https://doi.org/10.15388/TMP.2021.12

TREČIŲJŲ ŠALIŲ SLAPUKAI: KOKS PASAULIS BE JŲ?

Justė Juškaitė, Milda Aušrinė Janušauskaitė
Vilniaus universiteto Teisės fakulteto 2 kurso studentės
Saulėtekio al. 9, I rūmai, 10222 Vilnius
El. paštas: ausrine.janusauskaite@tf.stud.vu.lt; juste.juskaite@tf.stud.vu.lt
Mokslinio straipsnio akademinis kuratorius dr. Paulius Jurčys
El. paštas: pjurcys@gmail.com
Mokslinio straipsnio praktinis kuratorius Jelena Jonis
El. paštas: jelena.jonis@prevence.legal

2020 metų sausio 14 dieną Google priėmė sprendimą, kuriame paskelbė, kad nuo 2022 metų bus atsisakomi trečiųjų šalių slapukai. Tai lėmė visuotinę reakciją dėl šio siekiamo pokyčio tarptautinėje rinkoje, kadangi „sausainėlių" pabaiga užkirs kelią rinkti bei naudoti informaciją apie vartotojus. Todėl bendrovės bus priverstos ieškoti naujų metodų, kaip pasiekti rinkodarai reikiamus duomenis. Straipsnyje analizuojama, kokios pirmosios rinkos dalyvės ėmėsi šio sprendimo įgyvendinimo, koks viso to teisinis pagrindas ir tikslai. Be to, darbe rašoma, kokią tai turės reikšmę tokiems faktoriams kaip reklamos ekosistemai, verslo modeliams bei vartotojų duomenų apsaugos reikalavimų išpildymui.

Pagrindiniai žodžiai: *Slapukai, pirmųjų šalių slapukai, trečiųjų šalių slapukai, e. Privatumo direktyva.*

Įvadas

Mokslinio straipsnio **tikslas** yra ištirti, kaip trečiųjų šalių slapukų panaikinimas paveiks dabartinę rinką. Šio tikslo bus siekiama analizuojant tarptautinių kompanijų pozicijas, „sausainėlių" reguliavimo ypatumus Europos Sąjungos kontekste, trečiųjų šalių slapukų atsisakymo reikšmę verslo modeliams, įtaką duomenų bei vartotojų teisių apsaugai.

Atliekamo tyrimo **objektas** – trečiųjų šalių slapukai.

Darbo **aktualumą** lemia tai, jog šiuo metu yra keliama daug klausimų, kaip gali atrodyti rinka po Google įgyvendinto sprendimo atsisakyti trečiųjų šalių slapukų. Be to, figūruoja svarbus aspektas, kokią reikšmę vartotojų duomenų apsaugai turės šis pokytis, kadangi šiuo metu ši technologija teisiškai nėra reguliuojama eksplicitiškai.

Darbe taikomi **tyrimo metodai**: 1) istorinis – jį taikant atskleidžiama, kokią įtaką iki šiol turėjo trečiųjų šalių slapukai; 2) sisteminis – šiuo metodu atskleidžiamas teisės aktų turinys, straipsnių prasmė; 3) lingvistinis – padeda ištirti moksliniam straipsniui aktualius šaltinius ir juos tikslingai pritaikyti; 4) lyginamasis – taikomas vertinant trečiųjų šalių slapukų buvimą šiandieninėje rinkoje ir jų visišką atsisakymą ateityje; 5) tarpdisciplininis – šiuo metodu siekiama ištirti skirtingų mokslo sričių bendradarbiavimą slapukų kontekste.

Darbo **originalumą** lemia tai, jog ši tema nėra plačiai nagrinėjama Lietuvos teisės mokslo akademinėje veikloje. Taip pat, verta paminėti, jog ši tema yra aktuali ne tik Lietuvos, bet ir tarptautiniu lygmeniu.

Darbui išskirtinai reikšmingi **šaltiniai**: Vienas iš pagrindinių straipsnyje minimų šaltinių – BDAR (Bendrasis duomenų apsaugos reglamentas) (angl. *GDPR (General Data Protection Regulation)*), kuriame įtvirtinti pagrindiniai reikalavimai siekiant užtikrinti vienodo ir aukšto lygio fizinių asmenų duomenų apsaugą. Šis dokumentas svarbus įtvirtinant pagrindinius principus ir taisykles valdant, tvarkant bei perduodant surinktą asmeninio pobūdžio informaciją. Vis dėlto BDAR eksplicitiškai neįtvirtina elektroninių ryšių reguliavimo, todėl svarbu išskirti kitą šiam darbui reikšmingą teisės aktą – Europos Parlamento ir Tarybos direktyvą 2002/58/EB (Direktyva dėl privatumo ir elektroninių ryšių). Direktyva dėl privatumo ir elektroninių ryšių yra reikšminga, kadangi joje minima „sausainėlių" sąvoka, įtvirtintas šių technologijų reguliavimas bei nurodomi reikalavimai, kurių duomenų vykdytojai turi laikytis naudodami surinktus asmenų duomenis. Šiuo teisės aktu užtikrinama pagrindinių teisių ir laisvių, visų pirma teisės į privatų gyvenimą ir komunikacijos konfidencialumą, apsauga ir asmens duomenų apsauga elektroninių ryšių sektoriuje. Tačiau siekiant visuotinai taikomo reglamentavimo norima priimti aukštesnės galios teisės aktą – reglamentą, kadangi direktyvos reguliavimo sritis yra kur kas siauresnė. Neaiški tam tikrų nuostatų redakcija ir teisinių sąvokų dviprasmybė kelia kliūtis siekiant suvienodinti taikymo praktiką. Todėl kitas itin svarbus šaltinis – Europos Parlamento ir Tarybos reglamento pasiūlymas dėl teisės į privatų gyvenimą ir asmens duomenų apsaugos elektroninių ryšių sektoriuje, kuriuo panaikinama Direktyva 2002/58/EB (Reglamentas dėl privatumo ir elektroninių ryšių). Be to, straipsnyje taip pat remiamasi teismų praktika, kuri reikšminga sprendžiant klausimus, kokie teisės aktai turi reguliuoti slapukus ginant asmens teisę į duomenų apsaugą.

1. Trečiųjų šalių slapukų reikšmė

1.1. Pirmųjų ir trečiųjų šalių slapukų palyginimas

Pradedant, svarbu aptarti, kuo skiriasi pirmųjų šalių slapukai nuo trečiųjų ir kokia yra jų reikšmė dabartinėje rinkoje. Neretai tai sukelia diskusijų vartotojams, kurie, nors ir baimindamiesi dėl savo asmeninės informacijos saugumo, visgi nežino, kaip

duomenų vykdytojai juos valdo bei kur jie keliauja po to, kai internetinių svetainių naudotojai sutinka, kad būtų naudojami slapukai. Tai rodo, kad šis išskyrimas turi ne tik teisinės, bet ir praktinės reikšmės. Taigi pradžioje svarbu yra aptarti pirmųjų šalių slapukų sąvoką.

Pirmiausia, pirmųjų šalių slapukai sukuriami interneto svetainėse, kuriose lankosi vartotojai. Jose saugoma tik pagrindinė informacija, kuri nesukelia asmens duomenų apsaugos reikalavimų pažeidimų. Šie „sausainėliai" yra būtini siekiant vystyti internetinių puslapių veiklą tokia kryptimi, kuri atspindėtų vartotojų norus.

Tuo tarpu trečiųjų šalių slapukai naudoja kitų svetainių perduotą informaciją siekiant reklamos tikslų. Remiantis gautais duomenimis, vartotojui yra pateikiama individualizuota informacija, kuri leidžia paslaugų teikėjui siųsti skelbimus internetinės svetainės lankytojui, siekiant, kad jis įsigytų kokio nors pobūdžio prekę. Tačiau nepaisant fakto, jog „sausainėliai" yra itin naudingi reklamuotojams, šie taip pat kelia daugiausiai diskusijų dėl jų teisėtumo.

