

KONKURENCIJOS TEISĖS UNIVERSALUMAS NAGRINĖJANT SU DUOMENŲ APSAUGOS PAŽEIDIM AIS SUSIJUSIUS NESĄŽININGOS KONKURENCIJOS ATVEJUS

Greta Petkutė

Mykolo Romerio universiteto Teisės mokyklos
Privatinės teisės institutas
Elektroninis paštas greta.petkute@mruni.eu

Pateikta 2024 m. kovo 31 d., parengta spaudai 2024 m. spalio 3 d.

DOI: 10.13165/JUR-24-31-2-12

Santrauka. Skaitmeninėje ekonomikoje duomenims užimant vieną pagrindinių kriterijų, galinčių lemti konkurencinį pranašumą, priežiūrą vykdančios institucijos susiduria su iššūkiais, kaip užtikrinti veiksmingą skirtingų teisės šakų saugomų gėrių apsaugą. Neseniai pradėta formuoti praktika rodo, kad tokius pačius arba savo esme panašius pažeidimus priežiūrą vykdančios institucijos vertina skirtingai, vienos jų linkusios konstatuoti, kad duomenų apsaugos pažeidimai per se reiškia ir antikonkurencinį ūkio subjektų elgesį, kitos konstatuoja pažeidimus privatumo ar vartotojų teisių apsaugos srityse. Susijungimų bylose Europos Komisija apskritai laikosi nuoseklios pozicijos, kad duomenų apsauga ir konkurencijos teisė yra dvi atskiros teisės sritys ir kiekviena yra reguliuojama skirtingų teisės aktų, kurių taikymo priežiūra priskirta skirtingoms institucijoms. Tokį skirtingą požiūrį lemia tai, kad nėra jokių universalių taisyklių. Kol kas nėra universalaus reguliavimo, skirto spręsti problemas, susijusias su duomenų apsaugos pažeidimais taip pažeidžiant sąžiningą konkurenciją. Nepaisant to, straipsnyje analizuojama, ar dabartinis teisinis reguliavimas yra pakankamas spręsti duomenų apsaugos ir konkurencijos teisės pažeidimus.

Reikšminiai žodžiai: duomenys; duomenų apsauga; nesąžininga konkurencija; technologijų įmonės; vartotojų apsauga.

Įvadas

Pastarųjų dešimtmečių technologinė plėtra įmonėms leido išmokti rinkti, saugoti ir naudoti didelius kiekius duomenų. Duomenys tapo vienu iš konkurencinių parametrų, kuris leidžia vystyti naujus ir tobulinti esamus produktus ir paslaugas¹. Suprantant šiuolaikinę duomenų svarbą galima kelti prielaidą, kad jų reikšmė ir poveikis didės ateityje². Duomenys jau dabar yra traktuojami kaip valiuta, kuri turi savo vertę³, tačiau vertės nustatymui dar nėra vieningo mechanizmo. Analizuojant didžiųjų technologijų įmonių veikimo modelį tampa aišku, kad net ir atvejais, kai duomenų subjektas su internetine platforma nesidalija savo duomenimis, nereiškia, kad prie tokių duomenų tokio tipo ūkio subjektai neturi galimybės prieiti per trečiuosius asmenis, kurie sutikimus dėl prieigos prie duomenų yra davę. Pavyzdys gali būti *Google* nemokamos elektroninės pašto dėžutės *Gmail*. *Google* turėtų turėti prieigą tik prie to subjekto duomenų, kuris jais dalijasi ir kuris naudojami *Google* paslaugomis, tačiau platforma, gaudama prieigą prie tiesioginio vartotojo, gauna ir prieigą prie kitų susirašinėjime dalyvaujančių dalyvių informacijos⁴, ir apie tai šie asmenys nebūtinai žino.

Tačiau duomenų rinkimas ir jų telkimas vienose rankose nebūtinai reiškia tik neigiamas pasekmes duomenų subjektui. Kai kada duomenų turėjimas lemia, kad trečiosios šalis, turėdamos tam tikrus duomenis apie naudotojus ir jų patirtį naudojantis platforma, gali gerinti ateities vartotojų patirtį. Dažnai taip nutinka su slapukais, kai juos pasitelkus renkami duomenys. Tai nulemta tikslo gerinti vartotojų patirtį naudojantis platforma ir tokiomis atvejais neturėtų nukentėti nei sąžininga konkurencija, nei duomenų subjektai. Tačiau vertinant ir matant, kad technologijų plėtra ir galimybės rinkti bei naudoti duomenis versle greičiausiai nesumažės, o kaip tik priešingai – didės, tikslinga kelti klausimus, koks reguliavimas turėtų būti pakankamas siekiant užtikrinti pakankamą konkurenciją ir duomenų apsaugą, iš to kylantį privatumą, taip pat ar dabartinis reguliavimas yra tinkamas norint suvaldyti šią riziką⁵. Straipsnyje atskleidžiama, kad vyrauja keli požiūriai į tai, kuri teisės šaka turėtų spręsti problemas tais atvejais, kai susiduriama su galimu sąžiningos konkurencijos pažeidimu dėl duomenų rinkimo pažeidžiant duomenų apsaugos teisinį reguliavimą. Tačiau diskusijų nemažėja, o 2023 m. Europos Sąjungos Teisingumo Teismas priėmė

- 1 Ben-Shahar Omri, „Data Pollution“, *The Journal of Legal Analysis* 11, 24 (2019): 110, <http://dx.doi.org/10.1093/jla/laz005>; Competition and Markets Authority, Information Commissioner’s Office, „Competition and data protection in digital markets: a joint statement between the CMA and the ICO“ (2021), 8, https://assets.publishing.service.gov.uk/media/60a3c893d3bf7f288aaa5c9b/Joint_CMA_ICO_Public_statement_-_final_V2_180521.pdf.
- 2 Jacques Crémer, Yves-Alexandre de Montjoye ir Heike Schweitzer, *Competition Policy for the digital era, Final Report* (European Commission, 2019), 2, <https://op.europa.eu/en/publication-detail/-/publication/21dc175c-7b76-11e9-9f05-01aa75ed71a1/language-en>.
- 3 Omri, *op. cit.*, 105.
- 4 *Ibid.*, 115–116.
- 5 Giuseppe Colangelo, „The Privacy-Antitrust Curse: Insights from GDPR Application in EU Competition Law“, *ICL White Paper* (2023): 3, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4599974.

