Vilniaus universiteto Teisės fakulteto

Viešosios teisės katedra

Manto Benkunsko,

V kurso, taikomosios jurisprudencijos

studijų šakos studento

Magistro darbas

Interneto technologijų įtaka demokratiškam valstybės valdymui

The Influence of Internet Technologies on the Democratic Governance of the State

Vadovas: Lekt. dr. Johanas Baltrimas

Recenzentas: Asist. dr. Donatas Murauskas

Vilnius

2022

ANOTACIJA IR PAGRINDINIAI ŽODŽIAI

Šiame magistro darbe analizuojamos interneto technologijų grėsmės ir galimybės demokratiniam valstybių valdymui. Darbo pradžioje yra ištiriamos demokratinės valstybės ir interneto technologijų sampratos bei šių dviejų institutų santykio problematika. Toliau akcentuojamos interneto technologijų grėsmės demokratiniam valstybių valdymui: dezinformacija, internetinis balsavimas, interneto technologijų sukelti duomenų apsaugos bei „Deepfake“ instituto iššūkiai. Taip pat yra ištiriamos ir interneto technologijų galimybės demokratiniam valstybės valdymui. Galiausiai nurodant, interneto technologijų grėsmes ir galimybės Lietuvos teisinei sistemai.

Pagrindiniai žodžiai: Interneto technologijos, demokratija, grėsmės, galimybės.

This master's thesis analyzes the threats and opportunities created by Internet technologies in regards to democratic governance of states. Initially, the concepts of democratic state and Internet technologies as well as the problems of the relationship between these two institutes are studied. The key threats to the democratic governance of states are as follows: disinformation, online voting, the challenges of data protection posed by Internet technologies, and the challenges of the Deepfake institute. The potential of Internet technologies for democratic governance are also explored. Finally, the threats and opportunities of the Internet technology to the Lithuanian legal system are also listed.

Key words: Internet technologies, democracy, threats, opportunities.

TURINYS

ĮŽANGA

Temos aktualumas. „Facebook“, „Instagram“, „Twitter“ ir kiti socialiniai tinklai moderniame pasaulyje padarė revoliuciją. Socialinių tinklų dėka saviraiškos laisvės sklaida tapo globali, užtikrinanti dalijimąsi informacija realiu laiku tarp atokiausių pasaulio vietų. Interneto technologijos leidžia naudotojams palaikyti ryšį tarpusavyje, dalintis informacija vos mygtuko paspaudimu. Šis įrankis tapo sudėtine žmonijos gyvenimo dalimi, kuriuo šiuo metu naudojasi daugiau nei 4,62 milijardai vartotojų, o tai sudaro 58,4 procento visų pasaulio gyventojų (Global Social Media Stats 2022). Atsižvelgiant į tai, kad interneto technologijų įtaką mūsų visuomenėje yra išties didelė, galime pastebėti, jog interneto technologijų ir demokratinės valstybės valdymo institutai dažnai tarpusavyje susiduria įvairiuose teisiniuose aspektuose.

Pastaruoju metu daugelis mokslininkų pripažįsta, jog interneto technologijos sudaro sąlygas skleisti populizmą ir dezinformaciją bei gali būti panaudotos prieš demokratiją nukreiptiems tikslams įgyvendinti. Juk dar 2018 m. įvykus Cambridge Analytica skandalui (The New York Times 2018) mokslininkai pradėjo kelti klausimus dėl interneto technologijų grėsmių demokratinių valstybių santvarkoms. Tačiau nepaisaint to, galima įžvelgti ir interneto technologijų galimybių demokratiniam valstybių valdymo institutui (John Street 1997).

Apibendrinant galima teigti, jog šio darbo tema yra aktuali tiek teisiniu, tiek socialiniu aspektu – didelis visuomenės naudojimasis socialiniais tinklais, su iššūkiais susiduriančios valstybių demokratijos bei egzistuojantis itin aukštas teisinio neapibrėžtumas lemia didelį šio darbo temos aktualumo lygį.

Darbo tikslas. Šio darbo tikslas – ištirti ir įvertinti interneto technologijų grėsmes ir galimybes demokratiniam valstybės valdymui.

Tyrimo hipotezė. Interneto technologijos demokratiniam valstybės valdymui sukelia daugiau grėsmių negu suteikia galimybių.

Darbo uždaviniai. Norint pasiekti aukščiau nurodytą darbo tikslą, yra keliami šie uždaviniai:

1. Remiantis specialiąja literatūra apsibrėžti darbe naudojamas demokratinės valstybės ir interneto technologijų sampratas.

2. Išanalizuoti interneto technologijų problematiką pasireiškiančią ar galinčią pasireikšti demokratiniam valstybės valdymui, kokia yra tokių problemų specifika. Išanalizuoti užsienio teisės doktriną – Europos Sąjungos ir Jungtinių Amerikos Valstijų viešųjų institucijų praktiką, susijusią su interneto technologijų grėsmėmis demokratiniam valstybės valdymui bei ištirti ir pateikti šių grėsmių vertinimą.

3. Ištirti ir įvertinti interneto technologijų taikymo galimybes demokratiniame valstybių valdyme susijusias su demokratinio valstybės valdymo gerinimu.

4. Išanalizuoti ir įvertinti interneto technologijų grėsmes bei galimybes Lietuvos teisinei sistemai ir pateikti Lietuvos teisinio reglamentavimo vertinimą.

Objektas. Šio darbo pirmoje dalyje yra apibrėžiama demokratinės valstybės samprata. Antroje dalyje yra perteikiamas interneto technologijų institutas. Trečioje dalyje yra vertinamas demokratinės valstybės ir interneto technologijų santykio problematika. Ketvirtoje dalyje yra tiriamos interneto technologijų grėsmes, o penktoje galimybės demokratiniam valstybės valdymui. Galiausiai šeštoje dalyje yra analizuojamos ir vertinamos grėsmės bei galimybės Lietuvos teisinei sistemai.

Tyrimo metodai. Rengiant darbą buvo pasitelkti šie mokslinio tyrimo ir aiškinimo metodai:

1. **Sisteminis metodas** – remiantis šiuo metodu buvo susisteminta gausi tyrimo medžiaga, išskirtos atskiros darbo dalys, apibendrintos teisės doktrinos ir užsienio valstybių viešųjų institucijų pozicijos.

2. **Lyginamasis metodas** – šis metodas darbe buvo naudojamas siekiant palyginti Lietuvos, Jungtinių Amerikos Valstijų ir Europos Sąjungos teisinį reglamentavimą susijusį su interneto technologijų įtaka demokratinių valstybių santvarkoms.

3. **Atvejo analizės metodas** – tai metodas, kuris buvo naudojamas siekiant ištirti užsienio teisės doktrinoje, užsienio valstybių praktikoje perteikiamas demokratinių valstybių viešųjų institucijų pozicijas interneto technologijų atžvilgiu.

4. **Lingvistinis metodas** – nurodytas metodas darbe buvo pasitelktas teisinio reglamentavimo gramatiniam analizavimui, siekiant nustatyti teisės normų pobūdį susijusį su interneto technologijų grėsmėmis ir galimybėmis demokratiniam valstybių valdymui.

5. **Teologinis metodas** – darbe pasitelkiant šį metodą buvo siekiama atskleisti įstatymų leidėjo, viešųjų institucijų tikruosius tikslus priimant interneto technologijas

reglamentuojančius įstatymus ar jų pakeitimus. Taip pat šiuo metodu buvo siekiama atskleisti darbe pateikiamų įstatymų ir viešųjų institucijų pozicijų reikšmę bei tikslus.

Darbo originalumas. Yra manoma, jog internetas aktyviai formuoja visuomenės ir demokratinės valstybės santykį, tačiau vis tik yra reikalinga atlikti tolesnius mokslinius tyrimus. Šiuo metu nedalyvaujančių asmenų politinis aktyvumas didėja (Abdurashid Solijonov 2016). Ir nors šiuolaikiniame pasaulyje interneto technologijų pažangos dėka pasikeitę pagrindiniai informacijos bendrinimo ir perdavimo būdai suteikė visuomenei daug galimybių, tačiau vyraujantys interneto technologijų atvejai turi didžiulę įtaką pačių demokratinių valstybių teisinėms sistemoms. Vertinant šio darbo aktualumą pažymėtina, jog per pastaruosius penkerius metus Lietuvoje buvo apginti tik keli magistro darbai tiriantis socialinius tinklus: Greta Aleksynaitė „Socialinių tinklų atsakomybė už jų vartotojų skelbiamą informaciją“ (Aleksynaitė 2019) ir Gabrielius Matonis „Garbės ir orumo gynimas socialiniuose tinkluose“ (Matonis 2020). Tačiau per pastaruosiuspenkerius metus nėra apginta magistro darbų susijusių su interneto technologijų įtaka demokratiniam valstybės valdymui. Nors galima rasti įvairių straipsnių ir mokslinių tyrimų užsienio praktikoje, tačiau užsienio teisės doktrinos darbai neanalizavo Lietuvos teisinės sistemos.

