcingas ([415]). MI5 nurodytos pagrindžiančios priežastys atitiko gerus standartus ir būtinumo bei proporcingumo principus ([416])“.

3.3.1.1.4.3. Masinių asmens duomenų rinkinių saugojimas ir nagrinėjimas

(239) Orderiais dėl masinių asmens duomenų rinkinių ([417]) žvalgybos tarnyboms leidžiama saugoti ir tirti duomenų, kuriuose yra asmens duomenų, susijusių su įvairiais pavieniais asmenimis, rinkinius. Remiantis Jungtinės Karalystės institucijų pateiktais paaiškinimais, tokių duomenų rinkinių analizė gali būti „vienintelis būdas UKIC toliau vykdyti tyrimus ir nustatyti teroristų tapatybę, remiantis labai ribotais pagrindiniais žvalgybos duomenimis, arba kai ryšiai buvo sąmoningai nuslėpti“ ([418]). Orderiai yra dviejų rūšių: klasės orderiai dėl masinių asmens duomenų rinkinių ([419]), kurie yra susiję su tam tikros kategorijos duomenų rinkiniais, t. y. duomenų rinkiniai, kurie savo turiniu ir siūlomu naudojimu yra panašūs, ir dėl jų kyla panašių klausimų, pvz., susijusių su ribojimo ir neskelbtinumo laipsniu ir duomenų naudojimo proporcingumu, taip sudarant sąlygas valstybės sekretoriui įvertinti visų atitinkamos klasės duomenų gavimo vienu metu būtinumą ir proporcingumą. Pavyzdžiui, klasės orderis dėl masinių asmens duomenų rinkinių gali būti taikomas duomenų rinkiniams, susijusiems su panašiais maršrutais ([420]). Konkretūs orderiai dėl masinių asmens duomenų rinkinių ([421]), priešingai, yra susiję su vienu konkrečiu duomenų rinkiniu, pvz., naujoviškos arba neįprastos informacijos, kuri nepatenka į klasės orderio dėl masinių asmens duomenų rinkinių taikymo sritį, duomenų rinkiniu arba duomenų rinkiniu, susijusiu su konkrečių rūšių asmens duomenimis ([422]), dėl kurių reikalingos papildomos apsaugos priemonės ([423]). Pagal 2016 m. TĮA nuostatas, susijusias su masinių asmens duomenų rinkiniais, tokius duomenų rinkinius leidžiama nagrinėti ir saugoti tik jei tai būtina ir proporcinga ([424]) ir laikantis bendrųjų su privatumu susijusių pareigų ([425]).

(240) Įgaliojimams išduoti orderį dėl masinių asmens duomenų rinkinių taikoma dvigubo patikrinimo procedūra: priemonės būtinumo ir proporcingumo vertinimą pirmiausia atlieka valstybės sekretorius, o paskui teismo komisaras ([426]). Reikalaujama, kad valstybės sekretorius išnagrinėtų prašomo išduoti orderio rūšį ir taikymo sritį, atitinkamų duomenų kategoriją ir atskirų masinių asmens duomenų rinkinių, dėl kurių gali būti išduodamas konkrečios rūšies orderis, skaičių ([427]). Be to, kaip nurodyta Masinių asmens duomenų rinkinių saugojimo ir naudojimo žvalgybos tarnybose praktikos kodekse, būtina saugoti išsamius įrašus, o IPC gali atlikti auditą ([428]). Masinių asmens duomenų rinkinių saugojimas ir tyrimas nesilaikant 2016 m. TĮA reikalavimų yra nusikalstama veika ([429]).

---

([414]) IPCO 2019 m. metinės ataskaitos 8.6 dalis, žr. 463 išnašą.
([415]) IPCO 2019 m. metinės ataskaitos 10.4 dalis, žr. 463 išnašą.
([416]) IPCO 2019 m. metinės ataskaitos 8.37 dalis, žr. 463 išnašą.
([417]) 2016 m. TĮA 200 straipsnis.
([418]) Diskusijoms dėl duomenų apsaugos tinkamumo skirto Jungtinės Karalystės aiškinamojo dokumento H skirsnis „Nacionalinis saugumas“, p. 34, žr. 29 išnašą.
([419]) 2016 m. TĮA 204 straipsnis.
([420]) Masinių asmens duomenų rinkinių saugojimo ir naudojimo žvalgybos tarnybose praktikos kodekso 4.7 dalis, galima rasti šiuo adresu: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715478/Bulk_Personal_Datasets_Code_of_Practice.pdf.
([421]) 2016 m. TĮA 205 straipsnis.
([422]) Pavyzdžiui, neskelbtini asmens duomenys, žr. 2016 m. TĮA 202 straipsnį ir Masinių asmens duomenų rinkinių saugojimo ir naudojimo žvalgybos tarnybose praktikos kodekso 4.21 ir 4.12 dalis, žr. 469 išnašą.
([423]) Prašymą išduoti konkretų orderį dėl masinių asmens duomenų rinkinių privalo individualiai nagrinėti valstybės sekretorius, t. y. dėl vieno konkretaus duomenų rinkinio. Pagal TĮA 205 straipsnį reikalaujama, kad žvalgybos tarnyba savo prašyme dėl konkretaus orderio dėl masinių asmens duomenų rinkinių išsamiai paaiškintų atitinkamos medžiagos pobūdį ir mastą ir išvardytų „operatyvinius tikslus“, kurių siekdama atitinkama žvalgybos tarnyba nori nagrinėti masinių asmens duomenų rinkinius (kai žvalgybos tarnyba siekia gauti saugojimo ir tyrimo orderį, o ne tik saugojimo orderį). Jeigu naudojamas klasės orderis dėl masinių asmens duomenų rinkinių, sekretorius visą duomenų rinkinių kategoriją nagrinėja vienu metu.
([424]) 2016 m. TĮA 204 ir 205 straipsniai.
([425]) 2016 m. TĮA 2 straipsnis.
([426]) 2016 m. TĮA 204 ir 205 straipsniai.
([427]) Masinių asmens duomenų rinkinių saugojimo ir naudojimo žvalgybos tarnybose praktikos kodekso 5.2 dalis, žr. 420 išnašą.
([428]) Masinių asmens duomenų rinkinių saugojimo ir naudojimo žvalgybos tarnybose praktikos kodekso 8.1–8.15 punktus, žr. 420 išnašą.
([429]) Diskusijoms dėl duomenų apsaugos tinkamumo skirto Jungtinės Karalystės aiškinamojo dokumento H skirsnis „Nacionalinis saugumas“, p. 34, žr. 29 išnašą.

3.3.2. *Tolesnis surinktos informacijos naudojimas*

(241) Pagal 2018 m. DAA 4 dalį tvarkomi asmens duomenys negali būti tvarkomi su tikslu, kuriuo jie buvo surinkti, nesuderinamu būdu ([430]). 2018 m. DAA nustatyta, kad duomenų valdytojas duomenis gali tvarkyti kitu tikslu, kuris skiriasi nuo tikslo, kuriuo buvo surinkti duomenys, kai tai yra suderinama su pradiniu tikslu ir jeigu duomenų valdytojui pagal įstatymą leidžiama tvarkyti duomenis ir toks tvarkymas yra būtinas ir proporcingas ([431]). Be to, pagal 1989 m. Saugumo tarnybų aktą ir 1994 m. Žvalgybos tarnybų aktą konkrečiai reikalaujama, kad žvalgybos agentūrų vadovai užtikrintų, kad jokia informacija nebūtų gaunama ar atskleidžiama, išskyrus atvejus, kai tai yra būtina agentūros funkcijoms tinkamai įvykdyti arba kitais ribotais ir konkrečiais tikslais, išvardytais atitinkamose nuostatose ([432]).

(242) Be to, 2018 m. DAA 109 straipsnyje nustatyti konkretūs reikalavimai dėl žvalgybos tarnybų vykdomo tarpvalstybinio asmens duomenų perdavimo į trečiąsias valstybes arba tarptautinėms organizacijoms. Remiantis šia nuostata, asmens duomenų neleidžiama perduoti į valstybę arba teritoriją, esančią už Jungtinės Karalystės ribų, arba tarptautinei organizacijai, išskyrus atvejus, kai duomenis perduoti yra būtina arba proporcinga duomenų valdytojui siekiant įvykdyti teisės akte nustatytas funkcijas arba kitais 1989 m. Saugumo tarnybų akto 2 straipsnio 2 dalies a punkte arba 1994 m. Žvalgybos tarnybų akto 2 straipsnio 2 dalies a punkte ir 4 straipsnio 2 dalies a punkte nustatytais tikslais ([433]). Svarbu pažymėti, kad šie reikalavimai galioja ir tais atvejais, kai taikoma nacionalinio saugumo išimtis pagal 2018 m. DAA 110 straipsnį, nes 2018 m. DAI 110 straipsnyje šio akto 109 straipsnis nenurodytas kaip viena iš nuostatų, kurios gali būti netaikomos, jei nacionalinio saugumo užtikrinimo tikslais reikia išimties tvarka netaikyti tam tikrų nuostatų.

(243) Be to, kaip ICO pabrėžė savo gairėse dėl žvalgybos tarnybų vykdomo duomenų tvarkymo, be 2018 m. DAA 4 dalyje nustatytų apsaugos priemonių, žvalgybos agentūrai, kai ji dalijasi duomenimis su trečiosios šalies žvalgybos įstaiga, taip pat taikomos kitose joms taikomose teisinėse priemonėse numatytos apsaugos priemonės, kuriomis siekiama užtikrinti, kad asmens duomenys būtų gaunami, jais būtų dalijamasi ir jie būtų tvarkomi teisėtai ir atsakingai ([434]). Pavyzdžiui, 2016 m. TĮA nustatytos papildomos apsaugos priemonės, susijusios su medžiagos, surinktos vykdant tikslinį ryšių perėmimą ([435]), tikslinį įrangos perėmimą ([436]), masinį perėmimą ([437]), masinį ryšio duomenų gavimą ([438]) ir masinį įrangos perėmimą ([439]), perdavimu į trečiąją valstybę (vadinamasis informacijos atskleidimas užsienyje) . Visų pirma orderį išduodanti institucija privalo užtikrinti, kad galiotų taisyklės, kuriomis užtikrinama, kad duomenis gaunanti trečioji valstybė ribotų medžiagą matančių asmenų skaičių, jos atskleidimo mastą ir bet kokių padarytų medžiagos kopijų skaičių tiek, kiek tai yra būtina siekiant 2016 m. TĮA nustatytų tikslų ([440]).