1 lentelė. *Pirmųjų ir trečiųjų šalių slapukų palyginimas*[1]

	Pirmųjų šalių slapukai	**Trečiųjų šalių slapukai**
Pagrindinis tikslas	Sklandesnė prieiga prie svetainės	Reklaminės programos įgalinimas
Veiklos kryptis	Išsaugo prisijungimo duomenis, pirkinių krepšelį	Nukreipiami būsimi klientai jiems pereinant iš vienos svetainės į kitą
Atsiradimo šaltinis	Domenas, kurio svetainėje asmuo lankosi	Skelbimų serveriai, socialinės žiniasklaidos svetainės, komentarų rinkėjai
Sekimo apimtis	Domenas, kuris yra vartotojo lankomas	Daugelio domenų naudotojai

1.2. Trečiųjų šalių slapukų keliama žala

Svarbu išskirti trečiųjų šalių slapukų neigiamą pusę, kuri lėmė siekį jų atsisakyti. Pirmiausia, slapukai renka asmens duomenis, kurie leidžia suasmeninti reklamą. Tai kelia abejonių ar dabartinė situacija neprieštarauja duomenų apsaugos įstatymams, kadangi manoma, jog rinkimo būdai yra netinkami ar neretai neteisėti. Pavyzdžiui, 2019 metais

[1] Michal Wlosik, Michael Sweeney. *What's the Difference Between First-Party and Third-Party Cookies?* [interaktyvus]. Prieiga per internetą: https://clearcode.cc/blog/difference-between-first-party-third-party-cookies/?fbclid=IwAR1C9NtRzKxHuuI_agUgRvb_4Me-VOG9ta80NaTwzNCV33pcMgpA6gvt42o [žiūrėta 2020 m. gruodžio 17 d.].

tarptautinės advokatų kontoros DLA Piper atlikta apklausa parodė, kad nuo Bendrojo duomenų apsaugos reglamento (toliau – BDAR) įsigaliojimo (2018 metų gegužės 26 dienos) buvo padaryta 59 430 duomenų apsaugos teisės pažeidimų, naudojant slapukus[2]. Be to, šis ginčas dažnai sukelia vartotojų nepasitikėjimą internetine svetaine. Tai įrodo atliktas tyrimas, kuriame ištirta, jog iš 150 dalyvių 68 respondentai neigiamai reaguoja į slapukų atsisakymo pranešimą dėl kylančios privatumo problemos[3]. Taigi galima teigti, kad po trečiųjų šalių slapukų taikymo pabaigos ši vartotojų dalis ims mažiau nerimauti dėl savo asmeninės informacijos neteisėto panaudojimo.

Antra, tekstiniai skelbimai su pranešimais apie slapukų naudojimą dažnai erzina vartotojus. Kiekvienoje svetainėje esantys tokio pobūdžio informaciniai pranešimai dažnai būna netinkami dėl savo turinio, formos bei juose pateiktos teisinės informacijos. Pavyzdžiui, byloje CNIL prieš Amazon Europe Core[4] buvo nustatytas Amazon pažeidimas dėl netinkamo informacijos suteikimo. Tikrindama amazon.fr svetainę, CNIL (Prancūzijos duomenų apsaugos agentūra) nustatė, kad vartotojams pateikta informacija nebuvo nei aiški, nei išsami. Svetainėje rodomoje slapukų juostoje buvo pateiktas bendras ir apytikslis slapukų tikslų aprašymas („pasiūlyti ir patobulinti mūsų paslaugas“). CNIL išaiškino, kad „Amazon Europe Core“ nesugebėjimas pateikti tinkamos informacijos buvo dar akivaizdesnis vartotojams, besilankantiems svetainėje, kai jie spustelėjo kitoje svetainėje paskelbtą skelbimą. Šiuo atveju jiems nebuvo pateikta jokia informacija[5]. Tai parodo, kad direktyvos reikalaujamas slapukų iššokantis pranešimas savo turiniu nėra suprantamas vartotojams.

Be to, tokia informacija apie „sausainėlius” eikvoja svetainių lankytojų laiką bei mažina susidomėjimą internetiniais puslapiais. Tai atskleidžia Kopenhagos universiteto inicijuotas tyrimas, kuriame iš 150 dalyvavusių asmenų 59 respondentai patvirtino, kad juos erzina iššokantis slapukų pranešimas bei tai vertina kaip naršymo patirties trikdymą[6]. Trečia, daugelis vartotojų per interneto naršykles ir „AdBlockers“ automatiškai blokuoja trečiųjų šalių slapukus dėl skirtingų priežasčių, todėl mažėja gaunama nauda, kurios tikisi paslaugų teikėjai *(žiūrėti diagramą Nr. 1)*.

Ketvirta, šie slapukai negali būti perduodami įvairiuose įrenginiuose ar net tarp programų, o tai reiškia, kad labai sunku sekti visą kliento pirkėjo kelionę. Verta paminėti,

---

2 Chris Brook. *Almost 60,00 Post-GDPR Data Breaches Reportes in Europe* [interaktyvus]. Prieiga per internetą: https://digitalguardian.com/blog/almost-60000-post-gdpr-data-breaches-reported-europe [žiūrėta 2021 m. vasario 15 d.].

3 Kulyk O. and others (2020). Has the GDPR hype affected users' reaction to cookie disclaimers? *Journal of Cybersecurity*, Volume 6, p. 1-14 [interaktyvus]. Prieiga per internetą: https://academic.oup.com/cybersecurity/article/6/1/tyaa022/6046452?login=true [žiūrėta 2021m. vasario 21 d.].

4 *AMAZON EUROPE CORE v. CNIL* [CNIL], No. SAN-2020-013, [7-12-2020].

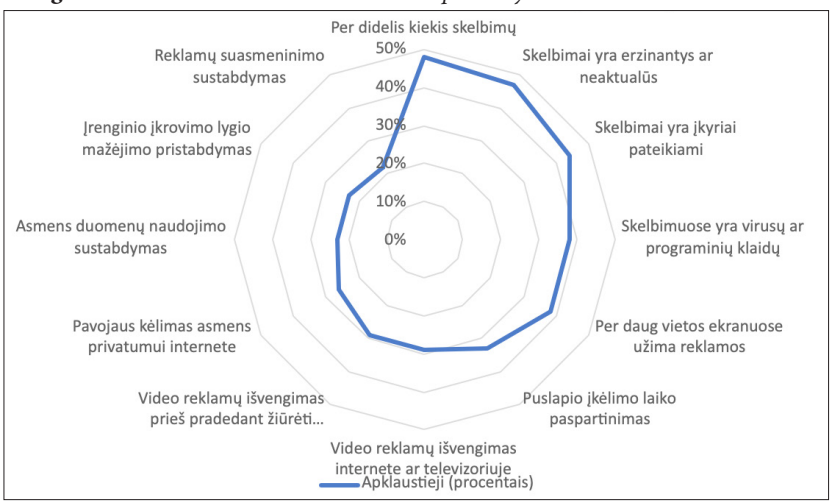
5 Hunton Andrews Kurth's Privacy and Cybersecurity (2020). Privacy and Information Security Law Blog, [blog] 14 December. Prieiga per internetą: https://www.huntonprivacyblog.com/2020/12/14/cnil-fines-google-and-amazon-135-million-euros-for-alleged-cookie-violations/ [žiūrėta 2021 m. sausio 20 d.].

6 Žiūrėti išnašą Nr. 3

jog norint išsiaiškinti įprastą pirkėjo kelią nuo pradžios iki pabaigos, yra reikalingas milžiniškas duomenų kiekis. Dėl šios priežasties kyla dauguma problemų rinkodaros specialistams: įmonės dažnai gauna informaciją per tarpininkus, todėl tiesioginiai klientų duomenys ir atsiliepimai nėra žinomi[7]. Tai reiškia, jog kuriant verslo strategijas, tokių duomenų tikslumu pasikliauti negalima. Dėl šių priežasčių reklamos įmonėms yra sukeliami papildomi iššūkiai dėl teisingo lėšų skirstymo ir tai neretai lemia jų švaistymą, kai reklamuotojams yra pateikiami neteisingi ar pasenę slapukų duomenys.

Apibendrinant galima daryti išvadą, jog atsiradusios šios trečiųjų šalių slapukų keliamos problemos bei nestabili teisinė padėtis stimuliuoja duomenų vykdytojus strategiškai persiorientuoti ar taikyti kitas technologijas, kurios teiks naudą tiek jiems, tiek vartotojams bei visapusiškai atitiks BDAR bei Europos Parlamento ir Tarybos Direktyva dėl privatumo ir elektroninių ryšių direktyvos (toliau – e. Privatumo direktyva) reikalavimus. Visgi laukia ilgas ir nelengvas kelias ieškant naujų alternatyvų prisitaikant prie naujų rinkos pokyčių bei siekiant, kad nebūtų priverčiami pasitraukti iš šios ekonomikos krypties. Toliau straipsnyje bus nagrinėjama, kas pirmiausia ėmėsi veiksmų siekiant šių tikslų įgyvendinimo.

1 diagrama. *Svarbiausios reklamos blokavimo priežastys*[8]



---

7 Jeff Rajeck. *Why mapping the customer journey is so hard – and what you can do about it* [interaktyvus]. Prieiga per internetą: https://econsultancy.com/why-mapping-the-customer-journey-is-so-hard-and-what-you-can-do-about-it/ [žiūrėta 2021 m. sausio 14 d.].

8 Global Web Index. *Global Ad-Blocking Behavior* [interaktyvus]. Prieiga per internetą: https://www.globalwebindex.com/hubfs/Downloads/Global_Ad-Blocking_Behavior.pdf [žiūrėta 2021 m. vasario 9 d.].