Svarbiausi darbe nagrinėti šaltiniai. Šiame darbe yra analizuojami daugiausiai užsienio teisės mokslininkų darbai. Tokių mokslininkų kaip David Beetham, Frank Pasquale, Danielle Citron ir daugybės kitų užsienio mokslininkų darbai yra vieni pagrindinių šio darbo šaltinių. Be to, darbe yra tiriami ir vertinami Lietuvos, Europos Sąjungos, Jungtinių Amerikos Valstijų viešųjų institucijų teisės aktai, praktika bei rekomendacijos, kuriose yra nustatomos būsimo teisinio reglamentavimo gairės.

I. Demokratinė valstybė

Demokratinės valstybės sampratą atspindi demokratijos sąvoka, kuri yra priskirtina prie daugiaprasmių politinio mąstymo sąvokų. Graikai buvo pirmieji pateikę šios sąvokos aiškinimą, jungdami „demos“ ir „kreitein“ (liaudies valdžia). Sąvoka „demokratija“ nuo antikos laikoma mokslinės kalbos sąvoka. Tačiau demokratija buvo suprantama nevienareikšmiškai. Platonas demokratiją kartu su monarchija ir aristokratija laikė gerosiomis valstybės formomis, taip demokratija aiškiai atskirdamas nuo daugumos diktatūros. Tuo tarpu Aristotelis demokratiją suprato kaip daugumos diktatūrą ir priskyrė ją išsigimusiai valstybės formai (Lietuva. Mykolo Romerio universitetas 2009).

Nevartodamas pačios sąvokos „demokratija“ labai aiškiai demokratinės valdžios esmę apibūdino ir JAV prezidentas Abrahamas Lincolnas savo garsiajame Getisburgo kreipimesi 1863 m.: „Vyriausybė yra žmonių, iš tų žmonių išrinkta, dirbanti žmonėms (angl. government of the people, by the people, for the people)“. O pasak Davido Beethamo, demokratija yra sprendimų dėl visuotinai įpareigojančių taisyklių ir politikų priėmimo būdas, kurį kontroliuoja liaudis (Beetham 1992).

Teisinė valstybė, skelbianti ir įtvirtinanti žmonių santykiuose teisės viešpatavimą yra šiuolaikinė, naujo tipo valstybė. Ji pretenduoja įveikti klasikinės valstybės tradicija ir taip būti skirtingų socialinių grupių (klasių) bendradarbiavimo, visų socialinių grupių gerovės garantavimo politinė, teisinė organizacija (Vaišvila 2009).

Pažymėtina, kad demokratija nėra tik sklandūs Seimo ir Respublikos Prezidento rinkimai, perrinkimai ar parašų inicijuoti referendumą rinkimas. Šis principas iš esmės yra sudėtingiausias (kompleksiškiausias) tuo požiūriu, kad jį lemia ne tiek valstybės, kiek visuomenės (ne tik valstybinės bendruomenės, t. y. teisinės tautos) būsena ir raida. Todėl įstatymų leidyba, valdymas ar teisingumo vykdymas pajėgūs labiau įkūnyti nepriklausomybę ar teisinį valstybingumą nei demokratiją. Šiuo požiūriu neįmanoma demokratizuoti valstybės, nedemokratizavus visuomenės (o tai ne tiek konstitucinių ir teisinių, kiek socialinių normų, t.y. papročių ir tradicijų turinio klausimas). Todėl sunku išsamiai analizuoti demokratiją, neperžengiant įprastų jurisprudencijos ribų (neįsibraunant į politologijos ar istorijos aruodą) (Šileikis 2005).

Vertinant Lietuvos Respublikos demokratijos požymius galima pažvelgti į Lietuvos Statutus, kuriuose dar tuomet atsispindi tiek Seimo ir seimelių veikla, tiek ir bajorų demokratija. Pažymėtina, jog dar 1922 m. Lietuvos Respublikos gyvavimo metais Lietuvoje buvo įteisinta demokratinė valdymo sistema, o 20 amžiaus pabaigoje demokratija tapo vyraujančia valstybės valdymo forma, kuri garantuoja visas politinės ir pilietinės

laisves. 1992 m. Lietuvos Respublikos Konstitucijoje 2 straipsnyje nustatyta, kad Lietuvos valstybę kuria Tauta (Lietuva. Mykolo Riomerio universitetas 2017).

Konstatuotina, jog Lietuvos Respublikos Konstitucinis Teismas niekuomet nėra bandęs pateikti išsamaus demokratijos elementų ar atributų katalogo. Tačiau 2002 m. rugsėjo 19 d. nutarime (Lietuvos Respublikos Konstitucinio Teismo 2002 m. rugsėjo 19 d. nutarimas. Valstybės žinios, Nr. 93-4000) galima rasti savotišką pavyzdinį sąrašą, kuriame įvardijami kituose Konstitucinio Teismo aktuose iki tol minimi ir vėliau kartojami demokratijos aspektai. Šiame nutarime, referuodamas į Konstitucijos 1 straipsnį, kuriame nustatyta, kad Lietuvos valstybė yra nepriklausoma demokratinė respublika, Konstitucinis Teismas nurodė: „Lietuvos valstybė yra demokratinė, reiškia, kad valstybėje turi būti užtikrinama Konstitucijos viršenybė, žmogaus teisių ir laisvių apsauga, visų asmenų lygybė įstatymui ir teismui, teisė į teisminę gynybą, laisvi ir periodiški rinkimai, valdžių padalijimas ir pusiausvyra, valdžios atsakomybė piliečiams, demokratinis sprendimų priėmimo procesas, politinis pliuralizmas, galimybės plėtotis pilietinei visuomenei ir kt. Pažymėtina, kad nuostata, jog Lietuvos valstybė yra demokratinė, yra konstitucinis įpareigojimas nenukrypti nuo demokratijos reikalavimų, taikytinas visoms valstybės institucijoms, neišskiriant ir įstatymų leidėjo.“

Šiuo požiūriu taip pat pabrėžtina, kad Konstitucinis Teismas nurodo: „Konstitucija prieštaraujančiais įstatymais ar kitais teisės aktais pažeidus neatskiriama demokratijos dalimi pripažįstamą Konstitucijos viršenybės principą (taip pat kitas minėtas vertybes), kartu ne „yra“, o tik „gali būti kėsinamasi ir į Konstitucijoje įtvirtintus demokratijos elementus. <…> konstatavimas, kad įstatymas ar kitas teisės aktas prieštarauja Konstitucijai, savaime nereiškia, jog yra pažeista Konstitucijos 1 straipsnio nuostata, kad Lietuvos valstybė yra demokratinė. Kiekvienu atveju Konstitucinis Teismas turi įvertinti, ar teisiniu reguliavimu, pripažintu prieštaraujančiu Konstitucijai, nėra paneigiama Konstitucijos 1 straipsnio nuostata, kad Lietuvos valstybė yra demokratinė (Lietuvos Respublikos Konstitucinio Teismo 2011 m. birželio 21 d. nutarimas. Valstybės žinios, Nr. 76-3672).

Konstitucinio Teismo nutarimuose pačiai demokratijai yra skiriama ypatinga vieta: šalia prigimtinio žmogaus teisių ir laisvių pobūdžio, valstybės nepriklausomybės bei respublikinės valdymo formos, ji įvardijama kaip viena iš keturių pamatinių konstitucinių vertybių. Demokratija pripažįstama Konstitucijos, ja grindžiamo Tautos bendro gyvenimo, Lietuvos valstybės pamatu (Lietuvos Respublikos Konstitucinio Teismo 2012 m. gruodžio 19 d. nutarimas. Valstybės žinios, Nr. 152-7779).