prejudicinį sprendimą vadinamojoje *Facebook* byloje⁶. Tad šio straipsnio tikslas – išanalizuoti, ar dabartinio teisinio reguliavimo pakanka siekiant, kad technologijų įmonės, turėdamos technines galimybes prieiti prie skirtingų duomenų, neiškreiptų sąžiningos konkurencijos ir nepažeistų duomenų subjektų teisių. Tyrimo objektas – teisės į duomenų apsaugą ir sąžiningą konkurenciją įgyvendinimas skirtingų institucijų ir valstybių vertinimu. Užsienio literatūroje temos, susijusios su teise į duomenų apsaugą, privatumą ir konkurencijos teisę, taip pat šių objektų tarpusavio santykį, yra nagrinėjamos, tačiau Lietuvoje šiai temai nėra skiriama tiek dėmesio. Taigi šis mokslinis straipsnis yra naujas ir aktualus. Išsikeltam tikslui pasiekti pasitelkti tam tikri tyrimo metodai. Sisteminis metodas taikomas analizuojant galimas sąsajas tarp duomenų apsaugos ir konkurencijos teisės šakų. Šiuo ir lyginamuoju metodu sistemingai analizuojami esami požiūriai į asmens duomenų ir konkurencijos teisės santykį, kuris atskleidžiamas per mokslinę doktriną ir kompetentingų institucijų, taip pat teismų, priimtus dokumentus, kurie nagrinėjami pritaikant teisinių dokumentų analizės metodą. Loginis analitinis metodas pasitelktas norint išsakyti autorės poziciją, padaryti išvadas dėl asmens duomenų apsaugos ir konkurencijos teisės šakų galimos sąveikos. Mokslinės literatūros analizės metodas pritaikytas siekiant išanalizuoti ir palyginti skirtingas subjektų pozicijas, kai nagrinėjami iš esmės panašūs klausimai dėl teisės į duomenų apsaugą pažeidimų ir sąžiningos konkurencijos pažeidimų. Apibendrinimo metodas taikomas kiekvieno skyriaus pabaigoje ir formuluojant galutines straipsnio išvadas.

1. Duomenys ir jų svarba konkurenciniam pranašumui

Žvelgiant iš ekonominės perspektyvos duomenys, taip pat ir asmens, yra ypač svarbūs skaitmeninėje ekonomikoje. Nesvarbu, ar duomenys yra (i) individualizuoti, pavyzdžiui, tokie, kurie pagal Europos parlamento ir Tarybos reglamentą (ES) 2016/679, dar vadinamą Bendruoju duomenų apsaugos reglamentu⁷ (toliau – BDAR), suprantami kaip asmens duomenys ir kurie apibrėžiami kaip „bet kokia informacija apie fizinį asmenį, kurio tapatybę nustatyta arba kurio tapatybę galima nustatyti (duomenų subjektas); fizinis asmuo, kurio tapatybę galima nustatyti, yra asmuo, kurio tapatybę tiesiogiai arba netiesiogiai galima nustatyti, visų pirma pagal identifikatorių, kaip antai vardą ir pavardę, asmens identifikavimo numerį, buvimo vietos duomenis ir interneto identifikatorių arba pagal vieną ar kelis to fizinio asmens fizinės, fiziologinės, genetinės, psichinės, ekonominės, kultūrinės ar

6 „Europos Sąjungos Teisingumo Teismo 2023 m. liepos 4 d. sprendimas byloje Nr. C-252/21“, Info Curia Case-Law, žiūrėta 2024 m. kovo 15 d., <https://curia.europa.eu/juris/document/document.jsf?jsessionid=EE-1981CFCD9FE30F80218CD32C900432?text=&docid=276478&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=7676256>.

7 „2016 m. balandžio 27 d. Europos parlamento ir tarybos reglamentas (ES) 2016/679 dėl fizinį asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas)“, EUR-Lex, žiūrėta 2024 m. kovo 20 d., <https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A32016R0679>.

socialinės tapatybės požymius^{8c}; (ii) ar apibendrinti; (iii) ar duomenys nelaikytini asmens duomenimis pagal BDAR apibrėžimą, bet turintys panašių bruožų⁹, pavyzdžiui, naudotojo duomenys¹⁰, tokie kaip duomenys apie naudotojų pomėgius, veiklą internete. Arba kontekstiniai duomenys¹¹ apie svetainės turinį arba asmens buvimo vietą ir pan.; analitiniai duomenys¹² apie svetainę – kiek vartotojų matė svetainę, jos reklamas ar bet kokią kitą turinį¹³. Tokie duomenys turi vertę skaitmeninėje erdvėje veikiančioms įmonėms, nes jie padeda tobulinti kuriamus produktus ir net įgyti konkurencinį pranašumą. Be kita ko, įmonėms, kurių verslas pagrįstas skaitmenine reklama, itin svarbu gauti naujausią informaciją apie vartotojų elgesį, jų įpročius, pageidavimus¹⁴. Todėl reikšminga ne tik duomenų klasifikacija pagal jų turinį, tačiau ir šaltiniai, iš kurių tokie duomenys surenkami, nes ir nuo šaltinių gali priklausyti subjektų patiriami duomenų gavimo kaštai, duomenų tikslumas.

Manytina, kad tiksliausiais duomenimis galima laikyti gautus iš pirminių šaltinių, t. y. tokius, kuriuos verslas gauna dėl tiesioginės sąveikos su duomenų subjektu, pavyzdžiui, internetinė parduotuvė surinko duomenis apie jos svetainėje apsilankiusį ir ką nors įsigijusį vartotoją. O per trečiąją šalį gauti duomenys gali nebūti tokie tikslūs, kadangi jie gauti ne tiesiogiai sąveikaujant su vartotoju, o per kitą platformą, kuri turėjo sąveiką su vartotoju ir tuos duomenis surinko¹⁵. Vis dėlto toks skirstymas į duomenis, gautus iš pirminių šaltinių ir trečiųjų šalių, yra santykinis, ir ne visada galima pasakyti, kurie duomenys, ypač jeigu kalbėtume apie didžiųjų technologijų įmones, kurios dažnai valdo net ne vieną, o kelias bendroves ir vienos jų gali rinkti informaciją, o kitos ne, yra gauti iš pirminių, o kurie trečiųjų šaltinių.

Duomenų vertė taip pat didėja dėl skirtingų duomenų bazių kombinavimo, kurios leidžia gauti įžvalgas, kurių nepavyktų sužinoti duomenis laikant atsietai. Taigi surenkamų duomenų kaštai ir vertė, kurią gali generuoti surinkti duomenys, duomenų rinkėjus skatina galvoti, kaip juos išsaugoti ir panaudoti savo versle, o ne svarstyti, koks patogiausias būdas šiais duomenimis pasidalyti su kitais subjektais. Be kita ko, tam tikri įstatyminiai reikalavimai taip pat apriboja galimybes negavus duomenų subjekto sutikimo tokiais duomenimis dalytis¹⁶.

Šitokios duomenų ypatybės lemia, kad duomenis geriau turėti apibendrintus ir vienoje vietoje nei atskirai, tačiau didelių duomenų kaupimas vienoje rankose kelia kitas, konkurencijos, problemas¹⁷.

8 „2016 m. balandžio 27 d. Europos parlamento ir tarybos reglamentas (ES) 2016/679“, *supra note*, 7:4 str. 1 p.

9 Competition and Markets Authority, Information Commissioner's Office, *supra note*, 1:10.

10 Competition and Markets Authority, „Online platforms and digital advertising, Market study interim report, Appendix F the role of data in digital advertising“ (2019), 3, https://assets.publishing.service.gov.uk/media/5fe495438fa8f56af97b1e6c/Appendix_F_-_role_of_data_in_digital_advertising_v4_WEB.pdf.

11 *Ibid.*

12 *Ibid.*

13 Competition and Markets Authority, Information Commissioner's Office, *op. cit.*

14 *Ibid.*, 12.

15 *Ibid.*, 11.

16 „Bendrasis duomenų apsaugos reglamentas“, *supra note*, 7: preambulės 32 punktus.

