ASMENS DUOMENŲ APSAUGOS PAŽEIDIMAI SOCIALINIUOSE TINKLUOSE PAGAL ES BENDRĄJĮ DUOMENŲ APSAUGOS REGLAMENTĄ

Klaudija Jagminaitė
E. paštas: j.klaudija@gmail.com
Mykolo Romerio universiteto Teisės mokykla

Santrauka. Straipsnyje teoriniu ir praktiniu būdu analizuojamas bendrųjų asmens duomenų reglamentas, kuriuo grindžiama asmens duomenų subjektų teisė į teisėtą, sąžiningą, ir skaidrų jų asmens duomenų valdymą ir tvarkymą, vienodai aukštu lygiu užtikrinant visapusišką konfidencialumą. Teisė į asmens duomenų apsaugą – teisė į privatumą, būtent Europos Sąjungos priimtas bendrųjų duomenų apsaugos reglamentas apima asmens duomenų subjektų teises ir jas visapusiškai išplečia. Šiame straipsnyje autorė aptaria pagrindines asmens duomenų subjekto teises į asmens duomenų apsaugą ir analizuoja asmens duomenų valdytojų ir / ar tvarkytojų pažeidimus socialiniuose tinkluose, nepakankamą jų apsaugą ir neįgyvendinto reglamento ypatumus, kurie atsispindi autorės analizuojamuose bendrųjų duomenų apsaugos reglamento didžiausiuose pažeidimuose Europos Sąjungos ir Lietuvos mastu. Tik tinkamas ir visapusiškas reglamento įgyvendinimas gali apsaugoti asmens duomenų subjektus nuo pažeidimo į privatumą, o asmens duomenų valdytojus ir / ar turėtojus nuo reglamento pažeidimų.

Reikšminiai žodžiai: asmens duomenų subjektas, asmens duomenų valdytojas, asmens duomenų tvarkytojas, bendrųjų duomenų apsaugos reglamentas, socialiniai tinklai.

Įvadas

Bendrųjų duomenų apsaugos reglamento tikslas yra apsaugoti asmens duomenų subjektus nuo bet kokio masto pažeidimo į privatumą. Reglamentas apima rinkodaros ir net elgesio analizės teisės į privatumą užtikrinimą. Tai aktualiausia yra socialinių tinklų vartotojams siekiant juos apsaugoti nuo asmens duomenų valdytojų ir tvarkytojų pažeidimų.

2016 m. balandžio 27 d. buvo priimtas Europos Sąjungos bendrųjų apsaugos duomenų reglamentas, o šalyse narėse reglamentas perkeltas į nacionalinę teisę ir pradėtas taikyti nuo 2018 m. gegužės 25 d. Lietuvoje reglamentą įgyvendina Valstybinė asmens duomenų inspekcija, kurios tikslas yra priimti ir nagrinėti reglamento pažeidimus Lietuvoje.

Pagrindiniai reglamento tikslai yra tai, kad Europos Sąjungos valstybės narės vienodai ir aukštu lygiu gebėtų apsaugoti asmens duomenų subjektus ir remdamosi reglamentu užtikrintų jų teises ir privatumą taip siekiant stiprinti subjektų teises. Teisėtumo, sąžiningumo, skaidrumo ir konfidencialumo principai yra pamatiniai reglamento principai, kuriais grindžiami asmens duomenys kaip saugoma vertybė ir teisė į privatumą.

Siekdama užtikrinti asmens duomenų apsaugą socialiniuose tinkluose nuo galimų pažeidimų į asmens teisę į privatumą ir kibernetinių atakų, kurių padariniai yra didelio masto, ir norėdama išvengti tokių pažeidimų Europos Sąjunga įpareigojo nares įgyvendinti reglamentą nacionalinėje teisėje siekiant apsaugoti asmens duomenų subjektus.

Šio mokslinio straipsnio aktualumas siejamas su bendrojo duomenų apsaugos reglamento naujumu ir aktualumu, taip pat įgyvendinimu siekiant apsaugoti socialinių tinklų vartotojus.