3.3.3. *Priežiūra*

(244) Įvairios skirtingos įstaigos prižiūri, kaip vyriausybė naudojasi prieiga prie duomenų nacionalinio saugumo tikslais. Informacijos komisaras prižiūri, kaip tvarkomi asmens duomenys, atsižvelgdamas į 2018 m. DAA (daugiau informacijos apie komisaro nepriklausomumą, paskyrimą ir įgaliojimus žr. (85)–(98) konstatuojamąsias dalis), o

([430]) 2018 m. DAA 87 straipsnio 1 dalis.

([431]) 2018 m. DAA 87 straipsnio 3 dalis. Nors duomenų valdytojams šis principas gali būti netaikomas pagal 2018 m. DAA 110 straipsnį tiek, kiek tokia išimtis būtina siekiant užtikrinti nacionalinį saugumą, tokia išimtis turi būti vertinama kiekvienu konkrečiu atveju ir ja gali būti remiamasi tik tiek, kiek konkrečios nuostatos taikymas sukeltų neigiamų pasekmių nacionaliniam saugumui (žr. (132) konstatuojamąją dalį). Jungtinės Karalystės žvalgybos tarnybų nacionaliniai saugumo sertifikatai (galima rasti šiuo adresu: https://ico.org.uk/about-the-ico/our-information/national-security-certificates/) nepatenka į 2018 m. DAA 87 straipsnio 3 dalies taikymo sritį. Be to, kadangi bet koks duomenų tvarkymas kitu tikslu turi būti leistinas pagal įstatymą, žvalgybos tarnybos privalo turėti aiškų teisinį pagrindą, kuriuo remiantis duomenys tvarkomi toliau.

([432]) Daugiau informacijos apie šiuos tikslus pateikiama 312 išnašoje.

([433]) Žr. 312 išnašą.

([434]) ICO gairės dėl žvalgybos tarnybų duomenų tvarkymo (žr. 161 išnašą).

([435]) 2016 m. TĮA 54 straipsnis.

([436]) 2016 m. TĮA 130 straipsnis.

([437]) 2016 m. TĮA 151 straipsnis.

([438]) 2016 m. TĮA 171 straipsnio 9 dalis.

([439]) 2016 m. TĮA 192 straipsnis.

([440]) Taisyklėse turi būti nustatytos priemonės, kuriomis užtikrinama, kad kiekviena padaryta tos medžiagos kopija būtų saugiai saugoma tol, kol ji yra laikoma. Pagal orderį gauta medžiaga ir kiekviena bet kurios tos medžiagos kopija turi būti sunaikinta iš karto, kai nebėra jos saugojimą pateisinančių pagrindų (žr. 2016 m. TĮA 150 straipsnio 2 dalį, 150 straipsnio 5 dalį ir151 straipsnio 2 dalį). Verta pažymėti, kad panašios ankstesniu teisiniu pagrindu (RIPA 2000) numatytos apsaugos priemonės buvo numatytos laikantis Europos Žmogaus Teisių Teismo nustatytų reikalavimų dėl dalijimosi informacija, gauta masiniu būdu renkant duomenis kartu su užsienio valstybėmis arba tarptautinėmis organizacijomis (Europos Žmogaus Teisių Teismas (didžioji kolegija), *Big Brother Watch ir kt. prieš Jungtinę Karalystę*, (žr. 279 išnašą), 362 ir 399 punktai).

nepriklausomą ir teisminę tyrimo įgaliojimų pagal 2016 m. TĮA priežiūrą vykdo IPC. IPC prižiūri, kaip 2016 m. TĮA tyrimo įgaliojimais naudojasi teisėsaugos ir nacionalinės saugumo institucijos. Politinę priežiūrą garantuoja parlamento Žvalgybos tarnybos komitetas.

3.3.3.1. Priežiūra pagal DAA 4 dalį

(245) Žvalgybos tarnybų vykdomą asmens duomenų tvarkymą pagal 2018 m. DAA 4 dalį prižiūri informacijos komisaras ([441]).

(246) Bendrosios informacijos komisaro funkcijos, susijusios su žvalgybos tarnybų asmens duomenų tvarkymu pagal 2018 m. DAA 4 dalį, nustatytos 2018 m. DAA 13 priede. Jo užduotys, be kita ko, yra 2018 m. DAA 4 dalies stebėsena ir vykdymo užtikrinimas, visuomenės informavimo skatinimas, parlamento, vyriausybės ir kitų institucijų konsultavimas teisėkūros ir administracinių priemonių klausimais, duomenų valdytojų ir duomenų tvarkytojų informuotumo apie jų pareigas didinimas, duomenų subjektų informavimas apie duomenų subjektų teisių įgyvendinimą, tyrimų atlikimas ir pan.

(247) Pagal 2018 m. DAA 3 dalį komisaras turi įgaliojimus pranešti duomenų valdytojams apie įtariamą pažeidimą ir įteikti įspėjimus, kad tvarkant duomenis gali būti pažeistos taisyklės, taip pat įteikia papeikimus, kai pažeidimas patvirtinamas. Jeigu kurios nors akto nuostatos pažeidžiamos, jis taip pat gali teikti vykdymo pranešimus ir pranešimus dėl nuobaudų ([442]). Tačiau, kitaip, nei nustatyta kitose 2018 m. DAA dalyse, komisaras negali nacionalinei saugumo įstaigai įteikti vertinimo pranešimo ([443]).

(248) Be to, 2018 m. DAA 110 straipsnyje nustatyta tam tikrų komisaro įgaliojimų naudojimo išimtis, kai tai yra būtina siekiant užtikrinti nacionalinį saugumą. Tai yra komisaro įgaliojimai (bet kurios rūšies) įteikti pranešimus pagal DAA (informacijos, vertinimo, vykdymo pranešimai ir pranešimai apie nuobaudą), įgaliojimai atlikti patikrinimus laikantis tarptautinių pareigų, įgaliojimai patekti į patalpas ir atlikti patikrinimą, ir taisyklės dėl nusikalstamų veikų ([444]). Kaip paaiškinta (126) konstatuojamojoje dalyje, šios išimtys taikomos tik jei tai būtina ir proporcinga ir kiekvienu konkrečiu atveju.

(249) Informacijos komisaras ir Jungtinės Karalystės žvalgybos tarnybos pasirašė susitarimo memorandumą ([445]), kuriuo nustatoma bendradarbiavimo įvairiais klausimais sistema, įskaitant pranešimus apie duomenų saugumo pažeidimus ir duomenų subjektų skundų nagrinėjimą. Visų pirma jame nustatyta, kad informacijos komisaras, gavęs skundą, įvertins, ar bet kuri nacionalinio saugumo išimtis buvo taikoma tinkamai. Atsakymus į informacijos komisaro užklausas, pateiktas nagrinėjant pavienius skundus, atitinkama žvalgybos agentūra, naudodama tinkamus saugius kanalus, jei pateikiama slapta informacija, turi pateikti per 20 darbo dienų. Nuo 2018 m. balandžio mėn. iki šiol informacijos komisaras gavo 21 asmens skundą dėl žvalgybos tarnybų. Kiekvienas skundas buvo įvertintas, o duomenų subjektas buvo informuotas apie vertinimo rezultatą ([446]).

([441]) 2018 m. DAA 116 straipsnis.

([442]) Pagal 2018 m. DAA 13 priedo 2 dalį vykdymo pranešimai ir pranešimai apie nuobaudą gali būti įteikiami duomenų valdytojui arba duomenų tvarkytojui, jeigu jie yra susiję su 2018 m. DAA 2 skyriaus 4 dalies (duomenų tvarkymo principai), 2018 m. DAA 4 dalies nuostatos, kuria duomenų subjektui suteikiamos teisės, reikalavimo pranešti komisarui apie asmens duomenų saugumo pažeidimą pagal 2018 m. DAA 108 straipsnį ir asmens duomenų perdavimo į trečiąsias valstybes, Konvencijos nepasirašiusias valstybes ir tarptautinėms organizacijoms principų, išdėstytų 2018 m. DAA 109 straipsnyje, pažeidimais (daugiau informacijos apie vykdymo pranešimą ir pranešimą apie nuobaudą žr. (92) konstatuojamąją dalį).

([443]) Pagal 2018 m. DAA 147 straipsnio 6 dalį informacijos pareigūnas negali pateikti vertinimo pranešimo 2000 m. Informacijos laisvės akto 23 straipsnio 3 dalyje nurodytai įstaigai. Tai yra Saugumo tarnyba (MI5), Slaptoji žvalgybos tarnyba (MI6) ir Vyriausybės komunikacijų būstinė).

([444]) Nuostatos, kurioms gali būti taikomos išimtys: 108 straipsnis (pranešimas komisarui apie asmens duomenų saugumo pažeidimą), 119 straipsnis (patikrinimas pagal tarptautinius įsipareigojimus); 142–154 straipsniai ir 15 priedas (komisaro pranešimai ir įgaliojimai patekti į patalpas ir atlikti patikrinimą) ir 170–173 straipsniai (su asmens duomenimis susijusios nusikalstamos veikos). Taip pat, kalbant apie duomenų tvarkymą žvalgybos tarnybose, 13 priedo (kitos bendrosios Komisaro funkcijos) 1 punkto a ir g papunkčiai ir 2 punktas.

([445]) Informacijos komisaro biuro ir Jungtinės Karalystės žvalgybos bendruomenės susitarimo memorandumas, žr. 165 išnašą.