17 Competition and Markets Authority, Information Commissioner's Office, *supra note*, 1: 12.

Atsižvelgiant į skirtingą duomenų vertingumą ir į jų kiekį vienoje rankose, ypač jei kalbėtume apie užsakomosios tikslinės reklamos paslaugas, prieiga prie duomenų tampa svarbiu parametru tiek vertinant patekimo į rinką galimybes¹⁸, tiek paties verslo galimybę padidinti užimamos rinkos dalis ir jas gebėti išlaikyti. Nepaisant to, kad duomenys yra svarbūs skaitmeninių rinkų dinamikai, sąžininga ir veiksminga konkurencija nepriklauso nuo to, koku būdu subjektai renka ir tvarko duomenis. Sąžiningai ir veiksmingai konkurencijai svarbu, kad subjektų tarpusavio konkurencijai būtų užtikrinamos vienodos sąlygos konkurencijai. Tais atvejais, kai konkurentai turi skirtingas prieigos galimybes prie skirtingos apimties ir turinio duomenų, neabejotinai gali trūkti veiksmingos konkurencijos¹⁹. Atitinkamai dėl to vartotojams bus siūlomas mažesnis paslaugų pasirinkimas, prastesnė kokybė, aukštesnės kainos. Pavyzdžiui, Jungtinės Karalystės konkurencijos priežiūrą atliekančios institucijos tyrimas nustatė, kad *Google* ir *Facebook* turi reikšmingą prieigą prie įvairių duomenų, palyginti su konkurentais. *Google* duomenis gauna bent iš 50 skirtingų teikiamų paslaugų, įskaitant, bet neapsiribojant paieškos varikliu ir e. paštu *Gmail*; be kita ko, renka duomenis iš mobiliųjų įrenginių, kuriuose yra įdiegta *Android* arba *Google* operacinė sistema; taip pat iš analitikai skirtų techninių sprendimų, kurie diegiami į trečiųjų šalių platformas ir programėles²⁰. *Facebook* duomenis renka iš trijų pagrindinių programėlių naudotojų – *Facebook*, *Instagram*, *WhatsApp*, be abejonės, kaip ir *Google*, taip pat iš trečiųjų šalių platformų, kuriose turi savo įskiepius.

Nors pirminio duomenų rinkimo išlaidos gali būti gana didelės, tačiau ribinės dalijimosi duomenimis sąnaudos gali būti gana mažos nedarant skirtumo tarp to, ar duomenys būtų kopijuojami ir perduodami ar jais būtų tiesiog dalijamasi. Be to, duomenys nepraranda savo vertės net ir kelis kartus juos persidalijus.

Kuo didesnis vieno verslo subjekto prieinamumas prie įvairių duomenų, tuo didesnė tikimybė, kad sąžininga konkurencinė aplinka gali būti iškreipta. Pavyzdžiui, įtaką nevienodai konkurencinei aplinkai gali daryti:

- verslo subjektų turima prieiga prie duomenų apie paspaudimus (angl. *click*) ant nuorodų į internetinius puslapius ir užklausas: paieškos varikliai renka duomenis, kurių pagrindu moko algoritmus tuos duomenis panaudoti, pavyzdžiui, kaupia tokius duomenis apie tai, ko vartotojas ieškojo, kokius paieškos rezultatus pasirinko, kiek laiko praleido konkrečiame puslapyje²¹ ir pan. Vadinasi, kuo daugiau tokios informacijos turi algoritmas, tuo jam lengviau suprasti vartotoją ir atitinkamai patiekti jo lūkesčius, labiausiai patenkinančius paieškos rezultatus²²;

18 Competition and Markets Authority, „Online platforms and digital advertising, Market study interim report“ (2019), 15, https://assets.publishing.service.gov.uk/media/5dfa0580ed915d0933009761/Interim_report.pdf.

19 Competition and Markets Authority, Information Commissioner's Office, *op. cit.*, 13.

20 Competition and Markets Authority, *op. cit.*, 15.

21 Competition and Markets Authority, „Online platforms and digital advertising, Market study interim report, Appendix I search quality and economies of scale“ (2019), 7, https://assets.publishing.service.gov.uk/media/5fe4957c8fa8f56aeff87c12/Appendix_I_-_search_quality_v.3_WEB_.pdf.

22 Zhicheng Dou, Ruihua Song, Xiaojie Yuan ir Ji-Rong Wen, „Are Click-through Data Adequate for Learning Web Search Rankings?“, iš *CIKM '08: Proceedings of the 17th ACM conference on Information and knowledge management* (CIKM: 2008), 73–82, <http://dx.doi.org/10.1145/1458082.1458095>.

- verslo subjektų turima prieiga prie vartotojų profiliavimo duomenų tikslinės reklamos tikslais. Tiek *Google*, tiek *Facebook* turi prieigas prie duomenų tarp tarpusavyje susijusių vartotojų. Atitinkamai šios didžiųjų technologijų įmonės turi galimybę rinkti ir kaupti duomenis, kuriuos pasitelkusios vėliau gali sukurti labai išsamius vartotojų profilius. Su šiomis įmonėmis konkuruojantys subjektai neabejotinai turi žymiai mažesnę prieigą prie tokių duomenų apie vartotojus, todėl atitinkamai ir ne tokiais išsamiais profilius, o tai lemia, kad konkurencija gali būti apribota;
- verslo subjektų turima prieiga prie tikslinės reklamos analitinių duomenų, dėl kurių galima stebėti savo vartotojų elgseną per įskiepius trečiųjų šalių platformose. Tokie įskiepiai neabejotinai leidžia geriau pažinti savo klientus, o tai lemia, kad geriau pažindami savo vartotojus tokie ūkio subjektai reklamos užsakovams galės pasiūlyti geresnes sąlygas nei tokių įmonių konkurentai.

Taigi įvairių duomenų rinkimas ir jų naudojimas praktiškai paskatino diskutuoti, ar dabartinio reguliavimo pakanka norint suvaldyti riziką ir užtikrinti sąžiningą konkurencingą aplinką. Vieni mano, kad tokia skaitmeninės ekonomikos dinamika gali kenkti duomenų apsaugai ir privatumui, todėl tikslinga užtikrinti glaudų konkurencijos priežiūrą ir duomenų apsaugos priežiūrą vykdančių institucijų tarpusavio bendradarbiavimą²³, suteikti atitinkamas priemones taikyti net ir tuos teisės aktus, kuriuose *expressis verbis* nenurodyta, jog šį taikyti gali ir kita institucija nei nurodyta pačiame akte. Be to, manytina, reikia nepamiršti ir vartotojų teisių apsaugos, kadangi dėl prieš tai minėtų dviejų teisės šakų specifikos neišvengiamai aktualios ir vartotojų teisės ir jų apsauga²⁴.

Kiti mano priešingai: kadangi sąžiningos konkurencijos taisyklėmis ir reguliavimu, skirtu apsaugoti duomenis ir privatumą, yra siekiama skirtingų tikslų ir tam panaudojamos skirtingos priemonės²⁵, tai šios dvi teisės šakos jokiais būdais negali sutapti.