Šio mokslinio straipsnio tikslas yra išanalizuoti bendrųjų duomenų apsaugos reglamento taikymą asmens duomenų subjektams socialiniuose tinkluose ir išanalizuoti didžiausius reglamento pažeidimus Europos Sąjungos ir Lietuvos mastu.

Šio mokslinio straipsnio uždaviniai:

1. atskleisti bendrųjų duomenų apsaugos reglamento principų užtikrinimą;
2. aptarti asmens duomenų subjekto apsaugą socialiniuose tinkluose;
3. išanalizuoti didžiausius bendrųjų duomenų apsaugos reglamento pažeidimus Europos Sąjungoje ir Lietuvoje.

Šio mokslinio straipsnio objektas yra bendrųjų duomenų apsaugos reglamento sukurtos teisės į asmens duomenų apsaugą ir duomenų tvar-

kymą socialiniuose tinkluose.

Moksliniame straipsnyje taikyti šie teoriniai ir empiriniai metodai: lingvistinės ir lyginamosios analizės metodai pasitelkti siekiant atskleisti bendrųjų duomenų apsaugos reglamento teorinius ypatumus; nagrinėjant, kokiais teisės principais grindžiama asmens duomenų apsauga, taikyti loginis-analitinis ir sisteminės analizės metodai. Loginis-analitinis ir sisteminės analizės metodai taip pat pasitelkti apibendrinant teisės aktų ir teisės doktrinas, mokslinį straipsnį, atskleidžiant skirtingų teisės normų santykį, pagrindines problemas ir formuluojant išvadas.

1. Bendrųjų duomenų apsaugos reglamentas

Atsižvelgiant į pasaulyje vykstančius socialinius pokyčius dėl asmens duomenų rinkimo, jų naudojimo ir prieinamumo, Europos Parlamentas ir Europos Sąjungos Taryba 2016 m. priėmė naują reglamentą – bendrųjų duomenų apsaugos reglamentą (toliau – BDAR) 2016/679, kuriuo panaikino ES direktyvą 94/96/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, kuria buvo grindžiamas asmens duomenų tvarkymas ir jų judėjimas.

Naujasis reglamentas į valstybių narių nacionalinę teisę buvo perkeltas 2018 metais. Jo tikslas yra apsaugoti teisinį gėrį – fizinius asmens duomenis. Būtent šiuo reglamentu siekiama užtikrinti vienodo ir aukšto lygio fizinių asmenų apsaugą nuo duomenų turėtojų ir valdytojų. Remiantis tuo, kas išdėstyta reglamente, duomenų valdytoju yra laikomas fizinis arba juridinis asmuo, agentūra, valdžios įstaiga, kurie nustato duomenų tvarkymo tikslus ir priemones. Duomenų tvarkytojas nuo duomenų valdytojo skiriasi tuo, kad tvarkytojas duomenų valdytojo vardu tvarko asmeninius duomenis. Pabrėžtina yra tai, kad BDAR nėra taikomas tada, kai asmuo tvarko asmeninius duomenis vykdydamas tik asmeninę, namų ūkio priežiūros veiklą, nes toks asmuo nėra duomenų tvarkytojas ar valdytojas ir nesuteikia jokių priemonių asmens duomenų tvarkymui[1].

Duomenų valdytojai ir tvarkytojai, norėdami teisėtai valdyti ir tvarkyti asmenų duomenis, privalo gauti asmens duomenų turėtojo sutikimą,

[1] „2016 m. balandžio 27 d. Europos Sąjungos Reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo“, EUR-Lex, žiūrėta 2022 m balandžio 7 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=celex%3A32016R0679.

kad jis sutinka, jog jo asmens duomenys būtų tvarkomi ir valdomi būtent šio fizinio ar juridinio asmens ar kitos įstaigos ar organizacijos, – būtent tokia prievolė yra įtvirtinta BDAR 7 straipsnyje. Tačiau svarbus aspektas – asmens sutikimas turi būti suteiktas tokia forma, kad asmens duomenų valdytojas gebėtų įrodyti tokio sutikimo fakto buvimą. Tai reiškia, kad žodinis asmens sutikimas nėra toks sutikimas, kurį esant būtinybei būtų galima įrodyti, nebent tai fiksuotomis ryšio priemonėmis užfiksuotas asmens sutikimas valdyti jo asmens duomenis.