([446]) Septyniais iš tų atvejų informacijos komisaras rekomendavo skundo pateikėjui aiškintis su duomenų valdytoju (taip turi būti daroma, kai asmuo kreipiasi į informacijos komisarą, tačiau prieš tai turėjo kreiptis į duomenų valdytoją), vienu iš tų atvejų informacijos komisaras pateikė duomenų valdytojui bendrą rekomendaciją (tokia rekomendacija teikiama, kai paaiškėja, kad duomenų valdytojas teisės aktų nepažeidė, tačiau informacijos komisarui pateikto skundo būtų buvę galima išvengti, jeigu duomenų valdytojo praktika būtų patobulinta), o likusiais 13 atvejų duomenų valdytojas jokių veiksmų imtis neprivalėjo (tokia išvada daroma, kai asmens pateikti skundai patenka į 2018 m. Duomenų apsaugos akto taikymo sritį, nes jie teikiami dėl asmens informacijos tvarkymo, tačiau, remiantis duomenų valdytojo pateikta informacija, nustatoma, kad teisės aktai pažeisti nebuvo).

3.3.3.2. Tyrimo įgaliojimų naudojimo pagal 2016 m. TĮA priežiūra

(250) Pagal 2016 m. TĮA 8 dalį tyrimo įgaliojimų priežiūrą vykdo tyrimo įgaliojimų komisaras (IPC). IPC padeda kiti teismo komisarai, kurie kartu vadinami teismo komisarais ([447]). 2016 m. TĮA nustatytos teisminių institucijų narių nepriklausomumo apsaugos garantijos. Teismų komisarai privalo eiti aukštas teisėjo pareigas arba būti ėję tokias pareigas (t. y. turi dabar eiti arba būti ėję aukščiausiųjų teismų narių pareigas) ([448]) ir, kaip bet kuris teismų sistemos narys, jie turi būti nepriklausomi nuo vykdomosios valdžios ([449]). Pagal 2016 m. TĮA 227 straipsnį IPC ir teismo komisarus, kiek mano jų reikalinga, skiria Ministras Pirmininkas. Visi komisarai, nesvarbu, ar jie yra dabar dirbantys, ar buvę teismų sistemos nariai, gali būti skiriami tik remiantis trijų vyriausiųjų teisėjų – Anglijos ir Velso, Škotijos ir Šiaurės Airijos bei Lordo kanclerio – bendra rekomendacija ([450]). Valstybės sekretorius privalo aprūpinti IPC darbuotojais, patalpomis, įranga ir kitomis priemonėmis bei paslaugomis ([451]). Komisarai skiriami trejų metų kadencijai, kuri gali būti pratęsta ([452]). Kaip papildoma jų nepriklausomumo garantija, teismo komisarai iš pareigų gali būti pašalinti tik laikantis griežtų sąlygų, kuriomis nustatomos aukštos ribos: tai gali padaryti ministras pirmininkas konkrečiomis aplinkybėmis, kurių išsamus sąrašas pateiktas 2016 m. TĮA 228 straipsnio 5 dalyje (pvz., bankrotas arba laisvės atėmimo bausmė) arba jeigu abeji parlamento rūmai priėmė rezoliuciją, kuria patvirtinamas pašalinimas iš pareigų ([453]).

(251) IPC ir teismo komisarams pareigas padeda vykdyti Tyrimo įgaliojimų komisaro biuras (IPCO). IPCO personalą sudaro inspektorių grupė, biuro teisės ir techninių klausimų specialistai ir Patariamoji kolegija technologijų klausimais, kuri teikia ekspertų konsultacijas. Kaip ir atskirų teismo komisarų atveju, IPCO nepriklausomumas yra apsaugotas. IPCO yra Vidaus reikalų ministerijai pavaldi įstaiga, t. y. ji gauna finansavimą iš Vidaus reikalų ministerijos, tačiau savo funkcijas vykdo nepriklausomai ([454]).

(252) Pagrindinės teismų komisarų funkcijos išdėstytos 2016 m. TĮA 229 straipsnyje ([455]). Teismų komisarai visų pirma turi plačius įgaliojimus išankstinio patvirtinimo srityje, kurie yra tam tikra apsaugos priemonė, kuri Jungtinės Karalystės teisinėje sistemoje nustatyta 2016 m. TĮA. Teismo komisarai turi patvirtinti visus orderius, susijusius su tiksliniu duomenų perėmimu, įrangos perėmimu, masinių asmens duomenų rinkiniais, masiniu ryšių duomenų rinkimu ir pranešimais apie ryšių duomenų saugojimą ([456]). IPC taip pat visada turi išduoti išankstinį leidimą rinkti ryšių duomenis teisėsaugos tikslais ([457]). Jeigu komisaras atsisako patvirtinti orderį, valstybės sekretorius gali paduoti skundą Tyrimo įgaliojimų komisarui, kurio sprendimas yra galutinis.

([447]) Pagal 2016 m. TĮA 227 straipsnio 7 ir 8 dalis tyrimo įgaliojimų komisaras yra teismo komisaras, o tyrimo įgaliojimų komisaras ir kiti teismo komisarai kartu vadinami teismo komisarais. Dabar iš viso yra 15 teismo komisarų.

([448]) Pagal 2005 m. Konstitucinės reformos akto 3 dalies 60 straipsnio 2 dalį „aukštos teismo pareigos“ reiškia teisėjo pareigas kuriame nors iš toliau išvardytų teismų: i) Aukščiausiajame Teisme; ii) Anglijos ir Velso apeliaciniame teisme; iii) Anglijos ir Velso aukštajame teisme; iv) Sesijų teisme; v) Šiaurės Airijos apeliaciniame teisme; vi) Šiaurės Airijos aukštajame teisme arba tai gali būti teisės klausimus sprendžiantys lordai.

([449]) Teismų sistemos nepriklausomumas grindžiamas papročiais ir yra plačiai pripažįstamas nuo 1701 m. Susitarimo akto.

([450]) 2016 m. TĮA 227 straipsnio 3 dalis. Teismo komisarų kandidatūras taip pat teikia tyrimo įgaliojimų komisaras, 2016 m. TĮA 227 straipsnio 4 dalies e punktas.

([451]) 2016 m. TĮA 238 straipsnis.

([452]) 2016 m. TĮA 227 straipsnio 2 dalis.

([453]) Pašalinimo iš pareigų procesas yra tapatus kitų Jungtinės Karalystės teisėjų pašalinimui iš pareigų (žr., pvz., 1981 m. Aukštesniųjų teismų akto 11 straipsnio 3 dalį ir 2005 m. Konstitucinės reformos akto 33 straipsnį, pagal kurį taip pat reikalaujama, kad abeji parlamento rūmai po patvirtinimo procedūros priimtų rezoliuciją). Iki šiol nė vienas teismo komisaras nebuvo pašalintas iš pareigų.

([454]) Pavaldi įstaiga yra organizacija arba agentūra, gaunanti finansavimą iš vyriausybės, tačiau galinti veikti nepriklausomai (apibrėžtis ir daugiau informacijos apie pavaldžias įstaigas pateikiama Ministrų kabineto viešųjų įstaigų klasifikavimo vadove, kurį galima rasti šiuo adresu: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/519571/Classification-of-Public_Bodies-Guidance-for-Departments.pdf ir 2014–2015 m. sesijos Bendruomenių rūmų Viešojo administravimo atrankos komiteto pirmąją ataskaitą, galima rasti šiuo adresu: https://publications.parliament.uk/pa/cm201415/cmselect/cmpubadm/110/110.pdf).

([455]) Pagal 2016 m. TĮA 229 straipsnį teismo komisaras turi plačius priežiūros įgaliojimus, kurie taip pat apima žvalgybos agentūrų surinktų duomenų saugojimo ir atskleidimo priežiūrą.

([456]) Sprendimus dėl to, ar patvirtinti valstybės sekretoriaus sprendimą išduoti orderį, priima patys teismo komisarai. Jeigu komisaras atsisako patvirtinti orderį, valstybės sekretorius gali paduoti skundą Tyrimo įgaliojimų komisarui, kurio sprendimas yra galutinis.

([457]) IPC leidimo visada reikalaujama, kai ryšio duomenys gaunami teisėsaugos tikslais (2016 m. TĮA 60A straipsnis). Jeigu ryšio duomenys gaunami nacionalinio saugumo tikslais, leidimą gali išduoti IPC arba, kita vertus, paskirtasis atitinkamos valdžios institucijos vyresnysis pareigūnas (žr. 2016 m. TĮA 61 ir 61A straipsnius ir (203) konstatuojamąją dalį).

(253) JT specialusis pranešėjas teisės į privatumą klausimais ypač palankiai įvertino tai, kad 2016 m. TĮA sukurta teismo komisarų pareigybė, nes „ministrų kabinetas ir Tyrimo įgaliojimų komisaro biuras turi patenkinti vis daugiau su neskelbtina informacija arba intervencija susijusių prašymų vykdyti sekimo veiksmus“. Visų pirma jis pabrėžė, kad „šis teisminės peržiūros aspektas [atsižvelgiant į IPC vaidmenį], kurį padeda užtikrinti ištekliais geriau aprūpinta patyrusių inspektorių ir technologijų specialistų grupė, yra viena svarbiausių naujų apsaugos priemonių, nustatytų TĮA“, kuris pakeitė ankstesnę fragmentuotą priežiūros institucijų sistemą ir papildo parlamento Žvalgybos ir saugumo komiteto ir specializuoto Tyrimo įgaliojimų teismo vaidmenį“ ([458]).

(254) Be to, IPC turi įgaliojimus vykdyti *ex post* priežiūrą, be kita ko, atlikdamas auditą, tikrinimą ir tyrimą, naudodamasis tyrimo įgaliojimais pagal 2016 m. TĮA ([459]) ir tam tikrus kitus įgaliojimus ir funkcijas, numatytus atitinkamuose teisės aktuose ([460]). Tokios *ex post* priežiūros rezultatai įtraukiami į ataskaitą, kurią IPC turi kasmet parengti ir pateikti Ministrui Pirmininkui ([461]), taip pat paskelbti ir pateikti Parlamentui ([462]). Ataskaitoje pateikiami atitinkami statistiniai duomenys ir informacija apie tai, kaip žvalgybos agentūros ir teisėsaugos institucijos naudoja tyrimo įgaliojimus, taip pat apie tai, kaip naudojamos apsaugos priemonės, susijusios su daiktais, kuriems taikoma teisinė privilegija, konfidencialia žurnalistine informacija ir žurnalistų informacijos šaltiniais, informacija apie taikytas priemones ir operatyvinius tikslus, kurių siekiant buvo vykdomi masiniai orderiai. Galiausiai IPCO metinėje ataskaitoje nurodyta, kokiose srityse buvo pateikta rekomendacijų valdžios institucijoms ir kaip į jas atsižvelgta ([463]).