2. Pirmieji žingsniai siekiant sukurti internetą be slapukų

Nors šiuo metu slapukai yra labiausiai paplitęs būdas, kuriuo identifikuojamas vartotojas internete ir taip suteikiamas individualus naršymas, vis dėlto atrodo, jog toks metodas praras savo reikšmę. Tokia prielaida yra daroma remiantis besikeičiančiu supratimu apie vartotojo privatumą, naujus teisės aktus, kuriais yra įvedama nauja tvarka, aiškinanti slapukų tvarkymą, pavyzdžiui, Bendrasis duomenų apsaugos reglamentas, e. Privatumo direktyva. Nuo to laiko, kai įsigaliojo BDAR (2018 m. gegužės 25 d.), žiniasklaidoje buvo daug kalbama apie duomenų privatumą, tačiau interneto vartotojai retai skiria laiko, norėdami patikslinti savo naršyklės nustatymus dėl naudojamų slapukų ir iš tikrųjų apsaugoti savo duomenis – dažniausiai jie naršo internete naudodamiesi numatytaisiais nustatymais nesuprasdami tikrosios slapukų reikšmės.

Siekdamos suteikti vartotojams daugiau pasirinkimo ir galimybių bei taip sudarydamos sąlygas laikyti save palankesnėmis naršyklėmis nei kitos, šios per daugelį metų pristatė naujas bei skirtingas privatumo funkcijas. Verta paminėti ir tai, jog kai kurios naršyklės leidžia vartotojams blokuoti trečiųjų šalių slapukus, kurie dažniausiai yra naudojami reklamos tikslais. Kitos siekia užtikrinti gerą vartotojo patirtį, tačiau taip pat gali naudoti slapukus internetiniam stebėjimui. Tad galima daryti išvadą, jog kiekviena naršyklė trečiųjų šalių slapukus naudoja skirtingais tikslais, o vartotojai, neįsigilinę į tinklalapio nustatymus, naršo nežinodami tikrosios slapukų reikšmės bei galimų pasekmių.

Apibendrinant, svarbu paminėti, jog Google nėra pirmoji didžioji įmonė, kuri nusprendė atsisakyti trečiųjų šalių slapukų. Nors galėtų atrodyti, kad pradžią šiems pokyčiams lėmė jos įtaka, tačiau jau 2017 metais tokį sprendimą priėmė kitos didžiosios įmonės kaip Firefox bei Apple, kurios itin didelį dėmesį skyrė vartotojo privatumui.

2.1. Firefox

Firefox yra interneto naršyklė, kurią kuria pasaulyje vyraujanti atviruųjų programų organizacija Mozilla. Tai yra viena iš populiariausių interneto naršyklių, kuri 2019 m. sausio mėn. pristatė naujų privatumo valdiklių rinkinį „Firefox 65“. Šis žingsnis lėmė vartotojams nuolat įjungtą apsaugą nuo daugybės sekimo technologijų, kuriomis yra siekiama stebėti žmonių atliekamus veiksmus internete. Tačiau po šio pokyčio, Firefox inžinieriai toliau kūrė mechanizmą, saugantį vartotoją nuo sekimo internete, ir jau 2019 m. rugsėjo mėnesį išleido tobulesnę versiją.

Pirmiausia, verta paminėti tai, jog trečiųjų šalių slapukai yra vienas iš daugelio mechanizmų, kurį svetainių savininkai ir skelbimų tinklai naudoja laikydamiesi skirtukų apie tai, kokiose svetainėse jie lankosi ir su kokiu jų turinio ieško. Tinklai ir svetainių savininkai gali naudoti šią informaciją kurdami asmenų istorijas ir profilius, kuriuos

vėliau naudoja skelbimams ir kitam turiniui pritaikyti – reklamai, rinkodaros tikslams. 2019 m. rugsėjo 3 d. Firefox išleidus patobulintą stebėjimo apsaugą „Firefox 69" buvo suteikta žmonėms galimybė spustelėti piktogramą adreso juostoje, kad pamatytų, kuriuos konkrečius stebėjimo slapukus naršyklė blokuoja tam tikroje svetainėje. Ši naujovė taip pat apima apsaugą nuo kriptografų (asmenų, kurie stengiasi dešifruoti užšifruotą dokumentą (dar kitaip vadinamą kriptogramą) arba vietoje tikro dokumento perduoti pakeistą). Anot naujausių statistinių duomenų, daugiau kaip 66 % mažų ir vidutinių įmonių patyrė kibernetines atakas, kurių metu buvo siekiama pasisavinti bendrovių saugomus dokumentus. Viso to priežastis buvo plano prieš išpuolius neturėjimas, nors ir 32 % pasitelkė reikiamas priemones atakai užkirsti[9]. Galima daryti išvadą, kad net įmonėse, kuriose dirba kompetentingi informacinių technologijų sričių atstovai, negali būti visiškai užtikrinta duomenų apsauga. Tad vartotojas, kaip asmuo, neturintis specialių žinių, šioje situacijoje yra itin pažeidžiamas ir tokia naršyklė kaip Firefox suteikia papildomą apsaugos lygį.

Dabar naudojant Firefox naršyklę, vartotojams yra suteikiamos trys galimybės, kuriomis yra tiksliai sureguliuojami svetainėse vyraujantys slapukai: standartinė, griežta ir įprasta. Standartiškas pasirinkimas reiškia, jog iš pradžių užblokuoti žinomi trečiųjų šalių stebėjimo prietaisai yra tik asmeninio naršymo režimu, tačiau įsivyravus „Firefox 69", numatytasis nustatymas apėmė ir privataus, ir standartinio naršymo režimus. Tai reiškia, kad Firefox patobulinta stebėjimo apsauga veikia visiems vartotojams, blokuodama trečiųjų šalių stebėjimo ir kriptografinius įrenginius. Verta paminėti ir tai, jog Mozilla išbandė šį nustatymą naujoms naršyklės diegimo programoms jau 2019 m. birželio mėn. Griežtasis pasirinkimas blokuoja visus žinomus stebėjimo prietaisus, trečiųjų šalių stebėjimo prietaisus, kriptografus ir pirštų atspaudus visuose languose. Vartotojai, naudojantys įprastą naršyklę, tikslina savo privatumo nustatymus, tačiau tai gali reikšti, kad svetainės gali tinkamai neveikti. Tokiu būdu yra sustabdomas daugelio rūšių stebėjimas reklamos ar rinkodaros tikslais.

Anot Marissos Wood, „Mozilla" produkto viceprezidentės[10], šiuo metu daugiau nei 20% Firefox vartotojų yra įsijungę šią patobulintą stebėjimo apsaugą. Naudojant naršyklę, yra numatoma 100% vartotojų apsauga pagal jų pačių numatytus nustatymus ir veikia taip, jog nebūtų sudaromas interneto naudotojo profilis pagal naršymo elgesio stebėjimą, kuris yra galimas net ir tada, kai vartotojas neduoda sutikimo. Patobulinta stebėjimo apsauga padeda sušvelninti šią grėsmę ir vėl leidžia valdyti internetinę patirtį pačiam vartotojui.

---

[9] Adeya. Why is encrypted communications important in the workplace? [interaktyvus]. Prieiga per internetą: https://adeya.ch/why-is-encrypted-communications-important-in-the-workplace/ [žiūrėta 2021 m. sausio 31 d.].

[10] Dennis Fisher. *Firefox now blocks third-party cookies by default* [interaktyvus]. Prieiga per internetą: https://duo.com/decipher/firefox-now-blocks-third-party-cookies-by-default [žiūrėra 2021 m. vasario 10 d.].

Apibendrinant šias „Firefox 69" galimybes, galima teigti, jog numatytieji nustatymai daro didelį ir neigiamą poveikį visoms skaitmeninės reklamos bei rinkodaros pramonės įmonėms, nes tai apsunkina elgesio skelbimų taikymą, dažnumo ribos nustatymą, vertinimą ir priskyrimą.

2.2. Safari

Nors Microsoft Edge naršyklė jau pradėjo blokuoti trečiųjų šalių slapukus, o Google Chrome įsipareigojo juos visiškai blokuoti iki 2022 m., vis dėlto Safari yra pirmoji pagrindinė naršyklė, kuri pagal numatytuosius nustatymus blokuoja visus trečiųjų šalių slapukus. Šie veiksmai, kuriais daugiausia dėmesio yra skiriama vartotojo privatumui, tęsiasi kelerius metus nuo „Intelligent Tracking Prevention" (liet. *Pažangi stebėjimo prevencija*) (toliau – ITP) išleidimo, dar kitaip žinomos kaip privatumo funkcijos, pristatytos 2017 m. rugsėjo mėn.

Trečiųjų šalių slapukai buvo labai svarbūs ir tam tikra prasme vis dar yra reikšmingi formuojant skaitmeninės reklamos ekosistemą. Reklamuotojai, leidėjai ir technologijų kompanijos jais remiasi norėdami gauti pajamų iš vartotojų. Remiantis tuo, jog pagal numatytuosius nustatymus Safari blokuoja trečiųjų šalių slapukus, reklamuotojai negali tinkamai įgyvendinti skelbimų dažnio valdymo ir ribojimo, pakartotinio taikymo ar peržiūros priskyrimo modeliavimo. Nepaisant to, Safari vartotojai vis tiek matys skelbimus, tačiau jie bus netinkamai taikomi, neaktualūs ir greičiausiai kartosis per dažnai. Tad galima daryti prielaidą, jog šie laipsniški Safari žingsniai siekiant visiško trečiųjų šalių slapukų atsisakymo turi svarbų pagrindą – Apple kompanija yra itin susirūpinusi dėl savo vartotojų privatumo.