2. Socialiniai tinklai ir asmens duomenų apsauga

Socialiniai tinklai – tai bendruomenė, tarpusavyje susijusi tam tikromis temomis[2], tai virtuali erdvė, kurioje lengva rasti aktualią informaciją, naudotis tam tikromis paslaugomis. Net visos valdžios institucijos yra gyventojams sukūrusios portalus internete, kad jie galėtų naudotis valdžios paslaugomis ar gauti aktualią informaciją neišeidami iš namų, vos paspaudę kelis mygtukus. Socialinių tinklų atsiradimas ir laisvas jų prieinamumas lėmė nuolatinį socialinių pokyčių virsmą: kuriama daugybė interneto puslapių, o mobiliosios programėlės tam tikra prasme ragina visuomenę vis labiau integruotis į technologijų naujoves virtualiame pasaulyje. Nemokamas prisijungimas, naujienos sklaidos platformos, įvairių bendravimo būdų pasiekiamumas dažniausiai paskatina vis daugiau žmonių prisijungti prie socialinių tinklų, nes priėjimas prie socialinių tinklų yra lengvas, o kūrėjų tikslas yra orientuotas į visuomenės plėtimą ir prisijungimą[3].

Pastaruoju metu socialiniuose tinkluose yra gausu pasirinkimų, kuriais gali naudotis kiekvienas vartotojas. Tačiau dažniausiai, norint tapti tam tikros programėlės ar socialinio portalo vartotoju, reikia prisiregistruoti, dėl to yra prašoma įvesti savo asmens duomenis, kad sistema galėtų sugeneruoti virtualią paskyrą naujam vartotojui. Nuo 2018 m., kai buvo priimtas BDAR reglamentas, kiekvienas vartotojas turi būti supažindinamas su informacija dėl to, kaip bus valdomi ir tvarkomi jo pateikti asmens

---

2 „Socialinis tinklas“, Zodynas.vz.lt., žiūrėta 2022 m. kovo 15 d., http://zodynas.vz.lt/socialinis-tinklas.

3 Gintarė Sirbikytė, „Ar socialinio tinklo valdytojas atsako už šio tinklo naudotojo neteisėtais veiksmais padarytą žalą?“, *Teisės apžvalga* 1, 10 (2013): 30–85, https://portalcris.vdu.lt/server/api/core/bitstreams/20f7219d-f89f-492b-a360-43ce185fd531/content.

duomenys. Jis taip pat turi teisę paprašyti, kad asmens duomenys būtų pakoreguoti, jei jie yra neteisingi, apriboti duomenų tvarkymą, taip pat paprašyti, kad jie būtų ištrinti. Būtent tokios asmens teisės yra įtvirtintos BDAR reglamente siekiant būtino ir aukščiausio lygio asmens duomenų sąžiningumo ir skaidrumo, kiek tai yra susiję su asmens duomenų tvarkymu[4].

Remiantis valstybinės duomenų apsaugos inspekcijos (toliau – VDAI) 2021 m. veiklos ataskaita, nuo tada, kai buvo pradėtas taikyti BDAR, asmenų skundų dėl asmens duomenų pažeidimų kasmet vis daugėja. Pavyzdžiui 2021 m. gauti ir nagrinėti net 239 asmenų skundai. Dėl šių asmens saugumo pažeidimų buvo paveikti 3 379 123 paskyrų vartotojai. Pagrindinės nustatytų pažeidimų priežastys:

1. konfidencialumo praradimas (neautorizuota prieiga ar atskleidimas);

2. vientisumo praradimas (neautorizuotas asmens duomenų pakeitimas);

3. prieinamumo praradimas (asmens duomenų praradimas, sunaikinimas).

Opiausia problema – konfidencialumo praradimas. VDAI teigimu, didesnių ar mažesnių BDAR pažeidimų vyksta nuolatos[5]. Remiantis Lietuvos VDAI 2021 m. statistika, dažniausiai pažeidžiamas BDAR 32 str. 1 p. b p., nes asmens duomenų valdytojai ir tvarkytojai negeba užtikrinti asmens duomenų konfidencialumo, o tai lemia neteisingą techninių priemonių įgyvendinamą siekiant užtikrinti konfidencialumą.