Konstitucinio Teismo vertinimu, Konstitucijos nuostatų, įtvirtinančių šias pamatines konstitucines vertybes, paneigimas „reikštų pačios Konstitucijos esmės paneigimą“ (Lietuvos Respublikos Konstitucinio Teismo 2014 m. liepos 11 d. nutarimas. Valstybės žinios, Nr. 10117). Be kita ko, tai taip pat reiškia, kad jokiomis sąlygomis negali būti priimamos Konstitucijos pataisos, naikinančios prigimtinį žmogaus teisių ir laisvių pobūdį, demokratiją ar valstybės nepriklausomybę.

Aiškindamas demokratijos sampratą Lietuvos Respublikos Konstitucinis Teismas dažniau ją mini ne kaip atskirą dalyką, o valstybę arba visuomenę apibūdinantį terminą. Tačiau reikia pabrėžti, kad nors analogiškuose kontekstuose terminas „demokratija“ Konstitucinio Teismo jurisprudencijoje gali būti vartojamas siejant jį tiek su „valstybe“, tiek ir su „visuomene“, kiekybiniu požiūriu dominuoja sąvoka „demokratinė valstybė“.

Interpretuojant demokratijos principą viso konstitucinio reguliavimo kontekste pažymėtina, kad Konstitucijoje įtvirtinti demokratijos standartai determinuoja visą teisinį reguliavimą: vieną vertus teisės aktais negali būti nustatyta tokių institutų ir procedūrų, kurie pažeistų demokratijos standartus valstybės ar jos dalies mastu, kita vertus, institucijos įgyvendinančios demokratiškumą, turi ir pačios tvarkytis demokratiškai (Lietuva. Mykolo Romerio universitetas 2002).

Pažymėtina, jog demokratinis valstybės valdymas suprantamas kaip tautos valdžia. Šiame valdyme visa valdžia kyla iš tautos ir jai tarnauja visos valdžios institucijos. Be to šis valdymui yra būdingi tam tikri bruožai be kurių jis negalėtų būti laikomas demokratiniu.

Demokratinį politinį režimą apibūdina tokie bruožai: 1) demokratinių piliečių teisių ir laisvių pripažinimas, užtikrinantis galimybę jiems savarankiškai ir aktyviai dalyvauti tvarkant bendruosius visuomenės reikalus; 2) politinis pliuralizmas – t. y. valstybėje veikia įvairios politinės partijos ir organizacijos, kurios nustatyta tvarka rungiasi dėl vadovavimo visuomenei, visos politinės partijos turi vienodų teisinių galimybių, laisvai veikia opozicinės partijos, siūlančios alternatyvius Vyriausybės politikos sprendimus, laisvieji susirinkimai – svarbiausiųjų valstybės institucijų sudarymo būdas; 3) valdžių padalijimo principo realus įgyvendinimas; 4) parlamento, kaip tautos atstovybės, aukščiausiosios įstatymų leidimo institucijos, funkcionavimas; tik parlamentas priima įstatymus, skirtus svarbiausiems visuomeniniams santykiams reguliuoti, taip pat nustato valstybės vidaus ir užsienio politikos pagrindus, tvirtina biudžetą, kontroliuoja vyriausybę. Parlamentas priima sprendimus balsų dauguma, bet kartu laiduojamos mažumos, politinės opozicijos teisės; 5) leidžiama bet kokios politinės ideologijos laisva propaganda, jeigu nekviečiama griebtis smurto, nepažeidžiamos visuomenės moralės ir bendrosios elgesio normos, nesikėsinama į kitų piliečių teises (Lietuva. Mykolo Riomerio universitetas 2017).

Apibendrinant galima teigti, kad demokratinė valstybė remiasi valdymo forma, kuria visa valdžia kyla iš valstybės piliečių valios, o pats valstybės valdymas įgyvendinamas laisvais ir reguliariais rinkimais, renkant valstybės valdžią ir veikiant valdžiai pagal Konstitucijoje nustatytus įgaliojimus. Demokratinėmis valstybėmis vadiname tas šalis, kurios turi konstituciškai įteisintą demokratiją kaip politinio valdymo formą ir pasižymi procedūromis, kurių realus įgyvendinimas atitinka demokratinių valstybių bruožus. Taigi demokratija nėra autokratija ar diktatūra, kur valdo vienas asmuo. Ir tai ne oligarchija, kur valdo mažas visuomenės segmentas. Tinkamai suprantama demokratija net neturėtų būti daugumos valdžia, jeigu tai reiškia, kad mažumų interesai yra visiškai ignoruojami. Demokratija, bent jau teoriškai, yra visų žmonių valdžia išreikšta pagal jų valią.

II. Interneto technologijų samprata

Internetas tai vienas reikšmingiausių šiuolaikinės visuomenės išradimų. Socialiniai tinklai „Facebook“, „Instagram“, „Twitter“ ir kitos interneto technologijų platformos suteikia mums galimybę bendrauti su žmonėmis, skaityti naujienas, dalintis informacija iš viso pasaulio. Internetas atvėrė naujas galimybes daugeliui žmonių suteikdamas prieigą prie anksčiau neprieinamų dalykų.

Jungtinių Amerikos Valstijų Aukščiausias Teismas (*See Reno v. ACLU* (1997) 521 U.S. 844) internetą apibūdina taip: „Internetas – tai tarpusavyje sujungtų kompiuterių tarptautinis tinklas.“, o Jungtinių Amerikos Valstijų (toliau – JAV) įstatymų leidėjas Interneto Mokesčių Laisvės įstatyme (*The Internet Tax Freedom Act 1998* (ITFA; P.L. 105–277)), pateikia išsamesni apibrėžimą – „Internetas – tai kolektyvinė kompiuterio ir telekomunikacinių įrenginių sankaupa, susidedanti iš techninės bei programinės įrangos, kuri apima tarpusavyje sujungtą pasaulinį tinklą (world–wide network), veikianti TCP/IP, bei visus buvusius (predecessor) ar būsimus (successor) protokolus, leidžiančius bevieliu ar kabeliniu būdu perduoti, keistis informacija.“

Tuo tarpu, Europos Žmogaus Teisių Teismas (*Yildirim v Turkey* (2012) EŽTT. Paraiškos Nr. 3111/10), teigia, jog socialiniai tinklai kaip komunikacijos internete forma, tapo viena svarbiausių priemonių, kurią pasitelkę individai naudojasi saviraiškos laisve, o kartu socialiniai tinklai suteikia galimybę dalyvauti veiklose ir diskusijose dėl politinių bei kitų su viešuoju interesu susijusių klausimų. Europos Tarybos Ministrų Komiteto rekomendacijoje (Europos Tarybos Ministrų Kabinetas 2012) yra nurodoma, kad socialiniai tinklai yra svarbi didėjančio žmonių skaičiaus gyvenimo dalis.

Konstatuotina, kad Lietuvos teisiniame reglamentavime (Lietuvos Respublikos Vyriausybės nutarimas 2003 (Žin Nr. 24–1002)) internetas apibrėžiamas kaip viešojo naudojimo kompiuterių tinklas – bendrosios prieigos informacinis tinklas, tarptinklinės sąveikos protokolais vienijantis techninę įrangą (kompiuterius) ir tinklus, priklausančius informacijos išteklių ir telekomunikacijų paslaugų teikėjams, kitiems juridiniams ir fiziniams asmenims. Tarpusavyje sujungti vidaus kompiuterių tinklai irgi laikomi viešojo naudojimo kompiuterių tinklais.

Interneto technologijų sąvoką šiame darbe suprantame kaip interneto galimybę perduoti informaciją, duomenis per skirtingus serverius ir sistemas. Nurodant, kad interneto technologijos yra svarbios daugelyje skirtingų pramonės šakų, kadangi jų dėka žmonės gali bendrauti vieni su kitais priemonėmis, kurios anksčiau nebuvo prieinamos.

Tam, kad suprasti interneto technologijų institutą turime atsižvelgti į pačią interneto istoriją. Teisinėje literatūroje (Lietuva. Mykolo Romerio universitetas 2004) nurodoma, jog 1960 m. JAV mokslų tyrimų institutams pradėjus jungti kompiuterius tarpusavyje, kilo kompiuterinio tinklo sąvoka. <...> Apie 1990–1994 m. internetą atrado komercinės organizacijos, suvokusios jo galimybes prisidėti prie elektroninės komercijos plėtros. <...> 2000 m. internetas tampa visiškai globaliu kompiuterių tinklu, visiems laikams apraizgiusiu planetą.