John Wilander, Apple inžinierius bei atsakingas asmuo už ITP[11], tikina, jog yra trys pagrindinės priežastys, kurios trečiųjų šalių slapukų atsisakymą paverčia itin reikšmingu bei svarbiu kompanijos žingsniu. Pirmiausia, nepaisant fakto, jog tokios technologijos kaip Tor ar Brave trečiųjų šalių slapukų blokavimą pavertė pranašumu prieš kitas interneto naršykles, Safari tai taip pat galėtų pasiekti ir turėtų nemažą žiniatinklio srautą. Be to, pasidalintų savo gauta patirtimi dėl visiško trečiųjų šalių slapukų blokavimo ir padėtų kitoms naršyklėms žengti šį didelį žingsnį. Antra, nebebūtų aktyvus prisijungimas naudojant piršto antspaudus, nes naršant internetiniame puslapyje, šis gali be vartotojo sutikimo aptikti paskyras, prie kurių asmuo yra prisijungęs. Toks vartotojo informacijos nutekinimas yra galimas bet kurioje svetainėje, jei yra įgalinami trečiųjų šalių slapukai – net saugioje naršyklėje, asmuo niekada negali būti tikras, jog jo duomenys yra saugūs. Tad šis „sausainėlių" blokavimas taptų itin svarbiu naršyklės žingsniu,

---

[11] Ted Vrountas. *Apple's Safari: The Latest Browser Blocking Third-Party Cookies & What It Means for Advertisers* [interaktyvus]. Prieiga per internetą: https://instapage.com/blog/safari-blocking-cookies [žiūrėta 2021 m. sausio 3 d.].

kuriuo būtų garantuojamas didesnis vartotojo duomenų saugumas. Trečia, visiškas trečiųjų šalių slapukų atsisakymas panaikina reikiamybę svetainėms turėti įsimenamąją paslaugą dėl slapukų blokavimo. Tai reiškia, jog internetiniams puslapiams nebeliktų reikiamybės įsiminti, ar vartotojas leidžia svetainėje naudoti slapukus. Tad apibendrinat galima daryti išvadą, jog trečiųjų šalių slapukų atsisakymas yra ne tik svarbus Apple kompanijos žingsnis, bet ir itin reikalingas siekiant sukurti internetą be slapukų. Tokiu būdu būtų sukurta saugesnė erdvė internete vartotojams bei garantuotas jų privatumas.

Bendrąja prasme, šie pokyčiai blokuojant trečiųjų šalių slapukus, yra Safari tiesioginė reakcija į naujas saugumo spragas, problemų sprendimo būdus, agresyvų stebėjimą ir šešėlinius verslo metodus. Saugumo funkcijų diegimas ir didinimas siekiant apsaugoti vartotojų privatumą nėra naujiena ir tai tęsiasi jau ne vienerius metus, tačiau kiekvienu atveju didžiausias laimėtojas ir naudos gavėjas yra bei bus vartotojas.

2.3. Google

Google – tai viena iš didžiausių kompanijų, kuri turi pačią didžiausią įtaką šiandieninėje rinkoje. Ne paslaptis, kad Google turi ilgalaikę monopolinę galią bendrosios internetinės paieškos rinkoje. Pavyzdžiui, 2019 metais Google pranešė, kad visos pajamos siekia 160,7 mlrd. USD – 45% daugiau nei 2017 m. – ir daugiau nei 33 mlrd. USD grynųjų pajamų[12]. Tai rodo jos galią bei pirmumą prieš kitas korporacijas, kurios siekia užimti jos vietą. Galima teigti, kad Google išlieka lyderiaujanti kompanija net ir prieš tokias dideles „gigantes" kaip Apple. Pavyzdžiui, Google, siekdama užkariauti internetines paieškos sistemas ne tik kompiuteriuose, bet ir mobiliuosiuose įrenginiuose, moka Apple[13]. Ji tą daro tam, kad internetinė paieškos sistema iš karto nukreiptų į Google paiešką, nors ir vartotojas, norėdamas apsilankyti svetainėje pirmus veiksmus atlieka ne su Google programėlės pagalba, bet per Safari. Dėl šios priežasties ne veltui sakoma, kad panaikinus trečiųjų šalių slapukus Google nukentės mažiau nei kitos įmonės, kadangi, turėdama savo rankose tiek monopolijos, ji valdys rinką. Piktnaudžiaudama jau dabar turima savo galia, Google buvo perėmusi slapukų surinktą informaciją iš trečiųjų šalių įmonių[14]. Šioms, neturint kito veiksmingo pasirinkimo bei atsižvelgus į dominavimą rinkoje, neliko kitos išeities kaip tik leisti pasisavinti neteisėtai įgytą informaciją. Tokiu būdu, Google pasinaudojo savo viršenybe pasitelkdama kitų įmonių investicijas ir jų taikomas naujoves. Tad tai tik įrodo, jog kiti paieškos paslaugų teikėjai negalės pasiekti vartotojų duomenų plačiu mastu, o Google, kaip šių duomenų saugotoja, turės

---

12 Subcommittee on antitrust commercial and administrative law of the committee on the judiciary. *Investigation of competition in digital markets* [interaktyvus]. Prieiga per internetą: https://www.nytimes.com/interactive/2020/10/06/technology/house-antitrust-report-big-tech.html [žiūrėta 2021 m. sausio 3 d.].

13 Žiūrėti išnašą Nr. 12

14 Žiūrėti išnašą Nr. 12

viršenybę prieš silpnesnius rinkos dalyvius. Todėl galima teigti, jog slapukų mirtis šią „milžinę" paveiks netgi teigiamai.

2020 metų sausio 14 dieną Google priėmus sprendimą atsisakyti trečiųjų šalių slapukų, kilo klausimas, kokių alternatyvų bus imtasi, kadangi, panaikinus šią technologiją, asmenų teikiamų duomenų poreikis vis tiek išliks. Nors Firefox bei Safari nieko nelaukiant ėmėsi būdų siekiant blokuoti trečiųjų šalių slapukus, Google pareiškė, kad, kol nebus tinkamos bei aiškios alternatyvos šiai technologijai, tol Chrome jie bus naudojami[15]. Dėl šios priežasties Google pasiūlė keletą būdų, kurie galėtų ilgainiui pakeisti slapukus. Pirmoji Google pasiūlyta alternatyva – „Privacy Sandbox" (žiniatinklio naršyklė API) (angl. *web browser APIs*). Tai reiškia naują duomenų mainų būdą internete, kai reklamuotojas turi „paskambinti" API, kad gautų tam tikrą informaciją apie turinčią panašių interesų vartotojų grupę, o ne atskirą asmenį, atlikusį tam tikrą veiksmą. Tai parodo, kad „Privacy Sandbox" suteiks galimybę reklamuotojams bei skelbimų įmonėms naudotis pačios naršyklės duomenimis, nepažeidžiant vartotojų privatumo. Visgi, nors procesas sprendžia privatumo problemą, tačiau tai taip pat labai apribos galimybę pasiūlyti pritaikymą vartotojui arba 1:1 patirtį, kurios daugelis vartotojų tikisi iš savo mėgstamų prekės ženklų[16], kadangi nebus atsižvelgta į atskiro asmens norus.

Antra, Google siekia, kad trečiųjų šalių slapukai būtų prieinami per HTTPS protokolą, kadangi tai užkerta kelią konfidencialių duomenų atskleidimui. Jis padeda užtikrinti serverio saugumą bei tikrumą ir tokiu būdu lankytojo kompiuterio serveriui siunčiama informacija yra suprantama tik šiems dalyviams ir tuo pat metu yra šifruojama. Tai ne tik garantuotų saugesnį internetą, bet ir leistų pačiam vartotojui tiksliai nustatyti svetainėje esančius slapukus.

Trečia, norima vėl imti naudoti kontekstinį taikymą (angl. *contextual targeting*), kuris užtikrina, jog svetainėje rodomi skelbimai atitiktų lankytojų auditoriją. Jis gali būti pagrįstas konkrečia svetaine, kanalu, puslapio tipu ar raktiniais žodžiais. Pasak „Marketing Land", „taikant pagal kontekstą, jūsų matomi skelbimai yra rodomi pagal jūsų žiūrimą turinį, o ne jūsų bendrą elgesio profilį. Taigi, žiūrėdami į savo mezgimo tinklaraštį, matote mezgimo adatų skelbimus, o kai skaitote, kaip padidinti paspaudimų rodiklį el. Pašto naujienlaiškiuose, matote atitinkamų el. Pašto automatizavimo platformų skelbimus[17]". Taigi ši technologija prisidės prie vartotojų saugumo internete užtikrinimo, kadangi trečiosios šalys nebežinos svetainių lankytojų naršymo istorijos.

---

15 Ubex AI. *Google Aims To Cancel Support For Third-Party Cookies In Chrome Browser Over The Next Two Years* [interaktyvus]. Prieiga per internetą: https://medium.com/ubex/google-aims-to-cancel-support-for-third-party-cookies-in-chrome-browser-over-the-next-two-years-973ca47945a [žiūrėta 2021 m. sausio 4 d].