Įvykus asmens duomenų pažeidimui, kai gali kilti reikšmingas pavojus asmens duomenų turėtojo teisėms ir laisvėms, asmens duomenų valdytojas privalo nedelsdamas informuoti asmens duomenų turėtoją apie įvykusį pažeidimą. Tačiau pabrėžtina tai, kad reglamente išskiriamos net trys išimtys, kai asmens duomenų valdytojas neprivalo pranešti apie įvykusį incidentą, pavyzdžiui: jeigu buvo pritaikytos aukščiausio lygio techninės priemonės, kai subjekto informacija buvo užšifruota ir kitas asmuo negalėtų peržiūrėti duomenų, susijusių su asmens duomenimis, ar

---

4 „2016 m. balandžio 27 d. Europos Sąjungos Reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo“, *supra note*, 1: 13 str.

5 „Valstybinės asmens duomenų apsaugos inspekcijos 2021 m. veiklos ataskaita“, vdai.lrv, 9, žiūrėta 2022 m. kovo 16 d., https://vdai.lrv.lt/uploads/vdai/documents/files/2021%20m_%20VDAI%20veiklos%20ataskaita.pdf.

po pažeidimo asmens duomenų valdytojas ėmėsi priemonių užtikrinimo, kad nekils pasekmių subjekto teisėms ir laisvėms, arba informacija apie pažeidimą yra paskelbiama viešai, nes tai reikalautų didelių pastangų informuoti kiekvieną asmens duomenų turėtoją[6]. Tokios išlygos, įtvirtintos reglamente, suteikia teisę asmens duomenų valdytojui nepranešti fakto asmens duomenų subjektams, kad įvyko asmens duomenų pažeidimas.

3. Bendrųjų asmens duomenų reglamento pažeidimai socialiniuose tinkluose

Dėl socialiniuose tinkluose nuolat vykstančių pažeidimų, kurių metu nukenčia asmens duomenys, Europos Sąjunga priėmė naują reglamentą. Būtent tai paskatino asmens duomenų apsaugos suvienodinimą ir aukšto lygio apsaugos reikalavimų įteisinimą kiekvienoje šalyje narėje.

Nors pažeidimų vyksta nuolatos, tačiau buvo išskirti 25 didžiausi pažeidimai socialiniuose tinkluose nuo 2019 m. Europos Sąjungos mastu. Reikšmingiausi yra šie keturi pažeidimai:

„Amazon Europe“ – 746 mln. eurų. Nors dar vyksta apeliacinis procesas ir baudos dydis nėra galutinis, tačiau tai buvo didžiausia kada nors paskirta bauda už BDAR pažeidimą[7]. Bauda paskirta už BDAR 7 str. pažeidimą, kone dažniausiai pasitaikantį reglamento pažeidimą, kai duomenų valdytojai, neturėdami asmens duomenų turėtojų sutikimo, siunčia jiems personalizuotą reklamą. Tokio pažeidimo būtų galima išvengti, jei įmonės kauptų kiekvieno asmens duomenų subjekto sutikimus personalizuotai reklamai gauti teisėtu būdu.

„WhatsApp“ – 225 mln. eurų. Įmonė kaltinama pažeidusi BDAR 5 str. – padariusi su asmens duomenimis susijusių principų – teisėtumo, sąžiningumo ir skaidrumo – pažeidimą[8]. Remiantis reglamento 5 str. 2 d., asmens duomenų valdytojas paklūsta atskaitomybės principui. Tai reiškia, kad duomenų valdytojas, pažeidęs reglamente įtvirtintus principus, kurie

---

6 „2016 m. balandžio 27 d. Europos Sąjungos Reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo“, *supra note*, 1: 34 str.

7 Raminta Stravinskaitė, „BDAR baudos 2021: ko galime pasimokyti?“, *LRT*, 2022 m. sausio 10 d., https://www.lrt.lt/naujienos/verslo-pozicija/692/1584663/raminta-stravinskaite-bdar-baudos-2021-ko-galime-pasimokyti.