Po interneto burbulo žlugimo atsirado vadinamoji „Web 2.0 “ (Meškauskaitė 2018), internetas, kuriame yra akcentuojamas socialinis tinklas ir vartotojų sukurtas turinys bei debesų kompiuterija. Socialinės žiniasklaidos priemonės kaip „Facebook“, „Instagram“ ir „Twitter“, tapo vienais populiariausių interneto technologijų įrankių. Taip pat tie patys išmanieji telefonai tapo efektyvia prieiga prie interneto, todėl interneto vartotojų skaičius visame pasaulyje šiuo metu yra išaugęs iki 4.95 milijardų (Global Social Media Stats 2022), o tai sudaro 62,5 procento visų pasaulio gyventojų. O tuo tarpu socialinių tinklų platformomis naudojasi daugiau nei 4,62 milijardo, kas sudaro 58,4 procento visų pasaulio gyventojų (Global Social Media Stats 2022).

Pabrėžtina, kad interneto technologijos, kurių sudėtinė dalis yra socialinė žiniasklaida – nuolat tobulėja ir keičiasi. Socialiniai tinklai kaip interneto technologijų įrankiai palengvina informacijos dalijimąsi per virtualius tinklus ir bendruomenes, o socialinė žiniasklaida yra pagrįsta internetu ir leidžia vartotojams greitai elektroniniu būdu, naudojant kompiuterį, planšetinį kompiuterį ar išmanųjį telefoną, perduoti turinį – asmeninę informaciją, dokumentus, vaizdo įrašus, nuotraukas ar kt.

Tačiau teisė, kaip socialinis reiškinys, negalėjo ir toliau negali atsilikti nuo sparčios informacinių technologijų plėtros ir naujų technologijų radimosi, o tai kelia naujų iššūkių ir problemų tarptautinėms institucijoms, Europos Sąjungos ir atskirų valstybių įstatymų leidėjams inicijuojant teisės aktų, kurie atspindi įvykusius technologinius pokyčius, leidimą, tiek verslo subjektams, tiek teisėsaugos institucijoms bei, ko gero, kiekvienam iš mūsų, nes šiuolaikinio žmogaus gyvenimas yra beveik neįsivaizduojamas be informacinių technologijų (Lietuva. Mykolo Romerio universitetas 2016).

Interneto technologijų plėtra ir spartus šio instituto keitimas daugybei mokslininkų kelia nerimą. Pasaulio ekonomikos forumo paskelbtoje baltojoje knygoje nurodoma: „atsižvelgiant į Ketvirtosios pramonės revoliucijos nepaprastai greitus technologinius ir socialinius pokyčius, neapgalvota yra pasikliauti tik vyriausybės teisės aktais ir paskatomis siekiant užtikrinti tinkamus rezultatus. Tikėtina, kad priimti teisės aktai bus pasenę arba pertekliniai iki tol, kol bus reglamentuoti.“ (World Economic Forum 2016).

Pažymėtina, kad geriausias būdas užtikrinti teigiamus rezultatus interneto technologijų teisiniame reguliavime yra remtis aiškiu vertybiniu pagrindu, sutelkiant dėmesį į tokius pagrindinius principus kaip žmogaus orumas ir bendrasis gėris. Tai svarbu, nes tik vertybiniu pagrindu pagrįstas teisinis reguliavimas gali užtikrinti teisinės valstybės stabilumą.

Taigi galima teigti, kad interneto technologijos tapo neatsiejama mūsų gyvenimo dalimi. Nesvarbu ar tai „Facebook“, „Instagram“, ar „Twitter“, žmonės naudojasi šiomis internetinėmis svetainėmis tam, jog susirastų draugų ar dalintųsi asmeninio pobūdžio turiniu. Internetas kaip didžiulis tinklas, jungiantis kompiuterius ir tuo pačiu visuomenės narius visame pasaulyje, suteikia galimybę naudotis interneto technologijomis. Tad interneto technologijos yra suprantamos kaip interneto įrankis, leidžiantis asmenims dalintis internetu tam tikra informacija ir bendrauti iš bet kurios pasaulio vietos, kurioje yra interneto ryšys.

III. Demokratinės teisinės sistemos ir interneto technologijų santykio problematika

Nuo pat pirmųjų dienų internetas buvo laikomas demokratinių vertybių sklaidos priemone. John Perry Barlow savo 1996 m. Nepriklausomybės deklaracijoje nurodė: „Mes kuriame pasaulį, į kurį visi gali patekti be privilegijų ar išankstinių nusistatymų pagal rasę, ekonominę galią, karinę jėgą ar gimimo vietą. Mes kuriame pasaulį, kuriame kiekvienas, bet kur gali išreikšti savo įsitikinimus, kad ir kokie jie išskirtiniai būtų, nebijodami būti nutildyti“ (Perry Barlow 1996).

Interneto technologijų egzistavimo pradžia demokratijos atžvilgiu buvo neabejotinai daug žadanti: įgalinti rinkimuose paprastai nebalsuojančius piliečius, skleisti politinę informaciją, kurti aktyvias pilietines bendruomenes. Tačiau dažnai galime išgirsti susirūpinimų, kad demokratiškiausios interneto savybės pasižymi tuo, jog kelia pavojų demokratijos santvarkai.

Interneto technologijų optimizmas vyravęs pirmuosius kelis interneto augimo dešimtmečius, dabar susidūrė su didžiuliais iššūkiais, kurie vyrauja demokratijos ir interneto technologijų sąveikoje. Be plataus akademinio susidomėjimo technologijų poveikiu visuomenei ir demokratijai per pastaruosius kelerius metus, demokratinės valstybės išreiškė didelį susirūpinimą dėl interneto bei demokratijos sąveikos. Europos Komisijos narys Julianas Kingas tvirtino, kad „kiekviena valstybė narė turi visapusiškai įvertinti grėsmę savo demokratiniams procesams ir institucijoms, nesvarbu, ar kyla tradicinių kibernetinių atakų, ar dėl manipuliavimo informacija“ (Julian King 2018).

Socialinės žiniasklaidos poveikio klausimas yra aktualus demokratiniam valstybių valdymui, nes pirma, socialinė žiniasklaida yra naujausia socialinių ir techninių naujovių interneto komunikacijos sritis, suteikianti galimybę naudotis naujomis ir skirtingų rūšių galimybėmis vartotojams bendrauti internete (Shelley Boulianne 2015). Antra, socialinė žiniasklaida ir socialinės tinklo svetainės pritraukia itin daug vartotojų. Socialinis tinklalapis „Facebook“ turi ne vieną milijardą vartotojų visame pasaulyje. „Youtube“, „Facebook“, „Wikipedia“, „Twitter“ ir „LinkedIn“ yra vieni iš labiausiai paplitusių interneto svetainių pasaulyje (Global Social Media Stats 2022). Trečia, daugybė politinių įvykių, susijusių su socialine žiniasklaida padidino susidomėjimą politikos ir socialinės žiniasklaidos sąveika bei socialinės žiniasklaidos naudojimu politikos tikslams pasiekti.

Išryškinant interneto technologijų ir demokratinių valstybių valdymų santykio problematiką, galime atkreipti dėmesį į politinius sukrėtimus bei dezinformaciją. Pavyzdžiui, kišimasis į JAV 2016 m. prezidento rinkimus (Michelle Ma 2018). Verta

paminėti, kad dauguma apžvalgininkų padarė išvadą, jog socialinė žiniasklaida buvo svarbus, jeigu net ne lemiamas veiksnys sudaręs prielaidas šiam neteisėtam įsikišimui į demokratinius JAV procesus.

Tačiau yra ir kitų nuomonių, kurios pabrėžia, jog visos komunikacijos revoliucijos (nuo spaustuvės, televizijos ar interneto) turi teigiamų ir neigiamų požymių. Tiek televizija, tiek internetas, tiek kitos komunikacinės priemonės dažnai yra kaltinamos (dažniausiai be priežasties) dėl politinių, socialinių ar kitokio pobūdžio nesutarimų. Naujoji žiniasklaida tarnauja kaip veidrodis, atspindintis visuomenes socialines negeroves, bet nebūtinai jas sukuriantis. Tad problemos, kurias tariamai sukelia interneto technologijos, vyravo dar prieš joms atsirandant.