1.1. Dabartinis reguliavimas

Svarstant, ar dabartinio reguliavimo pakanka siekiant apsaugoti sąžiningą konkurenciją ir galiausiai patį vartotoją, pirmiausia reikia analizuoti, ar apskritai egzistuoja problema renkant duomenis ir juos naudojant komerciniais tikslais. Bendriausia prasme, kol laikomasi įstatyminių reikalavimų, nėra draudžiama nei rinkti duomenis, ar jie būtų asmens duomenys, ar duomenys, nesusiję su asmens duomenimis, nei juos naudoti komercinėje veikloje ir iš to gauti pelną²⁶. Net pačių rizikų valdymui yra priimti teisės aktai ir priskirtos institucijos šių aktų vykdymo priežiūrai. Pavyzdžiui, asmens duomenų apsaugą reguliuoja

23 European Data Protection Supervisor, „Preliminary Opinion of the European Data Protection Supervisor, Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy“ (2014), žiūrėta 2024 m. kovo 22 d., https://www.edps.europa.eu/sites/default/files/publication/14-03-26_competition_law_big_data_en.pdf.

24 *Ibid.*, 26.

25 Federal Trade Commission, „Remarks of Commissioner Noah Joshua Phillips“ (2019), 5–10, https://www.ftc.gov/system/files/documents/public_statements/1546405/phillips_-_paris_forum_9-13-2019.pdf.

26 Competition and Markets Authority, Information Commissioner's Office, *supra note*, 1: 8.

BDAR ir nacionaliniai teisės aktai, pavyzdžiui, Lietuvoje asmens duomenų teisinės apsaugos įstatymas²⁷. Sąžiningai konkuruodami ūkio subjektai privalo laikytis Sutarties dėl Europos Sąjungos veikimo²⁸ reikalavimų ir valstybių narių nacionalinių teisės aktų reikalavimų²⁹. Tol, kol rinka nebuvo tokia dinamiška, kol technologijos nebuvo tokios pažangios ir pasi-
 telkus internetą veikiantys skaitmeniniai verslai, pavyzdžiui, *Google, Facebook, Apple* ir kt., negebėjo vienosė rankose sukaupti didelio kiekio duomenų ir juos panaudodami generuoti pelną, tol galima manyti, kad klasikinio teisinio reguliavimo pakako ir didelių svarstymų apie sinergiją tarp skirtingų teisės šakų apskritai net neprireikė. Tačiau kai paaiškėjo, kad reikšmingo kiekio duomenų turėjimas vienosė rankose gali reikšti ir rinkos galios turėjimą³⁰, tampa aktualus klausimas, ar dabartinio reguliavimo pakanka siekiant suvaldyti teisės į duomenų apsaugą pažeidimų riziką ir užkirsti kelią nesąžiningai konkurencijai.

2. Duomenų apsauga *versus* konkurencijos teisė

Neabejotinai išsūkiu tampa sinergijos paieška tarp duomenų apsaugos ir sąžiningos konkurencijos užtikrinimo. Apskritai kyla klausimas, ar reikia tokios sinergijos paieškos. Privatumas ir duomenų apsauga savaime nėra elementai, kurių pažeidimas *per se* galėtų nulemti ir konkurencijos teisės pažeidimą³¹, tačiau tai nereiškia, kad privatumas ir duomenų apsauga nėra svarbūs apskritai³², jei kalbama apie sąžiningą konkurenciją. Kai kuriais atvejais vartotojai bus linkę naudotis tomis platformomis, kurios teikia prioritetą privatumui ir duomenų apsaugai, pavyzdžiui, vartotojai bus linkę saugoti jautrius duomenis, pavyzdžiui, sveikatos, o tai lems, kad konkurencinėje kovoje nugalės tie ūkio subjektai, kurie tuo metu būtent ir padės apsaugoti vartotojų duomenis. Nepaisant to, kad duomenų subjektui turėtų būti svarbus duomenų saugumas, šių subjektų veiksmai gali būti priešingi, o tai lemia privatumo suvokimo ir apsaugos paradoksą³³. Toks reiškinys kaip privatumo paradoksas³⁴ leidžia daryti išvadą, kad privatumas yra vertinamas subjektyviai. Skirtingi

27 „Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas“, *Valstybės žinios*, 1996-07-03, Nr. 63-1479.

28 Sutarties dėl Europos Sąjungos veikimo 101 ir 102 str. draudžia sudaryti draudžiamus susitarimus ir piktnaudžiauti vyraujančia padėtimi.

29 Pavyzdžiui, Lietuvoje pagrindinis įstatymas, reguliuojantis sąžiningą konkurenciją, yra Lietuvos Respublikos konkurencijos įstatymas (*Valstybės žinios*, 1999-04-02, Nr. 30-856).

30 European Data Protection Supervisor, *supra note*, 23: 26.

31 Vokietijos konkurencijos priežiūrą vykdanči institucija 2019 m. prieš *Facebook*, kuri yra vyraujantis subjektas atitinkamoje rinkoje, pradėjo bylą ir norėjo parodyti, kad asmens duomenų apsaugos reikalavimų pažeidimas reiškia, kad socialinio tinklo veiksmai prilyginami piktnaudžiavimui vyraujančia padėtimi.

32 Federal Trade Commission, *supra note*, 25: 8–9.

33 Omri, *supra note*, 1: 12; Global Privacy Assembly, „Privacy and Data protection as factors in competition regulation: Surveying Competition Regulators to Improve Cross-Regulatory Collaboration“ (2021), 21–23, <https://globalprivacyassembly.org/wp-content/uploads/2021/10/Privacy-and-data-protection-as-factors-in-competition-regulation.pdf>.

34 Susan Athey, Christian Catalini ir Catherine Tucker, „The Digital Privacy Paradox: Small Money, Small Costs, Small Talk, National Bureau Of Economic Research“, *Working Paper 23488* (2017): 17, <http://www.nber.org/papers/w23488>.

virtotojai, vadovaudamiesi jau turima patirtimi ir norėdami patenkinti savo poreikius, vertina labai skirtingai jautrumą duomenų ir privatumo apsaugai³⁵, pavyzdžiui, tikėtina, kad norėdami naudotis socialiniais tinklais, virtotojai bus linkę labiau dalytis ir jų nesaugoti nei, tarkim, sveikatos duomenimis, kurie turėtų būti prieinami sveikatos priežiūros įstaigų darbuotojams. Atitinkamai atsiduriant tokiose dviprasmiškose situacijose, kai vienu atveju virtotojai itin kreipia dėmesį į duomenų apsaugą, o kitu į apsaugos svarbą gali net nesigilinti, yra sudėtinga priimti universalias taisykles, kurios leistų spręsti duomenų apsaugos ir sąžiningos konkurencijos užtikrinimo klausimus, todėl balanso tarp šių dviejų gėrių vis dar ieškoma. Apskritai tikslinga svarstyti, ar išplėstinas požiūris į tai, kad konkurencijos priežiūrą vykdančios institucijos gali ir yra kompetentingos konstatuoti, kad buvo padarytas pažeidimas, susijęs su duomenų apsauga, nekelia grėsmės, kad bus nukrypta į kraštutinumą, kai tokios institucijos, turėdamos tiek galių vienosė rankose, taptų vienintelėmis reguliuotojomis³⁶ ir formuojančiomis praktika. Skirtingų valstybių konkurencijos priežiūrą vykdančių institucijų praktika rodo, kad nagrinėjant tą patį klausimą (didelio kiekio duomenų turėjimą vienosė rankose), jį vertinant skirtingai, gaunami nevienodi sprendimai. Sprendimų pliuralizmas tik parodo, kad, norint išspręsti klausimą dėl duomenų apsaugos ir konkurencijos teisės sąveikos (ne)egzistavimo, būtinos dar gana ilgos diskusijos.