(255) Pagal 2016 m. TĮA 231 straipsnį, jei IPC sužino apie kokią nors svarbią klaidą, kurią valdžios institucijos padarė naudodamosi savo tyrimo įgaliojimais, jis turi informuoti atitinkamą asmenį, jei mano, kad klaida yra rimta ir kad visuomenės intereso labui tas asmuo turėtų būti informuotas ([464]). Visų pirma, 2016 m. TĮA 231 straipsnyje nurodyta, kad informuodamas asmenį apie klaidą IPC turi pateikti informaciją apie visas jo teises kreiptis į Tyrimų įgaliojimų teismą ir pateikti informaciją, kuri, komisaro nuomone, yra būtina norint pasinaudoti tomis teisėmis, ir atitinka viešąjį interesą atskleisti informaciją ([465]).

([458]) Specialiojo pranešėjo teisės į privatumą klausimais misijos pabaigos pareiškimas, padarytas įvykdžius misiją Jungtinėje Didžiosios Britanijos ir Šiaurės Airijos Karalystėje (žr. 281 išnašą).

([459]) 2016 m. TĮA 229 straipsnis. Teismų komisarų funkcijos tyrimų ir informacijos rinkimo įgaliojimų srityje išdėstytos 2016 m. TĮA 235 straipsnyje.

([460]) Tai yra pagal 2000 m. RIPA priimtos sekimo priemonės, funkcijų vykdymas pagal 1997 m. Policijos akto 3 dalį (leidimas imtis veiksmų dėl turto) ir Valstybės sekretoriaus funkcijų vykdymas pagal 1994 m. Žvalgybos tarnybų akto 5–7 straipsnius (orderiai dėl bevielio telegrafo perėmimo, patekimo į patalpas ir nuosavybės teisių apribojimas (2016 m. TĮA 229 straipsnis).

([461]) 2016 m. TĮA 230 straipsnis. IPC taip pat gali savo iniciatyva informuoti ministrą pirmininką bet kuriuo su jo funkcijomis susijusiu klausimu. IPC taip pat privalo informuoti ministrą pirmininką apie savo prašymą ir ministras pirmininkas gali liepti IPC peržiūrėti bet kurią žvalgybos tarnybų funkciją.

([462]) Kai kurios dalys gali būti neskelbiamos, jeigu tai prieštarautų nacionaliniam saugumui.

([463]) Pavyzdžiui, 2019 m. IPCO metinėje ataskaitoje (6.38 dalyje) paminėta, kad MI5 buvo rekomenduota pakeisti savo masinių asmens duomenų rinkinių saugojimo politiką, nes ji turėjo laikytis požiūrio, kuriuo būtų atsižvelgta į visų sričių turimų masinių asmens duomenų rinkinių ir kiekvieno turimo masinių asmens duomenų rinkinio saugojimo proporcingumą. 2018 m. pabaigoje IPCO nebuvo įsitikinęs dėl to, ar į šią rekomendaciją buvo atsižvelgta, ir 2019 m. ataskaitoje paaiškino, kad MI5 dabar rengia naują procesą, kad įvykdytų šį reikalavimą. 2019 m. metinėje ataskaitoje (8.22 dalis) taip pat paminėta, kad GHCQ buvo pateikta įvairių rekomendacijų, susijusių su atskaitomybės užtikrinimu proporcingumo srityje teikiant užklausas dėl masinių duomenų. Ataskaitoje patvirtinama, kad šioje srityje 2018 m. pabaigoje atlikta patobulinimų. 2019 m. metinė Tyrimo įgaliojimų komisaro biuro ataskaita, galima rasti šiuo adresu: https://www.ipco.org.uk/docs/IPC%20Annual%20Report%202019_Web%20Accessible%20version_final.pdf. Be to, po kiekvieno IPCO atlikto valdžios institucijos patikrinimo parengiama ataskaita, kuri pateikiama tai institucijai ir kurioje pateikiamos rekomendacijos, pagrįstos tuo patikrinimu. Nuo tada IPCO kiekvieną paskesnį patikrinimą pradeda peržiūrėdama ankstesnes rekomendacijas, ir naujoje patikrinimo ataskaitoje nurodo, ar į jas buvo atsižvelgta.

([464]) Klaida laikoma „rimta“, jeigu komisaras mano, kad dėl jos atitinkamam asmeniui buvo padaryta didelė žala arba skriauda (2016 m. TĮA 231 straipsnio 2 dalis). 2018 m. buvo pranešta apie 22 klaidas, iš kurių aštuonios buvo laikomos rimtomis klaidomis, apie kurias buvo informuotas atitinkamas asmuo. Žr. 2018 m. Tyrimo įgaliojimų komisaro biuro metinę ataskaitą, C priedas (žr. https://www.ipco.org.uk/docs/IPCO%20Annual%20Report%202018%20final.pdf). 2019 m. 14 klaidų buvo pripažintos rimtomis. Žr. 2019 m. Tyrimo įgaliojimų komisaro biuro metinę ataskaitą, C priedas žr. 463 išnašą.

([465]) 2016 m. TĮA 231 straipsnyje nustatyta, kad IPC, informuodamas asmenį apie klaidą, privalo pateikti tokią informaciją, kuri, komisaro manymu, yra būtina toms teisėms įgyvendinti, visų pirma atsižvelgdamas į tai, kokiu mastu informacijos atskleidimas prieštarautų viešajam interesui arba pakenktų sunkių nusikaltimų prevencijai arba nustatymui, Jungtinės Karalystės ekonominei gerovei arba nuolatiniam bet kurios žvalgybos tarnybos funkcijų vykdymui.

3.3.3.3. Parlamentinė žvalgybos tarnybų priežiūra

(256) Žvalgybos ir saugumo komiteto (ISC) vykdomos parlamentinės priežiūros teisinis pagrindas yra 2013 m. Teisingumo ir saugumo aktas (2013 m. TSA) ([466]). Jame nurodyta, kad ŽSK yra Jungtinės Karalystės parlamento komitetas. Nuo 2013 m. Žvalgybos ir saugumo komitetui buvo suteikti didesni įgaliojimai, įskaitant saugumo tarnybų operatyvinės veiklos priežiūrą. Pagal 2013 m. TSA 2 straipsnį Žvalgybos ir saugumo komitetui pavesta užduotis prižiūrėti nacionalinių saugumo agentūrų išlaidas, administravimą ir operacijas. 2013 m. TSA nurodyta, kad ŽSK gali vykdyti operatyvinių klausimų tyrimus, kai jie nėra susiję su vykdomomis operacijomis ([467]). Ministro pirmininko ir ŽSK susitarimo memorandume ([468]) išsamiai išdėstyta, į ką reikia atsižvelgti svarstant, ar veikla nėra kurios nors vykdomos operacijos dalis ([469]). Žvalgybos ir saugumo komiteto taip pat gali būti prašoma ištirti ministro pirmininko vykdomas operacijas ir jis gali peržiūrėti agentūrų savanoriškai pateiktą informaciją.

(257) Pagal 2013 m. TSA 1 priedą Žvalgybos ir saugumo komitetas gali bet kurio iš trijų žvalgybos tarnybų vadovų prašyti atskleisti informaciją. Agentūra privalo suteikti tokią informaciją, nebent valstybės sekretorius tai vetuoja ([470]). Remiantis Jungtinės Karalystės institucijų pateiktais paaiškinimais, Žvalgybos ir saugumo komitetui praktiškai nepateikiama labai mažai informacijos ([471]).

(258) ŽSK sudaro abiejų Parlamento rūmų nariai, kuriuos, pasikonsultavęs su opozicijos lyderiu, skiria ministras pirmininkas ([472]). ŽSK privalo kasmet pateikti Parlamentui ataskaitą apie savo funkcijų vykdymą ir teikti kitas, jo nuomone reikalingas, ataskaitas ([473]). Be to, Žvalgybos ir saugumo komitetas turi teisę kas tris mėnesius gauti operatyvinių tikslų sąrašą, kuris naudojamas tiriant gautą masinę medžiagą ([474]). Tyrimo įgaliojimų komisaro tyrimų, patikrinimų arba auditų kopijomis ministras pirmininkas dalijasi su Žvalgybos ir saugumo komitetu, kai ataskaitų klausimas yra svarbus teisės aktuose nustatytai komiteto kompetencijai ([475]). Galiausiai komitetas gali prašyti informacijos komisaro atlikti tyrimą ir komisaras privalo informuoti Žvalgybos ir saugumo komitetą apie sprendimą, ar atlikti tokį tyrimą ([476]).

(259) Žvalgybos ir saugumo komitetas prisidėjo rengiant 2016 m. TĮA, kuriuo remiantis padaryta įvairių pakeitimų, dabar įtrauktų į 2016 m. TĮA ([477]). Žvalgybos ir saugumo komitetas visų pirma rekomendavo sustiprinti privatumo apsaugos priemones nustatant įvairias privatumo apsaugos priemones, kurios taikomos patiems įvairiausiems

([466]) Kaip paaiškino Jungtinės Karalystės institucijos, TSA buvo praplėsta Žvalgybos ir saugumo komiteto kompetencija, kuria remiantis vykdoma ne tik trijų agentūrų priežiūra, ir sudarytos sąlygos vykdyti retrospektyvią agentūrų operatyvinės veiklos priežiūrą tiek, kiek ji susijusi su svarbiu nacionaliniu interesu.

([467]) 2013 m. TSA 2 straipsnis.

([468]) Ministro pirmininko ir ŽSK susitarimo memorandumas; galima rasti šiuo adresu: http://data.parliament.uk/DepositedPapers/Files/DEP2013-0415/AnnexA-JSBill-summaryofISCMoU.pdf.

([469]) Ministro pirmininko ir ŽSK susitarimo memorandumo 14 straipsnis, žr.468 išnašą.