Konstatuotina, kad socialinė žiniasklaida stipriai pakeitė žmonių naudojimąsi internetu, pasinaudodama naujomis galimybėmis jungtis, bendrauti ir keistis informacija. Žinoma, kyla pagunda dėl viso to kaltinti interneto atsiradimą, tačiau svarbu pripažinti, kad technologijų veikimą formuoja įstatymai. Ironizuojant, galima įsivaizduoti XXI amžių, kuriame nėra įstatymų, reglamentuojančių vaikų darbo draudimą ar įtvirtinančius darbuotojų teises. Vietoj to, kiekviena įmonė galėtų nuspręsti, kokias teises ji suteiks darbuotojams, kokią darbo santykių praktiką taikys ir kaip paskirstys įmonės pelną. Laimei, teisės ir įstatymai reglamentuojantys šiuos santykius egzistuoja jau dešimtmečius visose pasaulio demokratinėse šalyse.

Ne išimtis ir interneto technologijos, kurios negali vystytis be įstatymų leidėjo reguliavimo apsaugančio demokratinių valstybių piliečius nuo jų teisių pažeidimų. Suprantama, jog įstatymų leidėjas turi padaryti pasirinkimą. Galima turėti demokratines valstybes arba valstybes, kuriose sprendimų priėmimas yra sutelktas kelių interneto technologijų bendrovių rankose. Todėl jeigu demokratinės valstybės nereguliuos interneto technologijų sukuriamų grėsmių, turėsime pasekmes, kurios susilpnins ir galiausiai pakeis pačią demokratiją.

Vertinant interneto technologijų įtaką demokratijai svarbu įžvelgti pačios valstybės besikeičiančią rolę. Suprantama, jog valstybė turi priimti sprendimus, kadangi valstybė kartu su visuomene yra sudariusi visuomenės sutartį (Jean–Jacques Rousseau 2015). Šia sutartimi valstybė yra įsipareigojusi užtikrinti visuomenės saugumą, socialinę apsaugą, gerovę ir t. t. Valstybė yra kaip pagalbinis veikėjas, kuris gali ir turi priimti sprendimus, kadangi visuomenė jai tai leidžia padaryti.

Visuomenės sutartis yra reikalinga, nes taip ji išsprendžia viena iš pagrindinių demokratinių problemų: „Kaip rasti tokią organizacijos formą, kuri visa bendrąja jėga gintų ir globotų kiekvieno nario asmenį ir turtus ir per kurią kiekvienas, susijungdamas su visais,

vis dėl to klausytų tik pats savęs ir liktų taip pat laisvas, kaip ir anksčiau“ (Jean–Jacques Rousseau 2015).

Tačiau atsiradus interneto technologijoms valstybės vaidmuo yra iškreiptas. Valstybė nebevaidina tokios rolės, kuria užtikrintų visuomenės interesus. Internetinei erdvei esant atsietai nuo tam tikros teritorijos, pačios demokratinės valstybės įtakos ribos aiškiai sumažėja.

Tuo tarpu atsiradusios didžiosios interneto technologijų bendrovės turinčios didžiulę įtaką valstybės demokratiniams procesams, nesulaukia tinkamo valstybės atsako. Jeigu valstybė neužtikrins visuomenės ir demokratinių procesų saugumo, tuomet kyla klausimas – ar valstybės bei visuomenės sudarytas socialinis kontraktas yra patikimas? Ar demokratinė valstybė gali apsaugoti savo visuomenę nuo interneto technologijų grėsmių?

Pasaulyje girdisi daug nerimo dėl demokratijos silpnėjimo interneto technologijų atžvilgiu. Vykstant pokyčiams visuomenėje, tai siejama su internetine erdve. Atsirandanti nauja erdvė sukelia naujas galių varžybas tarp valstybių ir interneto technologijų bendrovių. Kadangi internetinė erdvė gali aiškiai paveikti tą pačią fizinę erdvę, kurios dalimi yra visi demokratinių valstybių piliečiai.

Šaržuojant galima teigti, jog bet kada galima apsisaugoti išjungiant internetą. Gal tuomet demokratinė valstybė išvengtų daugybės interneto technologijų grėsmių? Tačiau tai gali padaryti tik autoritariniai režimai kaip Kinija ar Rusija. Autokratijos gali lengvai susekti interneto technologijų pažeidimus ir juos užblokuoti, o demokratijos taip elgtis negali, kadangi jos yra įsipareigojusios saviraiškos, laisvo žodžio ir žiniasklaidos teisėms.

Pabrėžtina, jog demokratinės valstybės yra atviros, todėl yra įsipareigojusios atvirumui ir žodžio laisvei. Tuo tarpu autoritarinės valstybės gali pažeisti žodžio laisvę, taip apsaugodamos savo režimus, o demokratijos to padaryti negali. Todėl demokratinėse valstybėse priešiškai nusiteikę subjektai, siekdami pažeisti demokratinių valstybių institucijas, paveikti žmonių mąstymą ir taip gauti tam tikrą naudą, dažnai interneto technologijų pagalba pakenkia demokratinių valstybių santvarkoms.

Atsižvelgdama į dabartines interneto technologijų grėsmes Europos Sąjunga patvirtino Europos skaitmeninės transformacijos iki 2030 m. viziją, tikslus ir kryptis (Europos Komisija 2021). Šiame dokumente „Skaitmeninės politikos kelrodis“ aiškiai išdėstoma bendra Europos skaitmeninio dešimtmečio vizija ir sėkmingo jos įgyvendinimo tiek Europoje, tiek pasaulyje, veiksmai.

2022 m. sausio 26 d. Europos Sąjungos deklaracijoje (Europos Komisija 2022) nurodoma, kad šioje deklaracijoje bus galima rasti informaciją apie Europos skatinamą ir ginamą skaitmeninę pertvarką. Nurodyta rekomendacija gali vadovautis politikos

formuotojai ir su interneto technologijomis dirbančios bendrovės. Deklaracija yra glaudžiai susijusi su 2021 m. rugsėjo mėn. priimtu programos „Skaitmeninio dešimtmečio kelias“ pasiūlymu, kuriame nustatyti platesni skaitmeniniai tikslai ir jų įgyvendinimo planas. Deklaracijos tikslas - užtikrinti skaidrumą, stebėti tendencijas ir pasiektus rezultatus visose valstybėse narėse ir suteikti informacijos, padėsiančios tinkama linkme kreipti politiką galimais būsimais teisės aktais, susijusiais su sritimis, kurioms taikomi deklaracijoje įtvirtinti principai.

Iš pateiktos analizės galima spręsti, kad demokratinėms valstybėms yra ypač svarbu turėti tinkamą teisinį reglamentavimą reguliuojantį interneto technologijas. Šiandien vyraujantis teisinis neapibrėžtumas yra bandomas kompensuoti deklaracijomis ir viešais pareiškimais, jog ši problema yra ir bus sprendžiama. Tačiau pažymėtina, kad šiuo metu galiojantis teisinis reglamentavimas vis tiek yra nepakankamas. Todėl įstatymų leidėjai turi siekti teisinio reguliavimo, kuris sustiprintų demokratiją ir suvaldytų technologines grėsmes demokratinių valstybių atžvilgiu.

3.1. Dezinformacija internete – šiuolaikinės demokratijos iššūkis

Interneto technologijos kiekvieną dieną suteikia milžinišką informacijos kiekį dideliam skaičiui žmonių visame pasaulyje. Tačiau tuo pat metu interneto technologijos pagalba yra skleidžiama melaginga informacija. Suprantama, kad skaitmeninės platformos suteikia didesnę tiesioginę prieigą prie informacijos turinio, tačiau galima pastebėti, jog šiuo metu internetinėje žiniasklaidoje pirmenybė yra teikiama didesniam paspaudimų skaičiui „clickbait“, o ne profesionaliai žurnalistikai (Kornbluh and Goodman 2020).

Pabrėžtina, jog socialiniai tinklai pakeitė mūsų asmeninį požiūrį į informaciją. Pastaraisiais metais dezinformacijos skaičiai išaugo visame pasaulyje. MIT Media Lab tyrimas nustatė, kad melas yra skleidžiamas toliau, greičiau, giliau ir plačiau nei tiesa, o melas 70 proc. labiau tikėtina, kad bus pasidalintas „Twitter“ platformoje, nei teisingi faktai (Vosoughi et al. 2018).