2.1.1. Teisės į duomenų apsaugą įgyvendinimo pažeidimas = konkurencijos teisės pažeidimas

Tyrimas prieš *Facebook*, kurį Vokietijoje 2019 m. pradėjo konkurencijos priežiūrą vykdančios institucijos, neabejotinai yra vienas ryškiausių pavyzdžių, leidžiančių iškelti teoriją, kad, vyraujančiam ūkio subjektui pažeidus asmens duomenų apsaugos reikalavimus, taip pat pagal konkurencijos teisės reikalavimus galima nustatyti ir konstatuoti ir piktnaudžiavimą vyraujančia padėtimi³⁷. Vokietijos konkurencijos priežiūrą vykdanči institucija atlikusi tyrimą nustatė, kad socialinių tinklų Vokietijos teritorijoje, skirtų privatiems vartotojams, rinkoje *Facebook* užima vyraujančią padėtį³⁸. Tai reiškia, kad tokiam subjektui yra keliama tam tikri elgesio reikalavimai siekiant, kad socialinis tinklas savo veiksmis neiškraipytų sąžiningos konkurencijos sąlygų. Visi virtotojai, norėdami registruotis ir turėti paskyrą minėtame socialiniame tinkle, privalėjo sutikti su *Facebook* taisyklėmis, kuriose vartotojas mainais už galimybę naudotis socialiniu tinklu *Facebook* suteikia teisę rinkti apie

35 Jeffrey Prince ir Scott Wallsten, „How Much is Privacy Worth Around the World and Across Platforms?“, iš *TPRC48: The 48th Research Conference on Communication, Information and Internet Policy* (2020): 12, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3528386.

36 Giuseppe Colangelo ir Mariateresa Maggolino, „Antitrust über alles. Whither competition law after Facebook?“, *World Competition Law and Economics Review* 42, 3 (2019): 18, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3362428.

37 „2019 m. vasario 15 d. Bundeskartellamt, Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing“, Bundeskartellamt, žiūrėta 2024 m. kovo 27 d., https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=2.

38 *Ibid.*, 5.

vartotoją duomenis ne tik *Facebook* paskyroje, bet ir iš trečiųjų šalių platformų, kuriose yra *Facebook* įskiepai. Atsižvelgiant į tai, kad *Facebook* iš esmės privačių vartotojų socialinių tinklų rinkoje yra nepakeičiamas jokių kitu socialiniu tinklu, vartotojų duotas sutikimas duomenims rinkti, pasak Vokietijos priežiūros institucijos, neatitiko sutikimo reikšmės, apibrėžiamos ir suteikiamos pagal BDAR. Todėl *Facebook*, pažeisdamas BDAR reikalavimus ir surinkdamas didelį kiekį vartotojų duomenų, piktnaudžiavo vyraujančia padėtimi. Institucija, priimdama sprendimą prieš *Facebook*, manė ir parodė, kad konkurencijos teisė yra pajėgi spręsti ir su duomenų apsaugos pažeidimais susijusius klausimus.

2.1.2. Teisės į duomenų apsaugą įgyvendinimo pažeidimas = vartotojų teisių pažeidimas

Italijos konkurencijos priežiūrą vykdanči institucija metais anksčiau nei Vokietijos konkurencijos priežiūrą vykdanči institucija atliko tyrimą prieš *Facebook*, kuriuo nustatė, kad vartotojai registruodamiesi į socialinį tinklą buvo klaidinami, kadangi registracijos metu jiems nebūdavo atskleidžiama informacija, jog surinkti duomenys bus panaudoti komerciniais tikslais. *Facebook* apskritai pabrėžia nemokamą socialinio tinklo turinį ir galimybę juo naudotis nemokamai, tačiau ne komercinius tikslus, kuriais grindžiamas visas *Facebook* kaip socialinio tinklo paslaugos teikimas. Italijos konkurencijos priežiūrą vykdančios institucijos nuomone, jei vartotojams tokia informacija būtų atskleista iki užsiregistruojant socialiniame tinkle, galbūt vartotojai priimtų kitokį sprendimą, t. y. nesiregistruotų. Be kita ko, buvo nustatyta, kad pateikiama informacija yra bendrojo pobūdžio, vartotojui nėra paaiškinami duomenų rinkimo tikslai ir kam jie bus panaudoti. Institucija taip pat nustatė, kad *Facebook* komerciniais tikslais renka duomenis apie registruotus vartotojus iš trečiųjų šalių ir su jomis dalijasi. Toks socialinio tinklo elgesys su vartotojais yra išnaudotojiškas, kadangi *Facebook* registracijos metu vartotoją priverčia duoti plačiausią sutikimą asmens duomenims rinkti ir vėliau juos panaudoti. O jeigu vartotojas nori atšaukti tokį sutikimą vėliau, tai susiduria su problemomis, kadangi tokio sutikimo atšaukimas vartotojui stipriai apriboja galimybes naudotis tiek socialiniu tinklu, tiek trečiųjų šalių „sutikimo“ pagrindu teikiamomis paslaugomis. Buvo nustatyta, kad, nepaisant to, kad vartotojai gali atšaukti savo sutikimą, vis dėlto jie negali tokio sutikimo išreikšti laisva valia ir norima apimti, todėl toks *Facebook* elgesys pažeidžia vartotojų teises³⁹. Taigi, priešingai nei Vokietijos konkurencijos priežiūrą vykdanči institucija, Italijos kompetentinga institucija iš principo labai panašų klausimą įvertino kitaip ir nekonstatavo, kad konkurencijos teisė turi visus reikiamus įrankius sykiu nustatyti ir duomenų apsaugos pažeidimą.

39 „Facebook fined 10 million Euros by the ICA for unfair commercial practices for using its subscribers' data for commercial purposes“, Autorità Garante della Concorrenza e del Mercato, žiūrėta 2024 m. kovo 24 d., <https://en.agcm.it/en/media/press-releases/2018/12/Facebook-fined-10-million-Euros-by-the-ICA-for-unfair-commercial-practices-for-using-its-subscribers%E2%80%99-data-for-commercial-purposes>.

2.1.3. Teisės į duomenų apsaugą įgyvendinimo pažeidimas = privatumo pažeidimas

Už duomenų apsaugą atsakinga kompetentinga Belgijos institucija 2015 m. nustatė, kad *Facebook*, naudodamasis įskiepiais ir slapukais, tvarko subjektų, neturinčių *Facebook* paskyros, asmens duomenis. Nurodoma, kad, subjektui apsilankius interneto svetainėse per *facebook.com* domeną, *Facebook* automatiškai įrašydavo slapuką į interneto naudotojo kietąjį diską ir rinkdavo informaciją. Slapuke buvo saugomi unikalūs interneto naudotojo naršyklės identifikacijos duomenys, kurių saugojimo terminas buvo net dveji metai. Priežiūrą vykdanči institucija konstatavo, kad tokiais veiksmais socialinis tinklas pažeidė nacionalinius teisės aktus, taip pat Belgijos privatumą reguliuojantį aktą, todėl įpareigojo nedelsiant nutraukti automatinį ilgalaikių ir unikalinių neregistruotų *Facebook* naudotojų slapukų, leidžiančių identifikuoti asmenis, naudojimą⁴⁰.