16 Daniel Heer. *It's Finally Over for the 3rd Party Cookie - What Now?* [interaktyvus]. Prieiga per internetą:https://www.martechadvisor.com/articles/ads/its-finally-over-for-the-3rd-party-cookie-what-now/ [žiūrėta 2021 m. sausio 4 d.].

17 Theodore F. Claypoole (2020). Toss Out the Milk, The Cookie Party is Over. *The National Law Review*, Volume X, Number 182, p. 1-3 [interaktyvus]. Prieiga per internetą: https://www.natlawreview.com/article/toss-out-milk-cookie-party-over [žiūrėta 2021 m. vasario 13 d.].

3. Trečiųjų šalių slapukų reguliavimas Europos Sąjungos kontekste

3.1. Europos Sąjungos kompetencija duomenų apsaugos srityje

Visų pirma, reikia aptarti Europos Sąjungos (toliau – ES) kompetenciją duomenų apsaugos teisės srityje. ES, bendradarbiaudama su valstybėmis narėmis, užtikrina pagrindinių šių teisių apsaugą. Remiantis sutarties dėl Europos Sąjungos veikimo[18] (toliau – SESV) 16 straipsnio 1 dalimi bei Pagrindinių teisių chartijos[19] 8 straipsnio 1 dalimi matyti, kad ES turi išskirtinį vaidmenį pagrindinių teisių apsaugoje, kuris įtvirtintas SESV 16 straipsnio 2 dalyje.

Atkreiptinas dėmesys, kad viena iš ES sričių yra reglamentų priėmimas. Svarbu išskirti Bendrąjį duomenų apsaugos reglamentą, kuriame reglamentuojama duomenų apsauga, kaip turi būti renkami bei tvarkomi asmens duomenys[20]. Šios kompetencijos teisinis pagrindas įtvirtintas sutarties dėl Europos Sąjungos veikimo 16 straipsnyje. Jis įtvirtina Europos Parlamento bei Tarybos teisę nustatyti fizinių asmenų apsaugos Sąjungos institucijoms, įstaigoms ir organams bei valstybėms narėms tvarkant asmens duomenis, kai vykdoma veikla yra susijusi su Sąjungos teisės taikymo sritimi, taisykles ir laisvo tokių duomenų judėjimo taisykles[21]. Ši nuostata reiškia, kad ES turi kompetenciją priimti teisės aktus, kurie reguliuotų ne tik tokias nuostatas, kurios yra tiesiogiai reglamentuojamos BDAR, bet ir nurodytų taisykles, įtvirtinančias duomenų valdytojo pareigą tvarkant slapukus. Tai įrodo Europos Sąjungos Teisingumo teismo sprendimas byloje Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV prieš Planet49 GmbH[22], kurioje išaiškinta, kad interneto svetainės naudotojo galiniame įrenginyje saugoma arba naudojama informacija yra asmens duomenys.

Be to, svarbu išskirti Europos Sąjungos teisėkūros aktą – Europos Parlamento ir Tarybos direktyvą 2002/58/EB (Direktyva dėl privatumo ir elektroninių ryšių). Joje įtvirtinti reikalavimai, kurių turi laikytis duomenų valdytojai naudodami slapukus savo internetinėse svetainėse. Pavyzdžiui, nurodyti privatumo politikos (angl. *privacy*

---

18 Sutartis dėl Europos Sąjungos veikimo. OL C 202, p. 1, 16 str.

19 Europos Sąjungos pagrindinių teisių chartija. OL C 202, p. 389, 8 str.

20 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas). OJ L 119, p. 1

21 Sutartis dėl Europos Sąjungos veikimo, 16 str.

22 *Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband eV prieš Planet49 GmbH* [ESTT], Nr. C-673/17, [2019-10-01]. ECLI:EU:C:2019:801

police), slapukų politikos, iššokančio pranešimo (angl. *pop-up notification*), aktyvaus vartotojo sutikimo būtinybė. Nesilaikant šių privalomų reikalavimų gali būti taikoma atsakomybė už tokį pažeidimą. Be to, nesivadovaujant šiomis direktyvoje įtvirtintomis nuostatomis, kyla vartotojų nepasitikėjimas interneto puslapiu, kuris pasižymi mažesniu vartotojų įsitraukimu ar galiausiai jų praradimu.

3.2. Europos Sąjungos valstybių vaidmuo taikant Europos Sąjungos teisę

Išsiaiškinus ES kompetenciją reguliuojant slapukus bei šiai technologijai taikomus reikalavimus, svarbu išskirti, kaip ES valstybės tai įgyvendina savo jurisdikcijos ribose. ES narės turi laikytis visuotinai taikomų reglamentų bei įgyvendinti tiesioginį vertikalų veikimą turinčias direktyvas. Pavyzdžiui, BDAR yra privalomas visoms valstybėms narėms bei tiems juridiniams ar fiziniams asmenims, kurie savo veikloje tvarko asmens duomenis. Nesilaikant reglamente įtvirtintų reikalavimų, taikoma atsakomybė bei skiriamos sankcijos, kurių dydžiui gali turėti įtakos Europos Komisija, kuri, remiantis SESV 258 straipsniu, tiria pažeidimus dėl šio įsipareigojimo nevykdymo, pareikšdama pagrįstą nuomonę valstybei narei bei suteikdama galimybę išdėstyti savo pastabas[23]. Be to, ši ES institucija taip pat užtikrina tinkamą direktyvų įgyvendinimą, kuris reikšmingas siekiant Europos Sąjungos tikslų.

Svarbu paminėti e. Privatumo direktyvą. Siekiant ją įgyvendinti, vienas iš būdų yra priimti naują teisės aktą, kuris įtvirtintų ES siekius. Puikus pavyzdys yra Prancūzija, kuri, pasitelkdama teisėkūrą, išleido tokio pobūdžio dokumentą (angl. *French Data Protection Act*), kuriuo remiantis buvo priimtas sprendimas byloje Google LLC ir Google Ireland Limited prieš CNIL[24]. Jame buvo pripažintas pažeidimas Prancūzijos atžvilgiu dėl to, kad nebuvo prašomas vartotojų sutikimas prieš pradedant naudoti reklaminius slapukus, nebuvo vartotojams pateikiama informacija apie slapukų naudojimą bei nebuvo įdiegtas atsisakymo mechanizmas, kuriuo galėtų pasinaudoti internetinių puslapių lankytojai. Be to, sprendime buvo išaiškintas ir bylos teismingumo klausimas. Nors Google LLC bei Google Ireland Limited tvirtino, kad Prancūzijos įstatymas negali būti taikomas šioje byloje, kadangi turėtų būti taikomas BDAR bendradarbiavimo mechanizmas (žinomas kaip vieno langelio mechanizmas), o CNIL nėra pagrindinė jų priežiūros institucija taikant šį mechanizmą ir jų slapukų naudojimo praktika nepatenka į teritorinę Prancūzijos duomenų apsaugos įstatymo taikymo sritį. Buvo tvirtinama, kad turėtų būti taikomi Airijos įstatymai (Google siekė įrodyti, kad turėtų būti taikomas vieno langelio principas, kadangi jos filialas yra įsteigtas Airijoje. Teigta, jog Google

---

23 Sutartis dėl Europos Sąjungos veikimo, 258 str.

24 *GOOGLE LLC et GOOGLE IRELAND LIMITED v. CNIL* [CNIL], No. SAN-2020-012, [7-12-2020].

Ireland Limited yra tikroji Google būstinė Europoje. Dėl šios priežasties tvirtinta, jog Airijos duomenų apsaugos komisaras turėtų būtų vienintelė kompetentinga priežiūros institucija, galinti nagrinėti ginčą), tačiau visgi buvo pripažinta, kad turi būti taikomas Prancūzijos teisės aktas, kadangi šios valstybės piliečiai naudojasi Google internetinėmis svetainėmis. Taigi šiuo atveju buvo taikyta *lex specialis* taisyklė (*lex specialis derogat legi generali)*, todėl galima teigti, kad direktyva yra reikšmingas teisės aktas, kurį įgyvendinus valstybėse narėse, siekiama užkirsti kelią asmens duomenų apsaugos pažeidimams, kurie dažnai kyla naudojant trečiųjų šalių slapukus.

3.3. Elektroninių ryšių reguliavimo problematika

Svarbu išskirti tai, kad e. Privatumo direktyvos, reguliuojančios elektroninius ryšius, taikymui iškilo keletas reikšmingų problemų. Šios direktyvos keliama problematika sukėlė stimulą siekti, jog šis dokumentas būtų pakeičiamas visuotinai taikomu reglamentu. Pasiūlymas dėl e. Privatumo reglamento projekto yra pagrindinis žingsnis, kuriuo norima reguliuoti slapukus bei kitus elektroninius ryšius. Todėl būtina įvardinti, kokios šio sprendimo priežastys bei galimi rezultatai.