8 „25 biggest GDPR fines so far“, *Tessian*, 2022 m. sausio 27 d., https://www.tessian.com/blog/biggest-gdpr-fines-2020/>.

saugo asmens duomenų subjektus, yra teisiškai atsakingas už pažeidimą, jei negeba įrodyti, kad buvo laikomasi visų reglamente įtvirtintų principų, kurių siekis yra apsaugoti asmens duomenų turėtoją, kadangi subjektas, pateikdamas savo asmeninius duomenis, turi teisę į teisėtą, sąžiningą ir skaidrų valdymą. Tuo atveju, kai socialinio tinklo valdytojas siunčia personalizuotą informaciją asmens duomenų subjektui be laisvo jo sutikimo tokią informaciją gauti, yra pažeidžiama jo asmens duomenų apsauga, kurią duomenų valdytojas privalo apsaugoti.

„Google Ireland“ – 9 mln. eurų. Bauda skirta už BDAR 7 str. pažeidimą. „Google“ atvejis parodo, kad interneto svetainėje, vieną kartą sutikus su slapukais, labai sunku rasti, kur jų atsisakyti[9]. Tačiau BDAR 21 str. yra įtvirtinta, kad asmuo bet kuriuo metu turi teisę atsisakyti dėl jo asmens duomenų tvarkymo. Remiantis reglamentu, asmens duomenų subjektui suteikta teisė atsisakyti leidimo valdyti jo duomenis net tuo atveju, jeigu anksčiau asmuo ir buvo davęs sutikimą. Tačiau toks sutikimas negali būti laikomas kaip visam laikui pateiktas sutikimas valdyti ir tvarkyti asmens duomenis. Būtent todėl kiekvienas socialinis tinklas privalo užtikrinti, kad vartotojas, kuris anksčiau suteikė leidimą, galėtų lengvai ir bet kada to atsisakyti.

„Facebook“ – 90 mln. eurų. Bauda skirta už BDAR 7 str. pažeidimą analogiškai kaip ir „Google Ireland“. Tačiau „Facebook“ atveju tai dalinai buvo kitoks pažeidimas. Jo principas – iššokančiame langelyje nebuvo jokio kito pasirinkimo – tik sutikti su slapukais[10]. Taigi asmens duomenų valdytojas socialinio tinklo vartotojui nesuteikė teisės nesutikti. Ši teisė yra įtvirtina ir aiškiai apibrėžta BDAR. Taip pat svarbiausias aspektas yra tas, kad socialinio tinklo vartotojui informacija būtų suteikta aiškiai ir lengvai suprantamu būdu.

Lietuvoje taip pat buvo nustatyta keletas BDAR pažeidimų, dėl kurių juridiniai asmenys gavo dideles baudas. Išskiriama keletas svarbiausių ir didžiausių pažeidimų per pastaruosius metus Lietuvoje:

„CityBee“ – 110 tūkst. eurų. Bauda skirta už įmonės vartotojų konfidencialumo neužtikrinimą. Kibernetinės atakos metu iš įmonės varotojų duomenų bazės buvo atskleisti ir viešai paskelbti 110 tūkst. asmens duomenų turėtojų duomenys[11]. Taip įmonė pažeidė BDAR 24 str., kai duomenų valdytojas netinkamai įgyvendino organizacines ir techni-

[9] „25 biggest GDPR fines so far“, *supra note*, 8.

[10] *Ibid*.

[11] Stravinskaitė, *supra note*, 7.

nes priemones, numatytas reglamente, kurių tikslas yra apsaugoti asmens duomenų subjektą nuo konfidencialumo pažeidimo. Visais atvejais asmens duomenų valdytojas privalo užtikrinti, kad jis įgyvendina tinkamas organizacines ir technines priemones siekdamas išvengti kibernetinių atakų ar kitokio pobūdžio pažeidimo siekiant atskleisti ir paviešinti asmenų duomenis.