2.1.4. Teisės į duomenų apsaugą įgyvendinimas = konkurencijos teisės pažeidimas

Kanados konkurencijos priežiūrą vykdanči institucija nustatė tai, ką vėliau patvirtino ir teismai, kad Toronto nekilnojamo turto tarpininkų asociacijos elgesys, teisintas teisės į privatumą tinkamo įgyvendinimo užtikrinimu, prieštaravo konkurencijos teisės reikalavimams. Toronto nekilnojamo turto tarpininkų asociacija skelbimų svetainėje internete ribojo duomenų prieinamumą apie tuo metu pardavinėjamus turto vienetus ir istorinius duomenis apie jau parduotus objektus, pavyzdžiui, turto kainą. Nepaisant ribojimo internete, tokiais duomenimis nekilnojamo turto tarpininkai tarpusavyje ar su savo klientais galėjo dalytis kitokia forma, pavyzdžiui, siūsti informaciją elektroniniais laiškais ar faksu. Nekilnojamo turto tarpininkų asociacija taip pat nesidalijo tokių pardavimų duomenimis ir su savo nariais per tik jiems skirtą naujienų kanalą internetu ir taip apribojo galimybes kurti naujus analitinius produktus. Kanados priežiūros institucija konstatavo, kad tokiu elgesiu nekilnojamo turto tarpininkų asociacija ribojo naujų verslo modelių, galinčių konkuruoti su asociacija, tobulėjimą ir stiprėjimą rinkoje. O nekilnojamo turto tarpininkų asociacija tokį savo elgesį teisino privatumo apsaugos užtikrinimu pagal nacionalinius teisės aktus⁴¹. Tokie argumentai neįtikino nei priežiūros institucijos, nei vėliau teismų, todėl nekilnojamo turto tarpininkų asociacijos elgesys buvo pripažintas antikonkurenciniu.

40 „Nederlandstalige rechtbank van eerste aanleg Brussel, 2015/57/C“, Global Freedom of Expression Columbia University, žiūrėta 2024 m. kovo 24 d., <https://globalfreedomofexpression.columbia.edu/cases/belg-nederlandstalige-rechtbank-van-eerste-aanleg-brussel-201557c/>.

41 „Backgrounder: Abuse of dominance by the Toronto Real Estate Board“, Competition Bureau Canada, žiūrėta 2024 m. kovo 24 d., <https://www.canada.ca/en/competition-bureau/news/2018/08/backgrounder-abuse-of-dominance-by-the-toronto-real-estate-board.html>.

2.2. Europos Komisijos požiūris į asmens duomenų apsaugos ir konkurencijos teisės sinergiją

Europos Komisija (toliau – EK), priešingai nei aptartose pažeidimų bylose, susijungimų bylose laikosi pozicijos, kad nors konkurencijai duomenys ir jų turėjimas vienoje rankose gali turėti poveikį, tačiau labai aiškiai atskiria institucijų kompetencijas ir teisės aktų taikymą⁴². 2008 m. vykusiame *Google/DoubleClick*⁴³ susijungime EK konstatavo, kad duomenų turėjimas vienoje rankose yra mažai tikėtinas. Net jei nutiktų, kad duomenys staiga būtų sukonzentruoti vienoje rankose, menka tikimybė, kad naujasis subjektas įgytų tokį konkurencinį pranašumą, kurio negalėtų pasiekti rinkoje esantys konkurentai⁴⁴. Be kita ko, EK pažymėjo, kad jos sprendimas priimamas vadovaujantis konkurencijos taisyklėmis ir nedarant įtakos kitiems fundamentalius principus nustatantiems įstatymams, tarp jų ir duomenų apsaugai⁴⁵. Atitinkamai EK neižvelgė problemų šioje situacijoje, kad užkirstų kelią koncentracijai ar atliktų platesnę duomenų ir konkurencijos teisės sinergijos analizę. Žinoma, atkreipus dėmesį į tai, kuriuo metu buvo priimtas toks sprendimas, sprendimas nestebina, nes tada duomenų sutelkimas vienoje rankose nekėlė perdėto susirūpinimo.

2014 m. *Facebook/WhatsApp*⁴⁶ susijungimo byloje EK ir toliau plėtojo nuoseklią poziciją, kad konkurencijos ir asmens duomenų apsaugos teisės yra dvi atskiros sritys, kurių tarpusavyje nereikia painioti. Šioje byloje EK padarė išvadą, kad nepaisant to, jog šių įmonių susijungimas padidins *Facebook* duomenų kiekį apie *WhatsApp* vartotojus, kuriuos galės panaudoti tikslinei reklamai, tačiau internete ir po susijungimo bus daug vertingos informacijos, prie kurios prieigą tiek iki susijungimo, tiek po jo turės ne tik *Facebook*, bet ir jo konkurentai⁴⁷. Be to, EK pažymėjo, kad bet kokie klausimai, susiję su privatumu dėl duomenų koncentracijos vienoje rankose, turi būti sprendžiami taikant Europos Sąjungos asmens duomenų apsaugą užtikrinančius teisės aktus⁴⁸. Taip EK dar kartą patvirtino, kad šios dvi teisės šakos yra atskiros.

2016 m. vykęs *Microsoft/LinkedIn*⁴⁹ susijungimas neįnešė jokių pereinamųjų į EK poziciją dėl duomenų ir konkurencijos teisės atskirties aiškinimo. Atkreiptinas dėmesys į tai, kad leidimas susijungti buvo išduotas jau po to, kai buvo priimtas BDAR, kuriuo vadaudamasi EK nurodė, kad duomenų turėjimas vienoje rankose greičiausiai nekels jokių

42 Inge Graef, Damian Clifford ir Peggy Valcke, „Fairness and enforcement: bridging competition, data protection, and consumer law“, *International Data Privacy Law* 8, 3 (2018): 219–220, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3216198.

43 „2008 m. kovo 11 d. Google/DoubleClick COMP/M.4731“, European Commission, žiūrėta 2024 m. kovo 27 d., https://ec.europa.eu/competition/mergers/cases/decisions/m4731_20080311_20682_en.pdf.

44 *Ibid.*, 364 punktas.

45 *Ibid.*, 368 punktas.

46 „2014 m. spalio 03 d. Facebook/WhatsApp COMP/M.7217“, European Commission, žiūrėta 2024 m. kovo 27 d., https://ec.europa.eu/competition/mergers/cases/decisions/m7217_20141003_20310_3962132_EN.pdf.

47 *Ibid.*, 189 punktas.