Pirmiausia, manoma, kad BDAR nėra pakankamas teisinis instrumentas, kuris galėtų reguliuoti asmens duomenų apsaugą elektroniniame sektoriuje. Šio reglamento pagrindinis tikslas nėra apsaugoti teisę į ryšių konfidencialumą, jame išreikštos abstrakčios normos, kurios nėra visiškai atitinkančios siekį sureguliuoti šią sferą. Taip pat reglamente aiškiai neaptariamos programine įranga paremtų aplikacijų paslaugų teikėjų teikiamos tiesioginės rinkodaros paslaugos, siunčiamos naudojant VoIP technologiją[25]. Pavyzdžiui, vartotojas savo sutikimu suteikdamas leidimą paslaugų teikėjui siųsti reklamos skelbimus į lankytojo elektroninio pašto dėžutę turi teisę bet kuriuo metu atšaukti savo patvirtinimą ir toks siekis eksplicitiškai nurodytas pasiūlyme dėl e. Privatumo reglamento projekto.

Antra, tikima, kad iki šiol nėra užtikrinta veiksminga bei būtina teisių apsauga, kadangi sutinkama problemų, kurių sprendimas nėra niekur įtvirtintas. Pavyzdžiui, nesant priimto reglamento, vis dar nėra tinkamai sureguliuotos naujos kartos naujovės kaip Netflix, Viber ar Whatsapp. Šiuo metu galiojanti Sąjungos elektroninių ryšių sistema, įskaitant E. privatumo direktyvą, joms apskritai netaikoma[26]. Žinant tai, kad šis reglamentas turėtų būti taikomas elektroninių ryšių duomenims, kurie tvarkomi teikiant ir naudojant elektroninių ryšių paslaugas Sąjungoje, nepriklausomai nuo to,

---

[25] Markevičius, E. (2019). E. Privatumo direktyvos įgyvendinimo problemos ir jų sprendimai e. Privatumo reglamento projekte. *Teisė,* 113, 139-154.

[26] Pasiūlymas EUROPOS PARLAMENTO IR TARYBOS REGLAMENTAS dėl teisės į privatų gyvenimą ir asmens duomenų apsaugos elektroninių ryšių sektoriuje, kuriuo panaikinama Direktyva 2002/58/EB (Reglamentas dėl privatumo ir elektroninių ryšių).

ar duomenys tvarkomi Sąjungoje[27], galima teigti, jog ateityje priimtu dokumentu turės vadovautis ir tokios naujos technologijos, kurioms reikalingi vartotojų duomenys.

Trečia, keliama problema, susijusi su vidaus rinkos pokyčiais. Pasiūlyme dėl e. Privatumo reglamento projekto nurodoma, kad direktyva ne visiškai atitinka technologijų pokyčius ir tikrąją padėtį rinkoje, todėl reali elektroninių ryšių privatumo ir konfidencialumo apsauga yra nenuosekli arba nepakankama[28]. Vis tobulėjantys šiuolaikinio skaitmenizavimo procesai, lemiantys įrenginių naudotojų vartotojiškumą, tapo tinkamai nebereguliuojami direktyvos taikymo mastu. Valstybės, kurios priima įgyvendinimo aktus, neretai įtvirtina skirtingą teisinį reguliavimą, kuris nėra tapatus visose ES narėse. Tai lemia rinkos nenuoseklumą, kuris daro neigiamą poveikį Europos Sąjungos vidaus rinkos plėtrai bei skaidrumui ir sukelia problemų ūkio subjektams, kuriems tapo sunku vykdyti vienodą tarpvalstybinę veiklą.

Apibendrinus pagrindines priežastis, kodėl siekiama priimti tiesioginio veikimo reglamentą, galime išskirti pagrindines problemas: valstybių narių piliečių privatumas ir konfidencialumas ryšių srityje nėra visiškai užtikrintas; valstybių narių piliečiai nėra efektyviai apsaugoti nuo neužsakytų pranešimų (angl. *spam*); ūkio subjektai susiduria su kliūtimis ir nebūtinomis išlaidomis dėl neaiškaus, fragmentiško ir pasenusio teisinio reguliavimo[29]. Visgi manoma, kad šie sunkumai išnyks, priėmus e. Privatumo reglamentą, kuris apims visas netinkamai reguliuojamas ar išvis nereguliuojamas sritis, kurios taip pat bus svarbios ir ateityje.

4. Trečiųjų šalių slapukų poveikis verslo ekosistemai

4.1. Dabartinio verslo iššūkiai diegiant slapukus

Šiandieninės aktualijos rodo, kad trečiųjų šalių slapukai turi didelę reikšmę ne tik didžiosioms pasaulinės rinkos „milžinėms", kurios tarytum valdo visą ekosistemą, bet ir daro įtaką smulkiosioms įmonėms, kurioms taip pat „sausainėliai" yra būtinas komponentas siekiant pagrindinių rinkodaros tikslų. Visgi naudojant trečiųjų šalių slapukus kyla problemų bei neaiškumų siekiant, kad ši technologija atitiktų teisės aktų reikalavimus. Pavyzdžiui, atlikus REFIT (Reglamentavimo kokybės ir rezultatų programa) vertinimą nustatyta, kad galiojančios e. Privatumo direktyvos tam tikrų nuostatų redakcija ir teisinių sąvokų dviprasmybė buvo kliūtis suvienodinti praktiką, todėl įmonėms kilo sunkumų vykdant tarpvalstybinę veiklą[30].

---

27 Žiūrėti išnašą Nr. 26

28 Žiūrėti išnašą Nr. 26

29 Europos Komisijos užsakymu atlikta direktyvos 2002/58 įvertinimo ir peržiūros galutinė ataskaita, p. 230 [inter aktyvus. Prieiga per internetą: http://ec.europa.eu/newsroom/document.cfm?doc_id=41232 [žiūrėta 2021 m. vasario 1 d.].

30 Žiūrėti išnašą Nr. 26

Be to, remiantis vertinimo rezultatais, dėl kai kurių direktyvos[31] nuostatų įmonėms ir vartotojams atsirado nereikalinga našta. Pavyzdžiui, galinių įrenginių konfidencialumui užtikrinti skirtos sutikimo taisyklės tikslai nepasiekti, nes galutiniams paslaugų gavėjams tenka atsakyti į prašymus leisti naudoti ilgalaikius slapukus, nors jie ir nesupranta tokių slapukų prasmės, o kai kuriais atvejais slapukai išsaugomi netgi be jų sutikimo. Sutikimo taisyklės taikymo sritis yra pernelyg plati, nes ta taisyklė taikoma ir veiklai, kuri nedaro poveikio privatumui, ir kartu per siaura, nes į jos taikymo sritį nėra aiškiai įtrauktos tam tikrų rūšių sekimo priemonės (pavyzdžiui, įrenginių identifikavimas), kurios nebūtinai turi būti susijusios su prieiga prie duomenų arba jų saugojimu įrenginyje. Pagaliau, laikytis tokios taisyklės įmonėms gali būti brangu[32].

Sekantis iššūkis su kuriuo susiduria dabartiniai verslininkai – tai vartotojų nenoras priimti slapukus. Europos Sąjunga reikalauja, kad internetinių puslapių lankytojai duotų aktyvų sutikimą, kad svetainėje būtų naudojami slapukai. Visgi neretai vartotojai neatlieka šio veiksmo, todėl tokiu atveju verslas neturi teisės naudoti slapukus. Taigi kyla viena iš pagrindinių problemų – negaunama „sausainėlių" teikiama nauda. Kiekvienam verslininkui yra svarbu žinoti, ko nori vartotojai, kad galėtų nuspręsti, kokia kryptimi vystyti savo veiklą. Jeigu tokios informacijos jis negauna, šį tikslą pasiekti tampa kur kas sudėtingiau.

4.2. Ateitis ir sprendimo būdai

Nors Google ir yra nurodžiusi, jog įmonės gali naudoti slapukus tuo atveju, jei jie yra tinkamai administruojami, vis dėlto tai nereiškia, jog reklamuotojams neteks ieškoti naujų strategijų, pakeičiančių trečiųjų šalių slapukų teikiamą naudą. Jau šiuo metu didžioji dauguma rinkodaros bendruomenės narių dalinasi abejonėmis ir baimėmis. Daugelis sutinka, jog trečiųjų šalių slapukų atsisakymas buvo neišvengiamas sprendimas, tačiau kiti baiminasi, kad tai gali turėti itin svarbią įtaką dabar vyraujančiai skaitmeninės reklamos aplinkai. Ir nors yra tikinama, jog įmonės palaiko vartotojų privatumą, tačiau dėl šio teigimo atsiranda vis daugiau pagrįstų abejonių, nes būtent tai yra neatsiejama kompanijų dalis, į kurią yra investuojamos didelės įmonės lėšos. Tad kyla pagrįsti nuogąstavimai apie galimas pasekmės verslui įsigaliojus sprendimui atsisakyti „sausainėlių" bei sprendimo būdus, kurie būtų ir naudingi, ir teiktų reikiamą informaciją apie vartotojo elgesį internete.