([470]) Valstybės sekretorius gali vetuoti informacijos atskleidimą dviem pagrindais: informacija yra neskelbtina ir ji neturėtų būti atskleista Žvalgybos ir saugumo komitetui atsižvelgiant į nacionalinio saugumo interesus, arba informacija yra tokio pobūdžio, kad jeigu valstybės sekretoriaus būtų prašoma ją pateikti Bendruomenių Rūmų departamentų lygmens atskirajam komitetui, valstybės sekretoriaus nuomone (remiantis ne tik su nacionaliniu saugumu susijusiais pagrindais), derėtų to nedaryti (2013 m. TSA 1 priedo 4 straipsnio 2 dalis).

([471]) Diskusijoms dėl duomenų apsaugos tinkamumo skirto Jungtinės Karalystės aiškinamojo dokumento H skirsnis „Nacionalinis saugumas“, p. 43, žr. 31 išnašą.

([472]) 2013 m. TSA 1 straipsnis. Ministrai negali būti nariais. Žvalgybos ir saugumo komiteto narių kadencija sutampa su juos paskyrusio parlamento kadencija. Iš pareigų jie gali būti pašalinti rūmų, kurie juos paskyrė, rezoliucija arba kai jie netenka parlamento nario įgaliojimų arba tampa ministru. Narys taip pat gali atsistatydinti iš pareigų.

([473]) Komiteto ataskaitas ir pareiškimus galima rasti šiuo adresu: https://isc.independent.gov.uk/publications/. 2015 m. Žvalgybos ir saugumo komitetas paskelbė ataskaitą „Privatumas ir saugumas: šiuolaikinė ir skaidri teisinė sistema“ (žr. https://isc.independent.gov.uk/wp-content/uploads/2021/01/20150312_ISC_PSRptweb.pdf), kurioje jis nagrinėjo žvalgybos agentūrų naudojamų sekimo metodų teisinę sistemą, ir paskelbė įvairių rekomendacijų, paskui jos buvo išnagrinėtos ir įtrauktos į Tyrimo įgaliojimų akto bilį, paskui jis buvo priimtas įstatymo forma, t. y. 2016 m. TĮA. Vyriausybės atsakymą į privatumo ir saugumo ataskaitą galima rasti šiuo adresu: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20151208_Privacy_and_Security_Government_Response.pdf.

([474]) 2016 m. TĮA 142, 161 ir 183 straipsniai.

([475]) 2016 m. TĮA 234 straipsnis.

([476]) 2016 m. TĮA 236 straipsnis.

([477]) Parlamento žvalgybos ir saugumo komiteto ataskaita dėl Tyrimo įgaliojimų bilio projekto, galima rasti šiuo adresu: https://isc.independent.gov.uk/wp-content/uploads/2021/01/20160209_ISC_Rpt_IPBillweb.pdf

tyrimo įgaliojimams ([478]). Jis taip pat pasiūlė atlikti siūlomų pajėgumų, susijusių su įrangos perėmimu, masinių asmens duomenų rinkiniais ir ryšio duomenimis, pakeitimų ir paprašė atlikti kitus konkrečius pakeitimus, siekiant sustiprinti tyrimo įgaliojimų naudojimui taikomus apribojimus ir apsaugos priemones ([479]).

3.3.4. *Teisių gynimas*

(260) Vyriausybės prieigos nacionalinio saugumo tikslais srityje duomenų subjektai privalo turėti galimybę pareikšti ieškinį nepriklausomame ir nešališkame teisme, kad galėtų susipažinti su asmens duomenimis arba kad jiems būtų suteikta teisė ištaisyti arba ištrinti tokius duomenis ([480]). Tokia teisminė įstaiga visų pirma turi turėti įgaliojimus priimti privalomus sprendimus dėl žvalgybos tarnybos ([481]). Jungtinėje Karalystėje, kaip paaiškinta (261)–(271) konstatuojamosiose dalyse, duomenų subjektai gali pasinaudoti įvairiomis teisminėmis procedūromis, kad galėtų pritaikyti ir realizuoti tokias teisines teisių gynimo priemones.

3.3.4.1. Pagal DAA 4 dalį galimi teisių gynimo mechanizmai

(261) Pagal 2018 m. DAA 165 straipsnį duomenų subjektas turi teisę pateikti skundą informacijos komisarui, jeigu mano, kad, atsižvelgiant į jo asmens duomenis, buvo padarytas 2018 m. DAA 4 dalies pažeidimas. Informacijos komisaras turi įgaliojimus įvertinti, ar duomenų valdytojas ir duomenų tvarkytojas laikosi 2018 m. DAA, reikalauti, kad jie imtųsi būtinų veiksmų. Taip pat pažymėtina, kad pagal 2018 m. DAA 4 dalį asmenys turi teisę kreiptis į Aukštąjį teismą (Škotijoje – Sesijų teismą) su prašymu nurodyti duomenų valdytojui leisti pasinaudoti teise susipažinti su duomenimis ([482]), prieštarauti duomenų tvarkymui ([483]) ir ištaisyti arba ištrinti duomenis ([484]).

(262) Asmenys taip pat turi teisę reikalauti iš duomenų valdytojo arba duomenų tvarkytojo atlyginti žalą, patirtą dėl to, kad nebuvo laikomasi 2018 m. DAA 4 dalies reikalavimo ([485]). Žalą sudaro finansiniai nuostoliai ir su jais nesusijusi žala, pvz., stresas ([486]).

3.3.4.2. Pagal 2016 m. TĮA galimi teisių gynimo mechanizmai

(263) Asmenys nuo 2016 m. TĮA pažeidimų savo teises gali ginti specializuotame tyrimo įgaliojimų teisme.

(264) Specializuotas tyrimo įgaliojimų teismas įsteigtas 2000 m. RIPA ir jis yra nepriklausomas nuo vykdomosios valdžios ([487]). Pagal 2000 m. RIPA 65 straipsnį to specializuoto teismo narius penkerių metų kadencijai skiria Jos Didenybė. To specializuoto teismo narį iš pareigų pašalinti gali Jos Didenybė, remdamasi prašymu ([488]) iš abiejų parlamento rūmų ([489]).

---

([478]) Šios bendrosios su privatumu susijusios pareigos dabar yra išdėstytos 2016 m. TĮA 2 straipsnio 2 dalyje, kurioje nustatyta, kad valdžios institucija, veikdama pagal 2016 m. TĮA, privalo atsižvelgti į tai, ar tikslas, kurio siekiama orderiu, leidimu arba pranešimu, gali būti pasiektas mažiau intervencinėmis priemonėmis, ar informacijos gavimui pagal orderį, leidimą arba pranešimą taikytinas apsaugos lygis yra aukštesnis dėl konkretaus informacijos neskelbtino pobūdžio, viešojo intereso, susijusio su telekomunikacijų sistemų ir pašto paslaugų vientisumu ir saugumu, ir bet kuriais kitais viešojo intereso, susijusio su privatumo apsauga, aspektais.

([479]) Pavyzdžiui, gavus Žvalgybos ir saugumo komiteto prašymą, dienų skaičius, per kurį „skubus“ orderis pateikiamas tvirtinti teismo komisarui, sumažintas nuo penkių iki trijų darbo dienų, ir Žvalgybos ir saugumo komitetui suteikti įgaliojimai perduoti klausimus tirti tyrimo įgaliojimų komisarui.

([480]) *Schrems II*, 194 punktas.

([481]) *Schrems II*, 197 punktas.

([482]) 2018 m. DAA 94 straipsnio 11 dalis.

([483]) 2018 m. DAA 99 straipsnio 4 dalis.

([484]) 2018 m. DAA 100 straipsnio 1 dalis.

([485]) 2018 m. DAA 169 straipsnis, pagal kurį „asmuo, kuris patyrė žalą dėl duomenų apsaugos teisės aktų reikalavimų nesilaikymo” gali teikti ieškinį. Remiantis Jungtinės Karalystės institucijų pateikta informacija, praktiškai ieškinys arba skundas dėl žvalgybos tarnybų, tikėtina, bus teikiamas specializuotam Tyrimo įgaliojimų teismui, kuris turi plačią jurisdikciją, gali priteisti kompensaciją / žalos atlyginimą ir kuriame pareikšti ieškinį nieko nekainuoja.

([486]) 2018 m. DAA 169 straipsnio 5 dalis.

([487]) Pagal 2000 m. Tyrimo įgaliojimų reguliavimo akto 3 priedą nariai privalo turėti nurodytos teisminio darbo patirties ir juos turi būti galima paskirti naujai kadencijai.

([488]) Kreipimasis – tai parlamentui pateiktas prašymas, kuriuo siekiama informuoti monarchą apie parlamento nuomones konkrečiu klausimu.

([489]) 2000 m. Tyrimo įgaliojimų reguliavimo akto 3 priedo 1 dalies 5 punktas.

(265) Pagal 2000 m. RIPA 65 straipsnį specializuotas teismas yra tinkama teisminė įstaiga, galinti nagrinėti bet kokį asmens, nukentėjusio nuo veiksmų, nurodytų 2016 m. TĮA, 2000 m. RIPA, arba bet kurių kitų žvalgybos tarnybos veiksmų, skundą ([490]).

(266) Kad pagal 2000 m. RIPA 65 straipsnį pareikštų ieškinį specializuotame Tyrimo įgaliojimų teisme („procesinis veiksnumas“), asmuo turi būti įsitikinęs ([491]), kad žvalgybos tarnybos ėmėsi veiksmų dėl jo asmens, jo turto, bet kokių jo išsiųstų, jam atsiųstų arba adresuotų ryšių, arba jo naudojimosi pašto paslaugomis, telekomunikacijų paslauga arba telekomunikacijų sistema ([492]). Be to, reikalaujama, kad skundo pateikėjas manytų, kad veiksmai buvo atlikti „ginčytinomis aplinkybėmis“ ([493]) arba „juos atliko žvalgybos tarnybos arba tai buvo padaryta jų vardu“ ([494]). Šis „įsitikinimo“ standartas aiškinamas gana plačiai ([495]), todėl byla specializuotame teisme iškeliama laikantis žemų veiksnumo standartų.