48 Facebook/WhatsApp, *supra note*, 46: 164 punktas.

49 „2016 m. gruodžio 06 d. Microsoft/LinkedIn M.8124“, European Commission, žiūrėta 2024 m. kovo 27 d., https://ec.europa.eu/competition/mergers/cases/decisions/m8124_1349_5.pdf.

problemų, nes įsigaliojus BDAR duomenų subjektų apsauga yra sustiprinama⁵⁰. EK ir šiame sprendime pasinaudojo galimybe atskirti asmens duomenų apsaugą reguliuojančius teisės aktus nuo konkurencijos teisės ir padarė prielaidą, kad vykdomas dviejų verslo subjektų susijungimas nesukels neigiamų pasekmių konkurencijai⁵¹. EK nenagrinėjo to, kokią rinkos galią įgis ūkio subjektas po susijungimo ir kokias privatumą saugančias priemones taikys.

2018 m. *Apple/Shazam*⁵² susijungimo atveju EK išreiškė susirūpinimą, kuriame nurodė, kad nėra aišku, ar susijungęs subjektas galėtų sudaryti nepalankias konkurencines sąlygas konkurentams, jei tikslinei reklamai ir kampanijoms naudotų per susijungimą įgytus duomenis apie vartotojus⁵³. Tačiau nepaisant šio susirūpinimo, EK nurodė, kad visi klausimai, susiję su asmens duomenų apsauga ir privatumu, sprendžiami vadovaujantis asmens duomenų apsaugą ir privatumą reguliuojančiais teisės aktais⁵⁴.

2020 m. *Google/Fitbit*⁵⁵ susijungimas nuo suminėtų susijungimų skiriasi tuo, kad leidimas vykdyti susijungimą buvo išduotas tik po to, kai *Google* pasiūlė įsipareigojimus, kuriais techniškai atskyrė *Fitbit* vartotojų sveikatos duomenis nuo *Google* duomenų ir sutiko be aiškaus vartotojų sutikimo šių duomenų automatiškai nebendrinti su *Google* paskyromis ir įrenginiais, taip pat nerodyti tikslinės reklamos naudojantis iš *Fitbit* perimtais duomenimis. EK dar kartą priminė, kad duomenys turi būti tvarkomi naudojant tinkamas organizacines ir technines galimybes vadovaujantis BDAR reikalavimais⁵⁶.

Galiausiai, 2021 m. *Microsoft/Nuance*⁵⁷ ir 2022 m. *Meta/Kustomer*⁵⁸ įvykusiuose susijungimuose EK pakartojo, kad šalys asmens duomenų apsaugos reikalavimų privalo laikytis vadovaudamosi Europos Sąjungoje taikomais duomenų apsaugą užtikrinančių teisės aktų reikalavimais.

Nepaisant to, kad EK nei viename sprendime nepasisakė dėl to, kad ji būtų kompetentinga nagrinėti klausimus, susijusius su asmens duomenų apsauga, tačiau nei viename sprendimų ji ir nekonstatavo, kad to daryti negalėtų. Tiesiog konstatavo, kad klausimai, susiję su asmens duomenimis ir privatumu, sprendžiami tokius santykius reguliuojančių teisės aktų pagrindu.

50 „2016 m. gruodžio 06 d. *Microsoft/LinkedIn* M.8124“, *supra note*, 49:178 punktas.

51 *Ibid.*, 175–180 punktai.

52 „2018 m. rugsėjo 06 d. *Apple/Shazam* M.8788“, European Commission, žiūrėta 2024 m. kovo 27 d., https://ec.europa.eu/competition/mergers/cases/decisions/m8788_1279_3.pdf.

53 *Ibid.*, 221 punktas.

54 *Ibid.*, 314 punktas.

55 „2020 m. gruodžio 17 d. *Google/Fitbit* M.9660“, European Commission, žiūrėta 2024 m. kovo 27 d., https://ec.europa.eu/competition/mergers/cases1/202120/m9660_3314_3.pdf.

56 *Ibid.*, 410 punktas.

57 „2021 m. gruodžio 21 d. *Microsoft/Nuance*“, European Commission, 156–159 punktai, žiūrėta 2024 m. kovo 27 d., https://ec.europa.eu/competition/mergers/cases1/202231/M_10290_8431645_854_3.pdf.

58 „2022 m. sausio 27 d. *Meta/Kustomer*“, European Commission, 520–526 punktai, žiūrėta 2024 m. kovo 27 d., https://ec.europa.eu/competition/mergers/cases1/202242/M_10262_8559915_3054_3.pdf.

3. Skaitmeninių rinkų aktas – raktas į sėkmę?

Matant itin išsiskiriantį požiūrį į duomenų apsaugos ir konkurencijos teisės sinergiją, kai galimų pažeidimų tyrimuose norima vienai institucijai turėti pakankamai galios konstatuoti pažeidimą jos priežiūros srityje atsispiriant nuo pažeidimo duomenų apsaugai, ir priešingai, susijungimų atvejais – visišką konkurencijos priežiūrą vykdančios institucijos nenorą kištis į su duomenų reguliavimu susijusius klausimus, kyla klausimas, ar įmanoma sukurti universalias taisykles. Žvelgiant iš dabartinės perspektyvos, autorės nuomone, ateityje galbūt ir pavyks suformuluoti universalias taisykles, tačiau šiuo metu tai padaryti dar sudėtinga, nors užuomazgų tam jau yra.

Vienas tokių pavyzdžių – tai 2022 m. rugsėjo 14 d. Europos Parlamento ir Tarybos priimtas Skaitmeninių rinkų aktas⁵⁹ (toliau – SRA), kurio tikslas – „prisidėti prie tinkamo vidaus rinkos veikimo nustatant suderintas taisykles, kuriomis visoms įmonėms visoje Europos Sąjungoje užtikrinamos atviros konkurencijai ir sąžiningos skaitmeninio sektoriaus rinkos, kuriose veikia prieigos valdytojai, verslo klientų ir galutinių naudotojų naudai“⁶⁰. SRA yra nukreiptas prieš didelę rinkos galią turinčius subjektus⁶¹. Šiuo metu EK yra išskyrusi šešias įmones, kurioms taikomas SRA: *Alphabet, Amazon, Apple, ByteDance, Meta, Microsoft*⁶². SRA 5 straipsnio 2 dalyje iš esmės aprašyti veiksmai, kurių prieigos valdytojai negali atlikti. Tai aprašytos institucijų praktikos, kuriose nacionalinės priežiūros institucijos nustatinėjo, kokie su duomenų rinkimu, valdymu ir tvarkymu susiję pažeidimai leidžia konstatuoti teisės aktų reikalavimų neatitinkantį subjektų elgesį, atspindys.