Trečiųjų šalių slapukų atsisakymas buvo viena iš labiausiai nuspėjamų skaitmeninės rinkodaros tendencijų pastaraisiais metais. Tad ne veltui buvo pradėta kurti naujas strategijas dar prieš įsigaliojus Google sprendimui. Ne išimtis ir verslas, kuris užsiima

---

[31] 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių). OJ L 201, p. 37

[32] Žiūrėti išnašą Nr. 26

prekyba ar teikia paslaugas, kurios yra jam skirtos. Viena žinomiausių didmeninės prekybos sistemų yra B2B (angl. *business to business*) (liet. *verslas verslui*). Tai bendradarbiavimas tarp dviejų ar daugiau įmonių tiekiant vieni kitiems prekes, paslaugas ar informaciją[33]; verslo modelis, kuriam taip pat šiuo metu yra sunkių sprendimų metas siekiant sėkmingai įgyvendinti naujus sprendimus, pakeičiančius slapukų teiktą naudą. Viena svarbiausių sričių, į kurią pirmiausia yra telkiamas dėmesys, tai optimizavimo paieškos sistemos (angl. *Search Engine Optimization) (toliau – SEO)*, dar kitaip jos yra suprantamos kaip procesas, kurio tikslas yra padidinti vartotojų srautą svetainėje iš Google organinės paieškos. Kai vartotojas ieško konkretaus raktinio žodžio ar raktinių žodžių grupės, susijusios su verslu, įmonių svetainės, užsiimančios tokia veikla, bus pirmiausiai pastebimos paieškos sistemoje. Tad galima daryti išvadą, jog didžiausia nauda yra gaunama tuomet, kai svetainė yra optimizuojama pagal didelės apimties, labai tikslius raktinius žodžius, neatsižvelgiant į savo prekės ženklo pavadinimą. Tokiu būdu yra sutelkiamas dėmesys į natūralų, nemokamą vartotojų srautą pagal specifinius terminus, kuriuos į Google įveda vartotojai. Antrasis sprendimas, kuris taip pat reikalauja ypatingo įmonių dėmesio, tai laikymasis holistinio požiūrio dėl skaitmeninės rinkos. Tai reiškia, jog po truputį atsisakant trečiųjų šalių slapukų, B2B įmonės turi pažvelgti į internetinę reklamą visapusiškiau ir objektyviau: įsitraukti į socialinę žiniasklaidą, nuosekliai kurti prekės ženklą, racionaliai būti internete atlaikant vis labiau kintantį mokamos reklamos kraštovaizdį. Tad ši įvairi strategija užtikrintų, jog jei viena skaitmeninės rinkodaros plano dalis nukentėtų nuo tam tikrų išorinių veiksmų (kaip šiuo atveju, kai yra pašalinami trečiųjų šalių slapukai), tai neturėtų neigiamos įtakos prekės ženklo naudojimui ar kitoms sritims. Apibendrinant galima įžvelgti, jog galimų ir sėkmingų sprendimų būdų, kurie būtų įgyvendinti po trečiųjų šalių slapukų pašalinimo, iš tiesų yra. Kiekvienas verslas gali pasirinkti skirtingą kelią, kuriuo siektų pritraukti vartotoją, tačiau visi jie būtų vienu ar kitu atveju naudingi ir nešantys pelną.

Neišvengiama verslo dalis yra klientas ar fizinis asmuo. Tarp jų atsiranda ryšys tiekiant ar parduodant paslaugas, prekes, informaciją. Šis bendradarbiavimas reprezentuoja ir verslo sistemą B2C (angl. *business to consumer*) (liet. *verslas klientui*) – tai viena populiariausių ir plačiausiai žinomų pardavimo priemonių. Bet koks verslas, kuris remiasi B2C pardavimais, turi palaikyti gerus santykius su savo klientais, kad užtikrintų jų teigiamus atsiliepimus apie teiktas paslaugas ar kt. Verta paminėti ir tai, jog skirtingai nei „verslas verslui“, kurių rinkodaros kampanijos skirtos produkto ar paslaugos vertei parodyti, įmonės, besiremiančios B2C, savo klientams turi sukelti emocinį atsaką į savo rinkodarą – tai lemia ir gero klimato palaikymą, ir puikius pardavimus[34]. Tačiau šie

---

[33] Dešiniojiranka.lt. *Kas yra B2b (verslas verslui)?* [interaktyvus]. Prieiga per internetą: http://desiniojiranka.lt/kas-yra-b2b-verslas-verslui/ [žiūrėta 2021 m. sausio 12 d.].

[34] Will Kenton. *Business to Consumer (B2C)* [interaktyvus]. Prieiga per internetą: https://www.investopedia.com/terms/b/btoc.asp [žiūrėta 2021 m. sausio 14 d.].

modelių skirtumai nelemia fakto, jog trečiųjų šalių slapukų pašalinimas nepaveiks ir B2C. Kadangi vartotojų pasitikėjimas prekės ženklu visuomet buvo didžiausia įmonės siekiamybė, svarbu, jog toks tikslas būtų palaikomas ir toliau. O šiuo atveju, panaikinus „sausainėlius", naujų priemonių įgyvendinimas bei žingsnis link pirmosios šalies slapukų strategijos galiausiai vartotojus paskatins dar labiau pasitikėti įmone. Tai gali būti įgyvendinta praturtinant pirmosios šalies duomenimis, remiantis žmonių, teikiančių duomenis, pasiūlymais bei antrosios šalies teikiama informacija. Tad galima daryti išvadą, jog B2C verslo modeliui trečiųjų šalių slapukų pašalinimas gali atnešti itin teigiamos naudos. Tačiau įmonės turi naudoti naujus duomenų rinkimo metodus, kad paskatintų vartotojus teikti informaciją – klientai turi suprasti, kodėl jie pateikia rinkodaros specialistams savo duomenis.

Tikinama, jog trečiųjų šalių slapukų pašalinimas yra tik vienas iš pirmųjų Google žingsnių, kuriuos įgyvendins artimu metu. Vienu svarbiausiu klausimu lieka tai, koks bus tikrasis poveikis skaitmeninės rinkodaros sričiai. Tad įmonės, kurios yra visiškai priklausomos nuo trečiųjų šalių slapukų, turėtų kuo greičiau įgyvendinti pokyčius: skirti dėmesį SEO, įvairinti rinkodaros sritį, praturtinti pirmosios šalies duomenimis savo strategiją. Ši kūrybos ir medijos kombinacija padėtų užmegzti prasmingus verslo santykius bei sudaryti aukštos kvalifikacijos potencialų klientų sąrašą.

Išvados

1. Trečiųjų šalių slapukus pakeis tokios naujos technologijos kaip „Privacy Sandbox", kontekstinis taikymas, Firefox įgyvendinta patobulinta apsaugos programa „Firefox 69", Safari išleista privatumo funkcija „Intelligent Tracking Protection", kurios tikimasi, jog suteiks stabilumo bei saugumo siekiant suteikti visapusišką teisę į duomenų apsaugą.
2. Europos Sąjunga turi išskirtinį vaidmenį duomenų apsaugos teisės srityje. BDAR bei e. Privatumo direktyvoje yra įtvirtinti pagrindiniai reikalavimai, kurių duomenų valdytojai turi laikytis naudodami slapukus. Tai padeda įgyvendinti Europos Sąjungos valstybės vadovaudamosi šiais teisės aktais tiriant duomenų apsaugos teisės pažeidimus. Šis bendradarbiavimas suteikia vartotojų teisių veiksmingą gynimą, kuris turės teigiamos įtakos ir po slapukų pabaigos, siekiant reguliuoti naujas technologijas.
3. Trečiųjų šalių slapukus pakeičiančios technologijos bus reguliuojamos ateityje priimtu e. Privatumo reglamentu, jeigu asmens duomenų apsaugos pažeidimai bus padaryti Europos Sąjungos piliečių atžvilgiu. Tokiu būdu bus užpildyta teisės spraga, vyraujanti šiomis dienomis, kadangi BDAR visapusiškai neapima elektroninių ryšių reguliavimo, kuris ateityje taip pat bus reikšmingas siekiant atitikti naujų technologijų teisėtumo reikalavimus.

4. Verslo įmonės yra priverstos ieškoti naujų strategijų, kurios pakeistų „sausainėlių" teikiamą naudą, siekiant, kad toliau galėtų būti rinkos dalimi. Viena iš strategijų, kuria galėtų vadovautis verslas – optimizavimo paieškos sistemos. Naudojant raktinius žodžius, būtų padidinamas vartotojų srautas svetainėje iš Google organinės paieškos. Kita alternatyva – holistinio požiūrio dėl skaitmeninės rinkos laikymasis tam, kad B2B įmonės pažvelgtų į internetinę reklamą visapusiškiau ir objektyviau bei galėtų lengviau prisitaikyti prie technologinių pokyčių. Tačiau trečiųjų šalių slapukų atsisakymas turės ir teigiamos reikšmės verslo įmonėms, kadangi šio sprendimo įgyvendinimas paskatins vartotojus labiau pasitikėti jomis.