Tokios tendencijos neramina, kadangi dezinformacija gali turėti žalingą poveikį demokratijos veikimui. Dezinformacija gali suklaidinti piliečius arba jais manipuliuoti, sukurti nepasitikėjimą valstybių vyriausybėmis, institucijomis, tarptautinėmis organizacijomis. Dezinformacijos pagalba priešiškos jėgos gali suklastoti rinkimus, skatinti nepasitikėjimą demokratinės valstybės santvarka.

Europos Sąjungoje dezinformacijos sąvoka apibūdinama (Europos Komisija 2018) kaip „patikrintai melaginga ar klaidinanti informacija“, kuri yra sukurta, pristatoma ir platinama siekiant ekonominės naudos arba tyčia apgaunant visuomenę, taip jai padarant žalą“. Panašus apibrėžimas priimtas ir 2018 m. kovo mėn. paskelbtoje nepriklausomos aukšto lygio melagingų naujienų, ir internetinės dezinformacijos grupės ataskaitoje (Europos Komisija 2018). Pagal šį apibrėžimą, žalos riziką apima grėsmės demokratiniams politiniams procesams ir vertybėms.

Žinoma, reguliuojant pačia dezinformaciją galima išskirti keletą skirtingų modelių. Timothy Garton Ash išskiria tris skirtingus modelius (Timothy Garton Ash 2016) – Kinijos, JAV ir Europos. Šie trys modeliai pateikia tris skirtingas interneto kalbos ir interneto platformų reguliavimo sampratas.

Šiandien yra matomas plačiai paplitęs susirūpinimas, kad interneto technologijos kelia unikalių iššūkių visai demokratijai. Tačiau kaip su tuo kovoti? Valstybės svarsto įvairius modelius, kurie padėtų apsaugoti savo gyventojus nuo dezinformacijos.

Štai Kinijos požiūris į dezinformacijos reguliavimą yra pats kraštutiniausias reguliavimo pavyzdys (Gary King et al. 2017). Kinija cenzūruoja ir baudžia už „netinkamą“ internetinę kalbą, draudžią tokių internetinių platformų kaip „Google“ ir „Facebook“ veiklą

šalyje. Taip pat Kinijos piliečių veiklą internete stebi milijoninė žmonių stebėjimo komanda, kuri prižiūri diskusijas internetinėje erdvėje. Kinijos teisinis reguliavimas visiškai neatspindi vakarietiškos žodžio laisvės sampratos, todėl galima teigti, jog Kinija užima kraštutinio autoritarinio reguliavimo poziciją.

Priešingas kraštutinumas yra JAV. Verta pastebėti, kad šioje valstybėje teisinis reguliavimas dezinformacijos atžvilgiu yra išties libertarinio požiūrio. Pirmoji JAV pataisa (U.S. Const. amend. I) apsaugo kai kurias kalbos kategorijas, kurios yra plačiai reguliuojamos visame pasaulyje. JAV Aukščiausiojo Teismo doktrina dėl nepadorumo, neapykantos kurstymo, šmeižto, kampanijų finansavimo ir daugybės kitų laisvo žodžio sričių išskiria plačią visuomenės daugumos apsaugą šios kalbos kategorijoms.

JAV interneto technologijų teisinis reguliavimas (Communications Decency Act 1996 (47 U.S.C. § 230)) atleidžia interneto technologijų bendroves nuo atsakomybės už kitų šalių pasisakymus, vykstančius jų platformose, kuriose nėra vykdomi redakciniai kontrolės veiksmai. Šis teisinis reguliavimas egzistuoja dėl spartaus „Google“, „Facebook“ bei kitų interneto technologijų platformų augimo. Tai parodo akivaizdų JAV teisinio reguliavimo atsakomybės trūkumą, kuris leidžia įstatymų leidėjui pilnai nereguliuoti interneto technologijų platformų klientų kalbos.

Tuo tarpu Europoje yra taikomas griežtesnis tarpininko atsakomybės modelis ir interneto kalbos apribojimai nei JAV. Pavyzdžiui, Vokietijos NetzDG įstatymo 36 straipsnis (Network Enforcement Act 2017 (Nr. 2017/127/D)) numato baudas interneto technologijų platformoms iki penkiasdešimties milijonų eurų už neteisėtą kalbą, kuri lieka platformoje po to, kai jiems buvo pranešta (su kai kuriomis išimtimis). Šis įstatymas nukrypsta į didesnius apribojimus, numatytus Vokietijos įstatyme dėl šmeižto ir neapykantos kurstymo. Nors pats įstatymas interneto technologijų platformoms nenurodo, kokia kalba yra dezinformacija t.y. kokia kalba turėtų būti pašalinta. Tačiau atvirkščiai, jame nurodoma, kad reikia žiūrėti į įstatymą ir teisinius precedentus, siekiant nustatyti, ar kalba interneto technologijų platformose yra iš tikrųjų dezinformacija. Šiuo įstatymo teisinės atsakomybės perkėlimu pasinaudojo ir dauguma Europos valstybių, kurdamos teisinį reglamentavimą.

Pažymėtina, jog net ir neviršijant turinio apribojimų, Europa yra labiausiai pažengusi interneto technologijų bendrovių reguliavimo atžvilgiu. Pavyzdžiui, dėl antimonopolinių ir privatumo apsaugos pažeidimų, Europos Komisija skyrė griežtas (kelių milijardų ir kelių milijonų dolerių) baudas Google ir Facebook (Ian Bogost 2018).

2018 m. Europos Sąjunga paskelbė savo pirmąjį veiksmų planą (Europos Komisija 2018) prieš dezinformaciją, kuriame nurodė, kad prokremliška dezinformacija yra

didžiausia grėsmė Europos Sąjungai. Šiuo planu dezinformacija buvo įtraukta į hibridinių grėsmių kontekstą, taip pabrėžiant Europos išorės veiksmų tarnybos prioritetines tolesnio darbo sritis.

Dezinformacija tapo pagrindiniu diskusijų ir rūpesčių objektu Europos Sąjungoje. Dezinformacijos sklaida ypač klestėjo koronaviruso pandemijos kontekste, skatinant susiskaldymą ir mažinant pasitikėjimą viešosiomis institucijomis. Tokie dezinformacijos ženklai kelia grėsmę Europos stabilumui. Suprantama, kad dezinformacijos problemą išspręsti sudėtinga, kadangi melagienos yra labai sunkiai atskiriamos. Jos daugiausia atsiranda dėl antrinių ir dažnai privačių veikėjų duomenų perdavimo tam, jog pasiektų tikslinę auditoriją.

Socialinių tinklų problemos vyrauja visame pasaulyje - ne tik pagrindinėse socialinėse žiniasklaidos priemonėse „Facebook“, „Twitter“ ir „YouTube“, bet ir tokiuose forumuose kaip „Reddit“, „Discord“ ir „4chan“, kuriuose susekti melagienas yra dar sudėtingiau. Taigi kova su dezinformacija reikalauja itin apgalvotų strategijų.

Pabrėžtina, kad Europos Sąjunga siekia bendradarbiauti su privačiomis įmonėmis, jog padėtų sustabdyti priešiškos dezinformacijos bangą. Nuo 2018 m. Europos Komisija vadovaudama dezinformacijos internete teisėkūros darbotvarkei, taikė Dezinformacijos praktikos kodeksą (Code of Practice on Disinformation 2018) (toliau – DPK), kurį pasirašiusios šalys, įskaitant „Facebook“, „Twitter“ ir „TikTok“, savanoriškai įsipareigojo sumažinti dezinformaciją bei užkardyti kišimąsį į rinkimus.

Interneto technologijų platformos sutiko apsaugoti savo teikiamas paslaugas nuo neautentiško elgesio, skatindamos skaidrias reklamas ir atvirą dalijimąsi atitinkamais duomenimis su „tyrėjų bendruomene“ (Europos Komisija, 2020). DPK yra pirmoji pasaulyje tokio pobūdžio sistema, kurios pagalba nustatomi platformų ir įmonių įsipareigojimai kovoti su dezinformacija.

Taip pat ši savireguliavimo sistema nustato, kad interneto technologijų platformos neprivalo įgyvendinti jokios konkrečios praktikos, tačiau sutinka reguliariai pranešti apie savo veiklą Europos Komisijai. Galiausiai paskatos įgyvendinti DPK daugiausia priklauso nuo pačių interneto technologijų įmonių. Pabrėžtina, jog šiuo metu nėra jokios bendros privalomos sistemos, tikslingai sukurtos kovai su dezinformacija internete (De Cock Buning 2018).