Nacionalinis visuomenės saugumo centras (toliau – NVSC) ir „IT sprendimai sėkmei“ (toliau – IT). 3 tūkst. eurų bauda paskirta IT įmonei dėl sukurtos mobiliosios programėlės „Karantinas“, o NVSC paskirta 12 tūkst. eurų bauda. Įmonės pažeidė BDAR neatlikusios poveikio duomenų apsaugai tyrimo, nes duomenys buvo naudojami Lietuvoje ir už jos ribų. Teisėtumo ir atskaitomybės principus įmonės pažeidė todėl, kad nesugebėjo įrodyti, kad asmens duomenų turėtojų duomenys buvo tvarkomi teisėtu būdu, taigi pažeidė BDAR 5 str., nes įmonė visais atvejais yra atskaitinga už įvykdytą pažeidimą ir privalo gebėti įrodyti, kad asmens duomenų subjektai suteikė leidimą tai daryti laisva valia[12].

Remiantis išanalizuotais duomenis dėl BDAR pažeidimų Europos Sąjungos ir Lietuvos mastu matyti, kad tokie pažeidimai buvo nustatyti per laikotarpį nuo 2018 m. gegužės mėnesio, kai Europos Sąjungos šalys narės privalėjo perkelti BDAR į savo nacionalinę teisę. Tai akivaizdžiai atskleidžia faktą, kad socialinių tinklų asmens duomenų valdytojai, nesilaikydami reglamente įtvirtintų teisės normų, pažeidžia asmens duomenų apsaugą, į kurią turi teisę kiekvienas asmens duomenų subjektas.

Išvados

Apibendrinant išdėstytą medžiagą teigtina, kad bendrųjų duomenų apsaugos reglamentu siekiama vienodu ir aukščiausiu lygiu apsaugoti asmens duomenų subjektus, nes teisės tikslas yra ginti teisinį gėrį. Stebint situaciją, kai žmonija smarkiai pasistūmėjo į priekį ir vis labiau naudojasi socialinių tinklų suteiktomis galimybėmis, reglamente įtvirtinti teisėtumo, sąžiningumo ir skaidrumo principai tiesiogiai saugo asmens duomenų turėtojus. Taip yra dėl to, kad socialinių tinklų portalai – asmens duomenų valdytojai ir tvarkytojai – yra įpareigojami vadovautis reglamente įtvirtintomis teisės normomis ir būti atskaitingiems esant reglamento pažeidimui. Vykstant socialiniams pokyčiams Sąjunga privalėjo imtis tei-

[12] Stravinskaitė, *supra note*, 7.

sinių veiksmų ir keisti duomenų apsaugos reglamentą asmens duomenų subjekto naudai, kadangi socialiniuose tinkluose renkama, ir kaupiama asmens duomenų informacija juda ne tik tam tikroje šalyje, tačiau Sąjungos ar tarptautiniu mastu. O esant kibernetinės atakos galimybei asmens duomenys gali būti laisvai atskleisti ir paviešinti neįgyvendinus konfidencialumo principo vartotojo asmens duomenų apsaugai. Atkreiptinas dėmesys į tai, kad valstybės narės įgyvendino reglamentą nacionalinėje teisėje, tačiau pažeidimų kasmet vis daugėja ir tai patvirtina faktą, kad asmens duomenų valdytojai ir turėtojai vis dar negeba tinkamai įgyvendinti bendrųjų apsaugos duomenų reglamento, o dėl to pažeidžiamos asmens subjekto teisės į asmens duomenų apsaugą.

BREACHES OF PERSONAL DATA PROTECTION ON SOCIAL NETWORKS UNDER THE EU GENERAL DATA PROTECTION REGULATION

Klaudija Jagminaitė
Mykolas Romeris University, Lithuania

Summary. This article analyzes, in a theoretical and practical way, the General Personal Data Regulation, which underpins the right of personal data subjects to lawful, fair, and transparent management and processing of their personal data, ensuring a high level of full confidentiality. The right to the protection of personal data is the right to privacy, namely the general data protection regulation adopted by the European Union, which covers and extends the rights of personal data subjects. In this article, the author presents the basic rights of a personal data subject to personal data protection and analyzes violations of personal data controllers and/or processors on social networks, insufficient protection, and peculiarities of the unimplemented regulation. Only the proper and full implementation of the Regulation can protect personal data subjects from privacy breaches and personal data controllers and/or holders from breaches of the Regulation.

Keywords: personal data subject, personal data controller, personal data processor, general data protection regulation, social networks.