Šaltinių sąrašas

Teisės norminiai aktai:

1. Europos Sąjungos sutartis. OL C 202, p. 1
2. Sutartis dėl Europos Sąjungos veikimo. OL C 202, p. 1
3. Europos Sąjungos pagrindinių teisių chartija. OL C 202, p. 389
4. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas). OJ L 119, p. 1
5. 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių). OJ L 201, p. 37
6. Pasiūlymas EUROPOS PARLAMENTO IR TARYBOS REGLAMENTAS dėl teisės į privatų gyvenimą ir asmens duomenų apsaugos elektroninių ryšių sektoriuje, kuriuo panaikinama Direktyva 2002/58/EB (Reglamentas dėl privatumo ir elektroninių ryšių).
7. LOI n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles

Specialioji literatūra:

1. Markevičius, E. (2019). E. Privatumo direktyvos įgyvendinimo problemos ir jų sprendimai e. Privatumo reglamento projekte. *Teisė,* 113, 139-154.
2. Theodore F. Claypoole (2020). Toos Out the Milk, The Cookie Party is Over. *The National Law Review*, Volume X, Number 182, p. 1-3 [online]. Available at: https://www.natlawreview.com/article/toss-out-milk-cookie-party-over [Accessed 13 February 2021].
3. Kulyk O. and others (2020). Has the GDPR hype affected users' reaction to cookie disclaimers? *Journal of Cybersecurity*, Volume 6, p. 1-14 [online]. Available at: https://academic.oup.com/cybersecurity/article/6/1/tyaa022/6046452?login=true [Accessed 10 February 2021].

Elektroniniai leidiniai:

1. Michal Wlosik, Michael Sweeney. *What's the Difference Between First-Party and Third-Party Cookies?* [interaktyvus]. Prieiga per internetą: https://clearcode.cc/blog/difference-between-first-party-third-party-cookies/?fbclid=IwAR1C9NtRzKxHuuI_agUgRvb_4Me-VOG-9ta80NaTwzNCV33pcMgpA6gvt42o [žiūrėta 2020 m. gruodžio 17 d.].
2. Chris Brook. *Almost 60,00 Post-GDPR Data Breaches Reportes in Europe* [interaktyvus]. Prieiga per internetą: https://digitalguardian.com/blog/almost-60000-post-gdpr-data-breaches-reported-europe [žiūrėta 2021 m. vasario 15 d.].
3. Global Web Index. *Global Ad-Blocking Behavior* [interaktyvus]. Prieiga per internetą: https://www.globalwebindex.com/hubfs/Downloads/Global_Ad-Blocking_Behavior.pdf [žiūrėta 2021 m. vasario 9 d.].
4. Hunton Andrews Kurth's Privacy and Cybersecurity (2020). Privacy and Information Security Law Blog, [blog] 14 December. Prieiga per internetą: https://www.huntonprivacyblog.com/2020/12/14/cnil-fines-google-and-amazon-135-million-euros-for-alleged-cookie-violations/ [žiūrėta 2021 m. sausio 20 d.].
5. Jeff Rajeck. *Why mapping the customer journey is so hard – and what you can do about it* [interaktyvus]. Prieiga per internetą: https://econsultancy.com/why-mapping-the-customer-journey-is-so-hard-and-what-you-can-do-about-it/ [žiūrėta 2021 m. sausio 14 d.].
6. Dennis Fisher. *Firefox now blocks third-party cookies by default* [interaktyvus]. Prieiga per internetą: https://duo.com/decipher/firefox-now-blocks-third-party-cookies-by-default [žiūrėra 2021 m. vasario 10 d.].
7. Ted Vrountas. *Apple's Safari: The Latest Browser Blocking Third-Party Cookies & What It Means for Advertisers* [interaktyvus]. Prieiga per internetą: https://instapage.com/blog/safari-blocking-cookies [žiūrėta 2021 m. sausio 3 d.].
8. Subcommittee on antitrust commercial and administrative law of the committee on the judiciary. *Investigation of competition in digital markets* [interaktyvus]. Prieiga per internetą: https://www.nytimes.com/interactive/2020/10/06/technology/house-antitrust-report-big-tech.html [žiūrėta 2021 m. sausio 3 d.].
9. Ubex AI. *Google Aims To Cancel Support For Third-Party Cookies In Chrome Browser Over The Next Two Years* [interaktyvus]. Prieiga per internetą: https://medium.com/ubex/google-aims-to-cancel-support-for-third-party-cookies-in-chrome-browser-over-the-next-two-years-973ca47945a [žiūrėta 2021 m. sausio 4 d].
10. Daniel Heer. *It's Finally Over for the 3rd Party Cookie - What Now?* [interaktyvus]. Prieiga per internetą: https://www.martechadvisor.com/articles/ads/its-finally-over-for-the-3rd-party-cookie-what-now/ [žiūrėta 2021 m. sausio 4 d.].
11. Theodore F. Claypoole (2020). Toss Out the Milk, The Cookie Party is Over. *The National Law Review*, Volume X, Number 182, p. 1-3 [interaktyvus]. Prieiga per internetą: https://www.natlawreview.com/article/toss-out-milk-cookie-party-over [žiūrėta 2021 m. vasario 13 d.].
12. Faktų apie Europos Sąjungą suvestinės. *Asmens duomenų apsauga.* [interaktyvus]. Prieiga per internetą: https://www.europarl.europa.eu/factsheets/lt/sheet/157/la-protection-des-donnees-a-caractere-personnel [žiūrėta 2020 gruodžio 30 d.].

13. Europos Komisijos užsakymu atlikta direktyvos 2002/58 įvertinimo ir peržiūros galutinė ataskaita, p. 230 [interaktyvus. Prieiga per internetą: http://ec.europa.eu/newsroom/document.cfm?doc_id=41232 [žiūrėta 2021 m. vasario 1 d.].
14. Dešiniojiranka.lt. *Kas yra B2b (verslas verslui)?* [interaktyvus]. Prieiga per internetą: http://desiniojiranka.lt/kas-yra-b2b-verslas-verslui/ [žiūrėta 2021 m. sausio 12 d.].
15. Will Kenton. *Business to Consumer (B2C)* [interaktyvus]. Prieiga per internetą: https://www.investopedia.com/terms/b/btoc.asp [žiūrėta 2021 m. sausio 14 d.].
16. Adeya. Why is encrypted communications important in the workplace? [interaktyvus]. Prieiga per internetą: https://adeya.ch/why-is-encrypted-communications-important-in-the-workplace/ [žiūrėta 2021 m. sausio 31 d.].

Teismų praktika:

1. *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV prieš Planet49 GmbH* [ESTT], Nr. C-673/17, [2019-10-01]. ECLI:EU:C:2019:801
2. *GOOGLE LLC et GOOGLE IRELAND LIMITED v. CNIL* [CNIL], No. SAN-2020-012, [7-12-2020].
3. *AMAZON EUROPE CORE v. CNIL* [CNIL], No. SAN-2020-013, [7-12-2020].

TREČIŲJŲ ŠALIŲ SLAPUKAI: KOKS PASAULIS BE JŲ?

Santrauka

Straipsnyje „Trečiųjų šalių slapukai: koks pasaulis be jų?" yra analizuojamas sprendimas panaikinti trečiųjų šalių slapukus. Šio tikslo siekiama, visų pirma, dėl išryškėjusių problemų, kurias kelia „sausainėlių" atitikimo teisės aktų reikalavimams stoka. Pirmosios šių pokyčių pradėjo imtis Firefox bei Safari nuo kurių neatsiliko ir didžiausia rinkos „milžinė" Google. Žinant apie trečiųjų šalių slapukų teikiamą naudą, tapo akivaizdu, jog kils būtinybė atrasti alternatyvų, pakeisiančių šią technologiją. Buvo pasiūlyti šie sprendimo būdai: „Privacy Sandbox", kontekstinis taikymas, Firefox įgyvendinta patobulinta apsaugos programa „Firefox 69" bei Safari išleista privatumo funkcija „Intelligent Tracking Protection".

Darbe taip pat aprašomas galimas skaitmeninės reklamos rinkos pobūdis įgyvendinus šį pokytį, kuris nulems būtinybę marketingo bei verslo įmonėms keisti strategijas vystant savo veiklą. Taip pat straipsnyje analizuojami teisiniai mechanizmai bei Europos Sąjungos institucijų siekiai teisėkūros procese, kurie padės užtikrinti vartotojų teises duomenų apsaugos srityje.

THIRD PARTY COOKIES: WHAT KIND OF WORLD IS WITHOUT THEM?

Summary

In the article "Third-party cookies: what kind of world is without them?" the decision to remove third-party cookies is being analysed. This objective is being pursued, firstly, because of the problems that have arisen as a result of the "cookies" lack of compliance with law norms. Firefox and Safari were the first ones to make these changes, followed by Google, the largest "giant" in the market. Knowing the benefits of third-party cookies, it has become clear that there will be a need to find alternatives to replace this technology. The following solutions were proposed: "Privacy Sandbox", contextual targeting, Firefox implemented an enhanced security program "Firefox 69", and Safari's privacy feature "Intelligent Tracking Protection".

The article also describes the possible nature of the digital advertising market after the implementation of this change, which will determine the necessity for marketing and business companies to change the strategies in the development of their activities. The article also analyses the legal mechanisms and aspirations of the European Union institutions in the legislative process, which will help to ensure consumer rights in the field of data protection.