Manytina, kad nors SRA ir sveikintina iniciatyva, tačiau ji nesprendžia problemų, susijusių su duomenų apsaugos pažeidimais ir konkurencijos teisės sąveika. Pirmiausia, šis teisės aktas skirtas kelioms didžiosioms didžiųjų technologijų įmonėms. Ar tai reiškia, kad nesąžiningai negali elgtis mažas rinkos žaidėjas, pavyzdžiui, skaitmeninėje rinkoje kaip atitinkamoje rinkoje, tačiau rinkos galią turintis siauresnėje atitinkamoje rinkoje. Tokiu atveju, teigtina, gali kilti problemų dėl to, kad priežiūros institucijos nesiims vertinti mažesnių žaidėjų veiksmų, nes jiems netaikomas SRA, o ir savo institucinių resursų nenorės skirti tokiam tyrimui. Antra, SRA 1 straipsnio 6 dalyje nurodyta, kad šis reglamentas nedaro poveikio konkurencijos taisyklių taikymui, tai reiškia, kad konkurencijos teisė ir šis reglamentas tarsi turėtų būti taikomi atskirai. Tačiau atsiranda priešara preambulės 10 punkte, kuriame nurodoma, kad šiuo reglamentu siekiama papildyti konkurencijos teisės vykdymo užtikrinimo priemones. Be to, preambulės 11 punkte nurodyta, kad SRA nedaro įtakos ir BDAR taikymui. Taigi, matyti, kad teisės aktas iš principo priimtas ir taikytinas

59 „2022 m. rugsėjo 14 d. Europos Parlamento ir Tarybos reglamentas (ES) 2022/1925 dėl atvirų konkurencijai ir sąžiningų skaitmeninio sektoriaus rinkų, kuriuo iš dalies keičiamos direktyvos (ES) 2019/1937 ir (ES) 2020/1828 (Skaitmeninių rinkų aktas)“, EUR-Lex, žiūrėta 2024 m. kovo 27 d., <https://eur-lex.europa.eu/legal-content/LI/TXT/PDF/?uri=CELEX:32022R1925>.

60 *Ibid.*, 1 str. 1 p.

61 *Ibid.*, 3 str. 1–2 d.

62 „Digital Markets Act“, European Council of the European Union, žiūrėta 2024 m. kovo 27 d., <https://www.consilium.europa.eu/en/policies/digital-markets-act/>.

tik dėl kelių pasaulinių rinkos subjektų, dėl kurių jau anksčiau buvo formuota institucijų praktika, kurios pagrindu, tikėtina, ir atsirado SRA, kuris, sprendžiant iš jo struktūros ir taikymo srities, nėra universalus taisyklių rinkinys, sujungiantis konkurencijos teisę ir duomenų apsaugą.

Taigi, kad ir kaip norėtusi, jog būtų priimtas universalus teisės aktas, apimantis integruotą požiūrį į duomenų apsaugos ir konkurencijos teisės sąveiką, tačiau tokio teisės akto dar nėra ir apskritai vis išlieka iškeltas klausimas, ar jis reikalingas, jeigu institucijos, spręsdamos labai panašius klausimus, taiko skirtingus požiūrius ir teisės aktus. Iš vienos pusės, vieningo teisės akto reikia, kadangi ūkio subjektams būtų suteikiamas tikrumas dėl jų elgesio teisėtumo, iš kitos pusės, tokį teisės aktą sunku sukurti, kai taip greitai keičiasi rinkos sąlygos.

Išvados

1. Skaitmeninėje ekonomikoje duomenys yra valiuta ir, nepaisant duomenų piniginės išraiškos, kuri skaitmeniniams verslams neša pelną, duomenys taip pat gali būti nekaininis parametras, lemiantis konkurencinį pranašumą. Didelė duomenų koncentracija viename rankose, ypač jei jie surinkti iš pirminių šaltinių, gali lemti sąžiningos konkurencijos iškreipimą. Tiesa, sąžiningos konkurencijos iškreipimas neatsiranda savaime, todėl turi susiklostyti tam tikrų aplinkybių visuma.
2. Duomenų sutelkimas viename rankose dažnai gali nulemti ir rinkos galios turėjimą, o tai kai kurių nacionalinių institucijų, vykdančių konkurencijos teisės priežiūrą, įsitikinimu gali sąlygoti piktnaudžiavimą vyraujančia padėtimi. Tačiau dėl vyraujančio pliuralistinio požiūrio į duomenų turėjimą viename rankose ir skirtingų valstybių taikomas skirtingas žalos teorijas skirtingų valstybių priežiūros institucijos tą pačią „problema“ (didelių duomenų sutelkimas viename rankose) vertina skirtingai ir nebūtinai įžvelgia vien tik konkurencijos teisės problemas. Aiškių ir universalių taisyklių nebuvimas lemia, kad kiekviena nacionalinė institucija, naujoviškai pritaikydama žalos teorijas, tokį patį ar panašų su duomenų apsaugos pažeidimu susijusį pažeidimą gali įvertinti skirtingai: nuo konstatavimo, kad buvo pažeistos vartotojų teisės, iki antikonkurencinio elgesio – piktnaudžiavimo vyraujančia padėtimi.
3. EK susijungimų bylose sistemingai ir nuosekliai laikosi pozicijos, kad duomenų ir privatumo apsauga yra ne konkurencijos teisės objektas, todėl šio aspekto susijungimų bylose nenagrinėja, nors kas kartą dalyvaujančioms šalims primena būtinybę laikytis duomenis ir privatumą saugančių teisės aktų reikalavimų. Taigi EK kol kas nekuria reikšmingos praktikos, kurioje būtų nurodyta, kaip ir kada reikėtų daryti takoskyrą tarp duomenų apsaugos ir konkurencijos teisės.
4. Skaitmeninių rinkų aktas nors ir turi užuominų į tai, kad jis yra skirtas sujungti tiek metų diskusijas keliančius klausimus dėl duomenų apsaugos ir konkurencijos teisės sąveikos, tačiau panašu, kad šis bandymas bent jau kol kas nėra sėkmingas.

Skaitmeninių rinkų aktas yra skirtas tik kelioms didžiosioms technologijų įmonėms, prieš kurias įvairios nacionalinės institucijos jau anksčiau ėmėsi atitinkamų veiksmų ir tyrimus užbaigė sankcijomis. Tačiau šis aktas neduoda universalių priežiūrą vykdančių institucijų elgesio gairių, tai tėra dar vienas papildomas aktas šalia kitų, jau egzistuojančių ir atskirai santykius reguliuojančių teisės aktų. Tačiau manytina, kad atliekant ateities tyrimus atitinkamos institucijos šiuo teisės aktu galėtų naudotis kaip analogu, gaires suteikiančiu teisės aktu.

THE UNIVERSALITY OF COMPETITION LAW IN DEALING WITH UNFAIR COMPETITION CASES INVOLVING DATA PROTECTION INFRINGEMENTS

Greta Petkutė

Mykolas Romeris University, Lithuania

Summary. *In the digital economy, with data being one of the main criteria for competitive advantage, supervisory authorities are faced with the challenge of ensuring the effective protection of goods protected by different branches of law. Recent practice shows that the same or substantially similar infringements are viewed and assessed differently by supervisory authorities, some of which tend to find that data protection infringements per se imply anti-competitive behavior by legal entities, while others find infringements in the area of privacy or consumer protection. In merger cases, the European Commission has generally taken the consistent position that data protection and competition law are two distinct areas of law, each governed by different legislation, the supervision of which is entrusted to different authorities. This divergence is due to the fact that there are no universal rules. Even though there is as yet no universal framework to address data protection infringements that undermine fair competition, the article analyses whether the current legal framework is sufficient to address data protection and competition law infringements.*

Keywords: *data; data protection; unfair competition; technology companies; consumer protection.*

Greta Petkutė, Mykolas Romeris universiteto Privatinių teisės instituto doktorantė, lektorė. Mokslinių tyrimų kryptys: konkurencijos teisė, asmens duomenų apsaugos teisė, vartotojų apsaugos teisė.

Greta Petkutė, PhD student, lecturer at the Institute of Private Law at Mykolas Romeris University. Research interests: competition law, data protection law, consumer protection law.