DPK peržiūros sistema audituoja penkias pagrindines sritis: reklamos tikrinimas, problemomis pagrįsta reklama, paslaugų vientisumas, vartotojų įgalinimas ir mokslinių tyrimų bendruomenės įgalinimas.

Nagrinėjant DPK veiksmingumą, galime pastebėti, jog praėjus dvejiems metams nuo DPK įgyvendinimo, rezultatai yra nevienodi. Nors Europos Komisija gyrė pasirašiusiųjų visapusiškas pastangas įtraukti faktų tikrintojus, tačiau pati Europos Komisija pastebi DPK įgyvendinimo greičio ir apimties problematiką įvairiose interneto technologijų platformose. Visa apimanti problema yra tai, jog savanoriškas DPK pobūdis neskatina konkretaus struktūrinio platformų bendradarbiavimo (Europos Komisija 2020). Platformoms negresia materialinės sankcijos už įgyvendinimo nesėkmes. Sunkiausia pasekmė – galimas pašalinimas iš DPK ir su tuo susijusi reputacijos žala.

Konstatuotina, kad dezinformacija Europoje atsiranda dėl paliktos savireguliacijos eigos, kuri turi baigtis. DPK, nors ir nustato svarbius įsipareigojimus, tačiau yra nepakankamai įgyvendinamas ir suteikia skaitmeninėms platformoms per daug veiksmų laisvės.

Dėl šios diskrecijos, kaip pripažino Europos Komisija, atsirado didelių įgyvendinimo spragų, kurios neleido koordinuotai reaguoti į dezinformaciją internete visoje Europoje (Madiega 2020). Tačiau tikėtina, jog būsimas Skaitmeninių paslaugų įstatymas (Europos Parlamentas ir Europos Taryba 2020) (toliau – SPĮ), įdiegs didesnį skaidrumą ir deramą patikrą, taip užtikrinant, kad interneto technologijų bendrovės būtų atsakingos už žalingą turinį savo platformose.

Svarbu pažymėti, kad ne viskas taip paprasta. Reaguojant į dezinformaciją vis dar kyla didelių spragų, o SPĮ nepašalina daugelio iš jų. Pagrindinis klausimas, dėl kurio diskusijos turėtų būti nukreiptos į ateitį, yra tai, ar žalingas, bet teisėtas turinys ir toliau turėtų vengti reguliavimo vien dėl to, kad jis pats savaime nėra neteisėtas?

Kaip nurodoma Europos Sąjungos Demokratijos veiksmų plane (Europos Komisija 2020) – teisė į laisvus ir sąžiningus rinkimus ir žiniasklaidos laisvės stiprinimas turėtų būti besikeičiančios darbotvarkės centre. Atitinkamai, reikia atsižvelgti į keletą svarbių dalykų. Pirma, ne visos dezinformacijos formos, o tik kai kurios iš jų yra neteisėtos. Ypač tuomet, kai yra pastebimi diskriminacinės ar rasistinės dezinformacijos aspektai, kurie gali prieštarauti tiek vidaus teisės aktams, tiek Europos Sąjungos teisei.

Antra, privalomų dezinformacijos taisyklių taikymas nebūtinai turi pasireikšti įpareigojimais pašalinti turinį. Turi būti taikomos apčiuopiamos ir konkrečios sankcijos platformoms, kurios nesugeba sumažinti dezinformacijos. Tai galėtų būti pagrįsta remiantis apsauga Europos Sąjungos demokratijai.

Akivaizdu, kad reikia griežtesnės priežiūros, suderintų požiūrių ir geresnės prieigos prie svarbių žinių, kaip ir kur dezinformacija atsiranda Europos Sąjungoje. Dėl nuolatinių

dabartinės sistemos trūkumų, ilgalaikiai klausimai, susiję su dezinformacijos įstatymu ir saviraiškos laisvės kompromisu, kol kas ir toliau liks neatsakyti (Helm and Nasu 2021)

Vis dėlto suprantama, kad dezinformacija sukelia unikalią teisinę problemą Europoje, kuri reikalauja nustatytos teisėkūros darbotvarkės, kurios pagrindu pagaliau baigtųsi interneto technologijų bendrovių savireguliacija. Dezinformacijos įtaka valstybių demokratijoms susiduria su nauja realybe. Europos Sąjunga išgyvena vidines dilemas nustatant pusiausvyrą tarp žodžio laisvės ir teisės būti tinkamai informuotam. Europos Žmogaus Teisių Teismas nedviprasmiškai yra pareiškęs, kad vyriausybės (ir tuo pačiu Europos Sąjunga) negali nutildyti kalbos remdamosi tuo, kad ji kvestionuoja oficialią nuomonę, nes vienas iš pagrindinių žodžio laisvės tikslų yra apsaugoti mažumų balsus, nes jie gali prisidėti prie diskusijų visuotinės svarbos klausimais (Colomina 2019).

Teigtina, kad savanoriškos internetinių platformų priemonės kovojant su dezinformacija yra nepakankamos. Todėl turime suprasti, jog Europos Sąjunga, o ypač JAV, per daug pasikliauja gera interneto veikėjų valia. Europos Sąjungai ir jos valstybėms narėms reikėtų taikyti veiksmingas sankcijas interneto technologijų bendrovėms, jeigu būtų nesilaikoma taisyklių. Tačiau yra problema, jog faktų tikrintojams daugeliu atveju apibrėžti netikras naujienas ir atskirti jas nuo kraštutinių pažiūrų išraiškos yra labai nelengva. Kritikai pagrįstai baiminasi, kad taip gali būti pažeista žodžio laisvė.

Remiantis aukščiau išdėstytomis žiniomis pastebime, kad šiuo laikotarpiu Europos Sąjungai kovojant su dezinformacija dabartinis teisinis reguliavimas nėra pakankamas. Dabartiniai dokumentai ir strategijos yra tik deklaratyvaus pobūdžio. Todėl šiuo metu vyraujantis teisinis neapibrėžtumas ir teisinio reglamentavimo stoka dezinformacijos atžvilgiu, kelia grėsmę tiek atskirų valstybių, tiek ir visos Europos Sąjungos demokratinei santvarkai.

3.2. Internetinio balsavimo problematika Europos Sąjungos kontekste

Per pastaruosius du dešimtmečius dinamiška interneto technologijų plėtra bei didžiulis visuomenės entuziazmas paskatino internetinio balsavimo programų diegimus visame pasaulyje. Tai sukėlė plačias diskusijas dėl internetinio balsavimo naudos ir rizikos demokratiniam valstybių valdymui.

Europos Sąjungos viešųjų institucijų ir Europos Sąjungos valstybių narių teisinis reglamentavimas bei pozicijos, aiškiai atspindi internetinio balsavimo problematiką demokratiniam valstybių valdymui. Tad svarstant balsavimo internetu įvedimą Europos Sąjungoje, konkrečiai Europos Parlamento rinkimuose, pirmiausia reikia pabrėžti, kad bet kokia balsavimo internetu programa turi būti sukurta ir įvertinta atsižvelgiant į pagrindinius Europos rinkimų principus, įtvirtintus dabartiniuose Europos Sąjungos teisės aktuose. Atsižvelgiant į tokią principais pagrįstą perspektyvą, teisinėje analizėje dėmesys turėtų būti skiriamas balsavimo internetu poveikiui rinkimų teisės principams.

Išskiriami penki pagrindiniai Europos rinkimų principai (Act concerning the election of the representatives of the Assembly by direct universal suffrage 1976 (No. L 278, 8.10.1976)): 1) visuotinė rinkimų teisė, 2) lygi rinkimų teisė, 3) laisva rinkimų teisė, 4) balsavimo slaptumas, 5) tiesioginė rinkimų teisė.

Antra, vertinant internetinio balsavimo galimybes Europos Sąjungoje reikėtų atsižvelgti ir į balsavimo internetu pasekmes bei išorines grėsmes, kurias pastaruoju laikotarpiu Europos Sąjunga dažnai išgyvena. Įvertinant internetinio balsavimo instituto atitiktį Europos rinkimų principams ir internetinio balsavimo pasekmes bei išorines grėsmes, turime taip pat suprasti internetinio balsavimo grėsmes ir galimybes.