(267) Jeigu specializuotas Tyrimų įgaliojimų teismas nagrinėja jam pateiktą skundą, jis turi pareigą ištirti, ar asmenys, kuriems skunde pateikiami kaltinimai, yra susiję su skundo dalyku, taip pat išsiaiškinti, kuri institucija įtariamai padarė pažeidimus ir ar buvo atlikti nurodyti veiksmai ([496]). Jeigu tas teismas nagrinėja kokią nors bylą, joje sprendimą jis privalo priimti remdamasis tais pačiais principais, kuriuos, atlikdamas teisminę peržiūrą, taikytų teismas ([497]). Be to, pagal 2016 m. TĮA išduotų orderių ir pranešimų adresatai ir bet kuris kitas Karalienei pavaldus pareigūnas, dirbantis policijos pajėgose, arba policijos tyrimų ir peržiūros komisaras turi pareigą atskleisti arba pateikti specializuotam teismui visus dokumentus ir informaciją, kurios jis gali prašyti siekdamas įgyvendinti savo jurisdikciją ([498]).

(268) Specializuotas tyrimo įgaliojimų teismas privalo informuoti skundo pateikėją, ar buvo priimtas jam palankus sprendimas ([499]). Pagal 2000 m. RIPA 67 straipsnio 6 ir 7 dalis specializuotas teismas turi įgaliojimus priimti laikinąsias nutartis ir priteisti bet kurią tokią kompensaciją arba priimti kitą nutartį, kuri, jo manymu, yra tinkama. Tai gali būti nutartis, kuria panaikinamas arba anuliuojamas bet kuris orderis arba leidimas, ir nutartis, kuria

([490]) 2000 m. RIPA 65 straipsnio 5 dalis.

([491]) Dėl „įsitikinimo“ patikrinimo žr. bylą *Human Rights Watch prieš Secretary of State* [2016] UKIPTrib15_165-CH, 41 punktas. Šiuo atveju specializuotas Tyrimo įgaliojimų teismas, remdamasis Europos Žmogaus Teisių Teismo praktika, nusprendė, kad tinkamas patikrinimas yra susijęs su tuo, ar, atsižvelgiant į nustatytą įsitikinimą, kad bet kurį veiksmą, kuriam taikoma 2000 m. RIPA 68 straipsnio 5 dalis, atliko žvalgybos tarnybos arba tai buvo padaryta jų vardu, esama pagrindo tokiam įsitikinimui, todėl asmuo gali teigti tapęs auka vien dėl slaptų priemonių arba teisės aktų, kuriais leidžiama taikyti slaptas priemones, egzistavimo ir tik tuo atveju, jei sugeba įrodyti, kad tokios priemonės gali būti taikomos atsižvelgiant būtent į jo padėtį.

([492]) 2000 m. RIPA 65 straipsnio 4 dalies a punktas.

([493]) Tokios aplinkybės – tai valdžios institucijų veiksmai pagal įgaliojimus (pvz., pagal orderį, leidimą ir (arba) pranešimą dėl pranešimų perėmimo ir pan.) arba aplinkybės (nepriklausomai nuo to, ar įgaliojimas yra, ar jo nėra), kuriomis taip elgtis nebūtų buvę tinkama neturint įgaliojimo arba bent neapsvarsčius, ar tokio įgaliojimo nereikėtų gauti. Teismo komisaro leisti veiksmai laikomi atliktais ginčytinomis aplinkybėmis (2000 m. RIPA 65 straipsnio 7ZA dalis), o kiti veiksmai, kurie atliekami turint teisėjo pareigas einančio asmens leidimą, laikomi atliktais negинčytinomis aplinkybėmis (2000 m. RIPA 65 straipsnio 7 ir 8 dalys).

([494]) Remiantis Jungtinės Karalystės institucijų pateikta informacija, žemesnioji riba skundui pateikti reiškia, kad specializuotam teismui nėra neįprasta atlikti tyrimo ir nustatyti, kad valdžios institucija skundo faktiškai nenagrinėjo. Naujausioje specializuoto Tyrimų įgaliojimų teismo statistinių duomenų ataskaitoje nustatyta, kad 2016 m. specializuotas teismas gavo 209 skundus, iš kurių 52 proc. pripažinti nepagrįstais, o 25 proc. pripažinti „neišspręstais“. Jungtinės Karalystės institucijos paaiškino, kad tai reiškia, jog nebuvo vykdomi slapti veiksmai / įgaliojimai, susiję su pareiškėju, arba kad buvo naudojami slapti metodai ir specializuotas teismas nusprendė, kad veikla buvo teisėta. Be to, 11 proc. skundų buvo atmesti, nepateko į specializuoto teismo jurisdikciją, buvo atsiimti arba pripažinti nepagrįstais, 5 proc. buvo pateikti pavėluotai, o 7 proc. skundų išnagrinėti pareiškėjų naudai. 2016 m. Tyrimo įgaliojimų komisaro biuro statistinių duomenų ataskaita, galima rasti šiuo adresu: https://www.ipt-uk.com/docs/IPT%20Statisical%20Report%202016.pdf.

([495]) Žr. sprendimą byloje *Human Rights Watch prieš Secretary of State* [2016] UKIPTrib15_165-CH. Šioje byloje Tyrimo įgaliojimų teismas, remdamasis su EŽTK susijusia teismų praktika, konstatavo, kad tinkamas kriterijus, kalbant apie įsitikinimą, kad koks nors žvalgybos tarnybos arba jos vardu vykdytas elgesys, patenkantis į 2000 m. Tyrimo įgaliojimų reguliavimo akto 68 straipsnio 5 dalies taikymo sritį, pasireiškė, yra tai, ar tokiam įsitikinimui yra pagrindo, įskaitant tai, kad asmuo gali tvirtinti, jog yra smurto auka vien dėl to, kad slaptos priemonės egzistuoja arba kad teisės aktuose yra leidžiama taikyti slaptas priemones, tik tada, jeigu gali įrodyti, kad dėl jo asmeninės padėties jis patiria riziką, kad tokios priemonės jam gali būti taikomos (žr. Sprendimo *Human Rights Watch prieš Secretary of State,* 41 punktą).

([496]) 2000 m. Tyrimo įgaliojimų reguliavimo akto 67 straipsnio 3 dalis.

([497]) 2000 m. Tyrimo įgaliojimų reguliavimo akto 67 straipsnio 2 dalis.

([498]) 2000 m. RIPA 68 straipsnio 6–7 dalys.

([499]) 2000 m. Tyrimo įgaliojimų reguliavimo akto 68 straipsnio 4 dalis.

reikalaujama sunaikinti bet kokius informacijos įrašus, gautus vykdant bet kokius orderiu, leidimu arba pranešimu suteiktus įgaliojimus, arba kuriuos dėl bet kurio asmens turi kuri nors kita valdžios institucija ([500]). Pagal 2000 m. RIPA 67A straipsnį specializuoto teismo sprendimą galima apskųsti, jeigu tai padaryti leidžia specializuotas teismas arba atitinkamas apeliacinis teismas.

(269) Galiausiai, reikia pažymėti, kad Tyrimo įgaliojimų teismo vaidmuo buvo aptartas nagrinėjant kelias bylas Europos žmogaus teisių teisme, pirmiausia byloje *Kennedy prieš Jungtinę Karalystę* ([501]) ir, neseniai, byloje *Big Brother Watch ir kt. prieš Jungtinę Karalystę* ([502]), kurioje teismas nusprendė, kad "Tyrimo įgaliojimų teismas užtikrino patikimas teisių gynimo priemones bet kuriam asmeniui, įtariančiam ‚kad jo ryšių duomenys buvo perimti žvalgybos tarnybų" ([503]).

3.3.4.3. Kiti galimi teisių gynimo mechanizmai

(270) Kaip paaiškinta (109)–(111) konstatuojamosiose dalyse, teisių gynimo priemonės pagal 1998 m. Žmogaus teisių aktą ir Europos Žmogaus Teisių Teisme ([504]) taip pat yra galimos tiek, kiek jos susijusios su nacionaliniu saugumu. 2000 m. RIPA 65 straipsnio 2 dalyje nustatyta, kad išimtinę jurisdikciją dėl visų pagal Žmogaus teisių aktą pareikštų reikalavimų, susijusių su žvalgybos tarnybomis, turi specializuotas tyrimo įgaliojimų teismas ([505]). Kaip pažymėjo Aukštasis teismas, tai reiškia, kad „klausimą, ar, atsižvelgiant į konkrečios bylos faktus, buvo pažeistas HRA, iš esmės gali išnagrinėti ir nuspręsti nepriklausomas specializuotas teismas, kuris gali susipažinti su visa atitinkama medžiaga, įskaitant slaptą informaciją. <...> Šiomis aplinkybėmis taip pat atsižvelgiame į tai, kad specializuoto teismo sprendimus galima apskųsti atitinkamam apeliaciniam teismui (Anglijoje ir Velse, t. y. apeliaciniam teismui) ir kad Aukščiausiasis Teismas neseniai nusprendė, kad specializuoto teismo sprendimus iš esmės galima peržiūrėti: žr. *R (Privacy International) prieš Investigatory Powers Tribunal* [2019] UKSC 22; [2019] 2 WLR 1219" ([506]).

(271) Iš to, kas išdėstyta, darytina išvada, kad tais atvejais, kai Jungtinės Karalystės teisėsaugos arba nacionalinio saugumo institucijos susipažįsta su asmens duomenimis, kuriems taikomas šis sprendimas, tokia prieiga reglamentuojama pagal įstatymus, kuriuose nustatytos sąlygos, kuriomis prieiga gali būti suteikta, ir kuriais užtikrinama, kad prieiga prie duomenų ir tolesnis jų naudojimas atitiktų tai, kas yra būtina ir proporcinga atsižvelgiant į siekiamą teisėsaugos arba nacionalinio saugumo tikslą. Be to, dėl tokios prieigos teisminė įstaiga, patvirtindama orderį arba įrodymų pateikimo orderį, dažniausiai išduoda išankstinį leidimą ir bet kuriuo atveju prieigai taikoma nepriklausoma priežiūra. Valdžios institucijoms susipažinus su duomenimis, jų tvarkymui, įskaitant tolesnį dalijimąsi ir perdavimą, taikomos 2018 m. DAA 3 dalyje nustatytos konkrečios duomenų apsaugos priemonės, atitinkančios Direktyvoje (ES) 2016/680 nustatytas priemones, jei duomenis tvarko teisėsaugos institucijos, ir 2018 m. DAA 4 dalis, jei duomenis tvarko žvalgybos agentūros. Galiausiai duomenų subjektai šioje srityje naudojasi veiksmingomis administracinėmis ir teisminėmis teisių gynimo teisėmis, įskaitant galimybę susipažinti su savo duomenimis arba ištaisyti arba ištrinti tokius duomenis.

(272) Atsižvelgdama į tokių sąlygų, apribojimų ir apsaugos priemonių svarbą šio sprendimo siekiamiems tikslams, Komisija atidžiai stebės, kaip taikomos ir aiškinamos Jungtinės Karalystės taisyklės, kuriomis nustatoma valdžios institucijų prieiga prie duomenų. Ji stebės atitinkamus teisėkūros, reguliavimo ir teismų praktikos pokyčius, taip pat

([500]) Šių įgaliojimų taikymo pavyzdys galėtų būti sprendimas byloje *Liberty & Others prieš the Security Service*, SIS, GCHQ, [2015] UKIP Trib 13_77-H_2. Specializuotas teismas priėmė dviem pareiškėjams palankų sprendimą, nes jų ryšiai vienu atveju buvo saugomi viršijant nustatytas ribas, o kitu atveju dėl to, kad nagrinėjimo procedūra vyko nesivadovaujant GCHQ nustatytomis vidaus taisyklėmis. Pirmuoju atveju teismas liepė žvalgybos tarnyboms sunaikinti ryšius, kurie buvo saugomi ilgiau, palyginti su atitinkamu terminu. Antruoju atveju nutartis dėl ryšių sunaikinimo nebuvo priimta, nes ryšiai nebuvo saugomi.

([501]) *Kennedy*, žr. 129 išnašą.

([502]) Europos Žmogaus Teisių Teismas (didžioji kolegija), *Big Brother Watch ir kt. prieš Jungtinę Karalystę* (žr. 268 išnašą), 413–415 punktai.

([503]) Europos Žmogaus Teisių Teismo sprendimo *Big Brother Watch* 425 punktas.

([504]) Pavyzdžiui, kaip matyti iš neseniai priimto Europos Žmogaus Teisių Teismo didžiosios kolegijos sprendimo *Big Brother Watch ir kiti prieš Jungtinę Karalystę* (žr. 279 išnašą), tai leidžia tarptautiniam teismui vykdyti veiksmingą teisminę kontrolę, panašią į tą, kuri taikoma ES valstybėms narėms, dėl to, kaip valdžios institucijos laikosi pagrindinių teisių naudodamosi asmens duomenimis. Be to, Europos Žmogaus Teisių Teismo sprendimų vykdymą konkrečiai prižiūri Europos Taryba.

([505]) Byloje *Belhaj & others* [2017] UKSC 3 sprendimas dėl medžiagos, kuriai taikoma teisinė privilegija, perėmimo neteisėtumo buvo tiesiogiai pagrįstas EŽTK 8 straipsniu (žr. 11 punktą).

([506]) Aukštojo teisingumo teismo sprendimo *Liberty*, [2019] EWHC 2057 (Admin), 170 punktas.

ICO ir kitų priežiūros institucijų veiklą šioje srityje. Labai atidžiai bus stebima ir tai, kaip Jungtinė Karalystė vykdo atitinkamus Europos Žmogaus Teisių Teismo sprendimus, įskaitant priemones, nurodytas veiksmų planuose ir veiksmų ataskaitose, pateiktose Ministrų komitetui vykdant Teismo sprendimų laikymosi priežiūrą.

## 4. **IŠVADA**

(273) Komisija mano, kad Jungtinės Karalystės BDAR ir 2018 m. DAA užtikrinamas iš Europos Sąjungos perduodamų asmens duomenų apsaugos lygis, kuris iš esmės yra lygiavertis pagal Reglamentą (ES) 2016/679 garantuojamam duomenų apsaugos lygiui.

(274) Be to, Komisija mano, kad pagal Jungtinės Karalystės teisę numatytais priežiūros mechanizmais ir teisių gynimo galimybėmis, vertinant juos kaip visumą, sudaromos sąlygos praktiškai nustatyti pažeidimus ir už juos bausti ir duomenų subjektui suteikiama teisių gynimo priemonių, kad jis galėtų susipažinti su savo asmens duomenimis ir vėliau pasiekti, kad šie duomenys būtų ištaisyti arba ištrinti.

(275) Galiausiai, remdamasi turima informacija apie Jungtinės Karalystės teisinę tvarką, Komisija mano, kad bet koks asmenų, kurių asmens duomenis Jungtinės Karalystės valdžios institucijos perduoda iš Europos Sąjungos į Jungtinę Karalystę viešojo intereso tikslais, visų pirma įstatymų vykdymo ir nacionalinio saugumo tikslais, pagrindinių teisių ribojimai turi būti susiję tik su tuo, kas yra griežtai būtina siekiant atitinkamo teisėto tikslo, ir kad nuo tokių apribojimų galima gintis veiksmingomis teisinės apsaugos priemonėmis.

(276) Todėl, atsižvelgiant į šio sprendimo išvadas, reikėtų nuspręsti, kad Jungtinė Karalystė užtikrina tinkamą apsaugos lygį, kaip apibrėžta Reglamento (ES) 2016/679 45 straipsnyje ir išaiškinta atsižvelgiant į Europos Sąjungos pagrindinių teisių chartiją.

(277) Šios išvados yra pagrįstos atitinkama Jungtinės Karalystės vidaus tvarka ir jos tarptautiniais įsipareigojimais, visų pirma Europos žmogaus teisių konvencijos laikymusi ir priklausymu Europos Žmogaus Teisių Teismo jurisdikcijai. Todėl tokių tarptautinių įsipareigojimų paisymas yra ypač svarbus šio sprendimo vertinimo pagrindą sudarantis aspektas.

## 5. **SPRENDIMO POVEIKIS IR DUOMENŲ APSAUGOS INSTITUCIJŲ VEIKSMAI**

(278) Valstybės narės ir jų institucijos privalo imtis priemonių, kurios yra būtinos siekiant užtikrinti atitiktį Sąjungos institucijų aktams, nes preziumuojama, kad Sąjungos institucijų teisės aktai yra teisėti, todėl sukelia teisinių pasekmių, kol nėra pripažinti netekusiais galios, panaikinti patenkinus ieškinį dėl panaikinimo, paskelbti negaliojančiais išnagrinėjus prašymą priimti prejudicinį sprendimą arba neteisėtumu grindžiamą prieštaravimą.

(279) Todėl Komisijos sprendimas dėl tinkamumo, kurį ji priėmė pagal Reglamento (ES) 2016/679 45 straipsnio 3 dalį, yra privalomas visoms valstybių narių, kurioms jis skirtas, institucijoms, įskaitant šių valstybių narių nepriklausomas priežiūros institucijas. Visų pirma taikant šį sprendimą, perdavimai iš Europos Sąjungos duomenų valdytojo arba duomenų tvarkytojo Jungtinėje Karalystėje esantiems duomenų valdytojams arba duomenų tvarkytojams gali vykti be jokio papildomo leidimo.

(280) Reikėtų priminti, kad pagal Reglamento (ES) 2016/679 58 straipsnio 5 dalį ir kaip išaiškinta Teisingumo Teismo sprendime *Schrems* ([507]), jeigu nacionalinė duomenų apsaugos institucija abejoja, įskaitant tuos atvejus, kai pateikiamas skundas, dėl Komisijos sprendimo dėl tinkamumo derėjimo su asmens pagrindinėmis teisėmis į privatumą ir duomenų apsaugą, nacionalinėje teisėje Komisijai turi būti numatyta teisinė teisių gynimo priemonė, kad ji šiuos prieštaravimus galėtų pareikšti nacionaliniame teisme, kuriam gali prireikti pateikti Teisingumo Teismui prašymą priimti prejudicinį sprendimą ([508]).

([507]) Sprendimo *Schrems* 65 punktas.

([508]) Sprendimo *Schrems* 65 punktas. „Šiuo atžvilgiu nacionalinis teisės aktų leidėjas turi numatyti teisių gynimo priemones, leidžiančias atitinkamai nacionalinei priežiūros institucijai remtis nacionaliniuose teismuose kaltinimais, kurie, jos nuomone, yra pagrįsti, tam, kad šie teismai, vertindami Komisijos sprendimo galiojimą, pateiktų prašymą priimti prejudicinį sprendimą, jei, kaip ir priežiūros institucija, turėtų abejonių dėl šio sprendimo galiojimo.“

## 6. **ŠIO SPRENDIMO STEBĖSENA, GALIOJIMO SUSTABDYMAS, PANAIKINIMAS ARBA PAKEITIMAS**

(281) Pagal Reglamento (ES) 2016/679 45 straipsnio 4 dalį Komisija privalo nuolat stebėti atitinkamus pokyčius Jungtinėje Karalystėje po to, kai bus priimtas šis sprendimas, siekdama įvertinti, ar ji vis dar užtikrina iš esmės lygiavertį apsaugos lygį. Tokia stebėsena yra ypač svarbi šiuo atveju, nes Jungtinė Karalystė administruos, taikys ir užtikrins naują duomenų apsaugos režimą, kuriam nebetaikoma Europos Sąjungos teisė ir kuris gali būti keičiamas. Šiuo atžvilgiu ypač bus stebima, kaip Jungtinė Karalystė praktiškai laikysis taisyklių dėl asmens duomenų perdavimo trečiosioms šalims, ir tai, kokį poveikį tai gali turėti pagal šį sprendimą perduodamų duomenų apsaugos lygiui; užtikrinant veiksmingą asmens teisių įgyvendinimą, įskaitant visus atitinkamus teisės aktų ir praktikos pokyčius, susijusius su išimtimis dėl tokių teisių taikymo išimtimis ar apribojimais (visų pirma su išimtimi dėl veiksmingos imigracijos kontrolės); Ir kaip laikomasi apribojimų ir apsaugos priemonių, taikomų valdžios institucijų prieigai. Be kita ko, Komisija stebės teismų praktikos raidą ir informacijos komisaro bei kitų nepriklausomų įstaigų vykdomą priežiūrą.

(282) Siekiant palengvinti šią stebėseną Jungtinės Karalystės institucijos turėtų nedelsdamos informuoti Komisiją apie bet kokius materialinius Jungtinės Karalystės teisinės tvarkos pokyčius, kurie daro poveikį pagal šį sprendimą reglamentuojamai teisinei sistemai, taip pat apie bet kokius praktikos, susijusios su šiame sprendime vertinamų asmens duomenų tvarkymu, pokyčius, tiek kiek tai susiję su duomenų valdytojų ir tvarkytojų pagal Jungtinės Karalystės BDAR vykdomu asmens duomenų tvarkymu, tiek taikant apribojimus ir apsaugos priemones, galiojančias valdžios institucijoms prieinant prie asmens duomenų. Be kita ko, turėtų būti pranešama ir apie pokyčius, susijusius su (281)konstatuojamojoje dalyje nurodytais elementais..

(283) Taip pat pažymėtina, jog tam, kad Komisija galėtų veiksmingai vykdyti stebėsenos funkciją, valstybės narės turėtų Komisijai pranešti apie visus atitinkamus veiksmus, kurių ėmėsi nacionalinės duomenų apsaugos institucijos, visų pirma dėl ES duomenų subjektų užklausų ar skundų, susijusių su asmens duomenų perdavimu iš Sąjungos duomenų valdytojams ar tvarkytojams Jungtinėje Karalystėje. Komisijai taip pat reikėtų pranešti apie bet kokius požymius, kad Jungtinės Karalystės valdžios institucijų, atsakingų už nusikalstamų veikų prevenciją, tyrimą, atskleidimą ar persekiojimą už jas, arba atsakingų už nacionalinį saugumą, įskaitant bet kokias priežiūros įstaigas, veiksmais nėra užtikrinama reikiamo lygio apsauga.

(284) Jeigu iš turimos informacijos, ypač iš informacijos, surinktos vykdant stebėseną pagal šį sprendimą, arba iš informacijos, kurią pateikia Jungtinės Karalystės arba valstybių narių institucijos, paaiškėja, kad Jungtinėje Karalystėje užtikrinamas duomenų apsaugos lygis nebėra pakankamas, Komisija turėtų apie tai informuoti kompetentingas Jungtinės Karalystės institucijas ir paprašyti per nustatytą terminą (jis negali būti ilgesnis nei trys mėnesiai) imtis tinkamų priemonių. Prireikus, atsižvelgiant į svarstomo klausimo pobūdį ir (arba) priemones, kurių reikia imtis, šis terminas gali būti pratęstas nustatytam laikui. Pavyzdžiui, tokia procedūra būtų taikoma tais atvejais, kai tolesnis duomenų perdavimas, be kita ko, remiantis Valstybės sekretoriaus priimtomis naujomis tinkamumo taisyklėmis arba Jungtinės Karalystės sudarytais tarptautiniais susitarimais, nebebūtų vykdomas taikant apsaugos priemones, kuriomis užtikrinamas apsaugos tęstinumas, kaip apibrėžta Reglamento (ES) 2016/679 44 straipsnyje.

(285) Jeigu, pasibaigus tam konkrečiam terminui, Jungtinės Karalystės kompetentingos institucijos nesiima tos priemonės arba kitaip įtikinamai neįrodo, kad šis sprendimas toliau grindžiamas tinkamu apsaugos lygiu, Komisija inicijuos Reglamento (ES) 2016/679 93 straipsnio 2 dalyje nurodytą procedūrą, siekdama iš dalies arba visiškai sustabdyti šio sprendimo galiojimą arba jį panaikinti.

(286) Kitu atveju Komisija pradės šią procedūrą, siekdama iš dalies pakeisti šį sprendimą, visų pirma nustatydama, kad duomenų perdavimui taikomos papildomos sąlygos, arba apribodama išvados dėl tinkamumo aprėptį taip, kad į ją patektų tik toks duomenų perdavimas, kurį vykdant toliau užtikrinamas apsaugos tęstinumas.

(287) Remdamasi tinkamai pagrįstais imperatyviais skubos pagrindais, Komisija pasinaudos galimybe pagal Reglamento (ES) 2016/679 93 straipsnio 3 dalyje nustatytą procedūrą priimti nedelsiant taikytinus įgyvendinimo aktus, kuriais sprendimo galiojimas sustabdomas, sprendimas panaikinamas arba iš dalies pakeičiamas.

## 7. **ŠIO SPRENDIMO GALIOJIMO TRUKMĖ IR ATNAUJINIMAS**

(288) Komisija privalo atsižvelgti į tai, kad, pasibaigus Susitarime dėl išstojimo nustatytam pereinamajam laikotarpiui, ir iš karto, kai nebebus taikomas ES ir Jungtinės Karalystės prekybos ir bendradarbiavimo susitarimo straipsnis 782, Jungtinė Karalystė administruos, taikys ir užtikrins naują duomenų apsaugos režimą, palyginti su tuo, kuris galiojo tuo metu, kai Jungtinė Karalystė buvo saistoma ES teisės. Tai visų pirma gali būti susiję su šiame sprendime vertinamos duomenų apsaugos sistemos pakeitimais arba pokyčiais, taip pat su kitomis atitinkamomis tendencijomis.

(289) Todėl šiame sprendime tikslinga numatyti, kad sprendimas bus taikomas ketverius metus nuo įsigaliojimo.

(290) Visų pirma, jeigu iš informacijos, kuri bus surinkta vykdant stebėseną pagal šį sprendimą, paaiškės, kad nustatyti faktai dėl Jungtinėje Karalystėje užtikrinamo duomenų apsaugos lygio tinkamumo faktiniu ir teisiniu požiūriais tebegalioja, Komisija turėtų ne vėliau kaip likus šešiems mėnesiams iki šio sprendimo galiojimo pabaigos pradėti šio sprendimo keitimo procedūrą ir, visų pirma, laikino taikymo laikotarpį pratęsti dar ketveriems metams. Bet koks įgyvendinimo aktas, kuriuo iš dalies keičiamas šis sprendimas, turi būti priimtas laikantis Reglamento (ES) 2016/679 93 straipsnio 2 dalyje nurodytos procedūros.

## 8. **BAIGIAMOSIOS PASTABOS**

(291) Europos duomenų apsaugos valdyba paskelbė savo nuomonę ([509]), į kurią buvo atsižvelgta rengiant šį sprendimą.

(292) Šiame sprendime numatytos priemonės atitinka pagal Reglamento (ES) 2016/679 93 straipsnį įsteigto komiteto nuomonę,

PRIĖMĖ ŠĮ SPRENDIMĄ:

*1 straipsnis*

1. Pagal Reglamento (ES) 2016/679 45 straipsnį Jungtinė Karalystė užtikrina tinkamą asmens duomenų, pagal Reglamentą (ES) 2016/679 perduodamų iš Europos Sąjungos į Jungtinę Karalystę, apsaugos lygį.

2. Šis sprendimas netaikomas asmens duomenims, perduodamais Jungtinės Karalystės imigracijos kontrolės tikslais arba kitaip patenkančiais į tam tikrų duomenų subjektų teisių išimties taikymo sritį siekiant išlaikyti veiksmingą imigracijos kontrolę pagal 2018 m. Jungtinės Karalystės duomenų apsaugos akto 2 priedo 4 straipsnio 1 dalį.

*2 straipsnis*

Jei kompetentingos valstybių narių priežiūros institucijos, siekdamos apsaugoti asmenis tvarkant jų asmens duomenis, įgyvendina savo įgaliojimus pagal Reglamento (ES) 2016/679 58 straipsnį dėl duomenų perdavimo, kuris patenka į 1 straipsnyje nustatytą taikymo sritį, atitinkama valstybė narė turi nedelsdama apie tai informuoti Komisiją.

*3 straipsnis*

1. Komisija nuolat stebi teisinės sistemos, kuria grindžiamas šis sprendimas, taikymą, įskaitant sąlygas, kuriomis vykdomas tolesnis duomenų perdavimas, įgyvendinamos asmens teisės ir Jungtinės Karalystės valdžios institucijoms suteikiama prieiga prie duomenų, kurie buvo perduoti pagal šį sprendimą, siekdama įvertinti, ar Jungtinė Karalystė ir toliau užtikrina tinkamą 1 straipsnyje nurodytą apsaugos lygį.

2. Valstybės narės ir Komisija viena kitą turi informuoti apie atvejus, kai informacijos komisaras arba bet kokia kita kompetentinga Jungtinės Karalystės institucija neužtikrina, kad būtų laikomasi Asmeninės informacijos apsaugos įstatymo.

3. Valstybės narės ir Komisija viena kitą turi informuoti apie bet kokius požymius, kad Jungtinės Karalystės valdžios institucijų kišimasis į asmenų teisę į savo asmens duomenų apsaugą viršija tai, kas yra būtina, arba apie tai, kad nuo tokio kišimosi nėra jokios veiksmingos teisinės apsaugos.

4. Jeigu Komisija turi žinių, kad tinkamas apsaugos lygis nebeužtikrinamas, ji informuoja kompetentingas Jungtinės Karalystės institucijas ir gali sustabdyti šio sprendimo galiojimą, jį panaikinti arba iš dalies pakeisti.

([509]) Nuomonė 14/2021 dėl Europos Komisijos įgyvendinimo sprendimo pagal Reglamentą (ES) 2016/679 dėl tinkamos asmens duomenų apsaugos Jungtinėje Karalystėje projekto, kurią galima rasti adresu https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-142021-regarding-european-commission-draft_en.

5. Komisija taip pat gali sustabdyti šio sprendimo galiojimą, jį panaikinti arba iš dalies pakeisti, jei dėl nepakankamo Jungtinės Karalystės Vyriausybės bendradarbiavimo Komisija negali nustatyti, ar nepaneigiama 1 straipsnio 1 dalyje nurodyta išvada.

*4 straipsnis*

Šis sprendimas baigia galioti 2025 m. birželio 27 d., nebent jo galiojimas būtų pratęstas pagal Reglamento (ES) 2016/679 93 straipsnio 2 dalyje nurodytą procedūrą.

*5 straipsnis*

Šis sprendimas skirtas valstybėms narėms.

Priimta Briuselyje 2021 m. birželio 28 d.

*Komisijos vardu*
Didier REYNDERS
*Komisijos narys*