Skiriant dėmesį pirmajam aspektui dėl pagrindinių Europos rinkimų principų laikymosi, reikia remtis internetinio balsavimo pasekmių analize (Garrone 2004), kurioje yra padaryta išvada, kad balsavimas internetu nekelia jokios grėsmės visuotiniam rinkimų teisės principui, pagal kurį kiekvienas pilietis turi teisę balsuoti. Tačiau pažymėtina, kad šiam principui gali būti pakenkta reglamentavus balsavimą tik internetu, kaip vienintelį balsavimo būdą, nes tuomet piliečiams, neturintiems prieigos prie interneto, gali būti atimta teisė balsuoti. Lygias rinkimų teises užtikrinti internetinio balsavimo būdu nėra taip paprasta, kaip taikant tradicines balsavimo priemones, kurios reikalauja rinkėjų tapatybės nustatymo vietoje, tačiau atkreiptinas dėmesys, kad tokia problematika yra būdinga ir balsavimui paštu.

Žinoma, jog kai kurios valstybės narės pasisako už internetinio balsavimo įvedimą, kai kurios nori laikytis tradicinių metodų. Ar tada galima susitaikyti su situacija kur vienos

valstybės įgyvendina internetinį balsavimą, o kitos ne? Europos įstatymai šiuo atžvilgiu yra gana aiškūs – tai, kas netaikoma iš dalies pakeistam 1976 m. Aktui (Act concerning the election of the representatives of the Assembly by direct universal suffrage 1976 (No. L 278, 8.10.1976)), priklauso valstybių narių ir jų vidaus kompetencijos.

Kitaip tariant, Europos parlamento rinkimų įstatymų skirtumai yra ir bus įprastas dalykas, net jeigu ir būtų įvestas internetinis balsavimas visoje Europos Sąjungoje. Lygybės problema, regis, kyla priklausomai nuo to, ar įvyks rinkimai Europos Sąjungos ar nacionaliniu lygiu. Žinoma, būtų galima įžvelgti ir dvigubų standartų, jeigu Europos Sąjungos valstybė reglamentuotų internetinį balsavimą Europos Parlamento rinkimuose, tačiau remdamasi savo iniciatyva ir Europos Sąjungos teise, tokios galimybės savo piliečiams nacionaliniuose rinkimuose nesuteiktų. Toks diferencijavimas būtų neteisingas. Rinkėjai galėtų jaustis nusivylę ir nebūtinai suprasti, kodėl Europos Parlamento rinkimuose naudojamas internetinio balsavimo metodas, nacionaliniuose rinkimuose - nėra taikomas.

Nors atrodytų, kad balsavimas internetu laisvam rinkimų teisės principui didelės grėsmės nekelia, tačiau grėsmes galima įžvelgti atskiruose šeimos narių balsavimuose. Galiausiai laisvo balsavimo užtikrinimas labai priklauso nuo internetinio balsavimo sistemos konstrukcijos ir kokybės – rinkėjams internetu turėtų būti suteikiama teisė esant reikalui pakeisti savo balsą iki tam tikro nustatyto termino. Aišku, toks reglamentavimas keltų papildomų klausimų dėl laisvos rinkimų teisės įgyvendinimo.

Vertinant balsavimo slaptumo principą, svarbu nurodyti, kad šis principas yra užtikrinamas keletu tarptautinių taisyklių, įskaitant ir 1976 m. Aktu (Europos Tarybos sprendimas 2002 (2002/772/EB, Euratom)), kuriame nurodyta: „Rinkimai vyksta tiesiogiai visuotine rinkimų teise, kuri yra laisva ir slapta“. Taip pat Europos Sąjungos pagrindinių teisių chartijos (Charter of Fundamental Rights of the European Union 2000 (2000/C 364/01)) 39 straipsnio 2 dalis patvirtina, kad Europos Parlamento nariai renkami remiantis tiesiogine, visuotine rinkimų teise, laisvu ir slaptu balsavimu.

Tačiau manytina, kad balsavimas internetiniu būdu neatitiks slapto balsavimo principo, kurie yra įtvirtinti 1976 m. Akto 1 straipsnyje (Gibson et al. 2003). Tokie įsitikinimai yra pagrįsti tuo, kad identifikavimo reikalavimai yra griežtesni už patį balsavimą. PIN kodo ir/ar elektroninio parašo naudojimas leidžia pareigūnams sekti elektroninius veiksmus, susiejančius atiduotą balsą su rinkėju. Kita vertus, visiškas slaptumas yra užtikrinamas tik tradicinio balsavimo atveju.

Pripažįstama, jog balsavimo internetu įgyvendinimas „turėtų būti griežtai nustatytas įstatymu“ (Auer and Mendez 2005). Kitaip tariant, nustatyti teisinį balsavimo internetu

įvedimo pagrindą yra svarbus iššūkis, kurį reikia spręsti svarstant galimybę šią naują balsavimo procedūrą taikyti visoms valstybėms narėms.

Remiantis šiais argumentais iškyla esminis klausimas – kokiu lygiu turėtų būti kuriama ir įgyvendinama teisinė bazė: bendru Europos Sąjungos lygiu ar atskirai valstybėse narėse? Aueris ir Mendezas pažymi (Auer and Mendez 2005), kad „Sutarties 190 straipsnio 4 dalis (Europos Sąjungos veikimo sutartis 2012 (OJ C 326, 26.10.2012)) numato, kad Europos Parlamentas parengia pasiūlymą dėl būtinų nuostatų, jog jo narius būtų galima išrinkti remiantis tiesiogine visuotine rinkimų teise, priėmimo pagal visose valstybėse narėse taikomą vienodą tvarką arba pagal visoms valstybėms narėms bendrus principus. Tačiau toks teisinis reglamentavimas internetinio balsavimo Europos Sąjungoje įdiegimo procedūrose susidūrė su daugybe kliūčių, kadangi Europos Parlamentas negalėjo priimti bendro internetinio balsavimo visoms valstybėms narėms nepaisant pasikartojančių bandymų. Tokias pasekmes lemia atskirų valstybių narių nelankstumas ir nuomonių įvairovė, kurios pagrindinė kliūtis – skirtingas požiūris į vienodą rinkimų procedūros nustatymą.

Galima teigti, jog visiško vienodumo paieška, internetinio balsavimo reglamentavimo Europos Sąjungos kontekste yra sunkiai įmanoma. Internetinis balsavimas gali būti įdiegimas nebent kiekvienoje valstybėje narėje atskirai, taip administruojant rinkimų rezultatus decentralizuotai.

Suprantama, jog Europos Sąjungos lygmeniu, internetinio balsavimo procedūros decentralizavimas būtų ambicingas tikslas, skirtas įtraukti įvairias valstybes nares, pasinaudojant jau egzistuojančiomis reglamentavimo struktūromis. Tačiau įvertinant internetinio balsavimo grėsmes išties svarbu apsaugoti internetinio balsavimo sistemas nuo kibernetinių atakų, kurios galėtų sukelti plataus masto pavojų demokratinių valstybių santvarkoms.

Vertinant internetinio balsavimo grėsmes Europos Sąjungos kontekste svarbu atkreipti dėmesį ir į tai, kad 1976 m. Europos Parlamento akto (Act concerning the election of the representatives of the Assembly by direct universal suffrage 1976 (No. L 278, 8.10.1976)), 8 straipsnyje yra nustatyta „vieno žmogaus, vieno balso“ taisyklė, kuri reiškia, jog Europos Parlamento rinkimuose niekas negali balsuoti daugiau nei vieną kartą.

Atsižvelgiant į tai, kad internetinio balsavimo metu balsavimas vyktų visose valstybėse, galimai net ir už Europos Sąjungos ribų, kyla pavojus, jog būtų pastebimi šios taisyklės pažeidimai, kurie gali likti taip ir nesankcionuoti. Problema yra sudėtinga, kadangi internetinio balsavimo schemos beveik neabejotinai priklausytų nuo skirtingų ir galbūt nesuderinamų programų, standartų ir autentifikavimo procedūrų tarp skirtingų valstybių

narių. Tad optimistiniu atveju svarstant apie internetinio balsavimo įvedimą, būtina priimti internetinio balsavimo teisės aktus, kuriais būtų apribotos valstybių narių piliečių teisės balsuoti internetu ne valstybėse narėse.

Svarbu pabrėžti, jog taip pat vienas iš pagrindinių su internetinio balsavimo įdiegimu siejamų klausimų yra saugumo užtikrinimas balsuojant internetu. Todėl turi būti skiriamas didelis dėmesys balsavimo internetu sistemos saugumui. Europos Sąjungos atskirų valstybių praktikoje matoma, jog visuotinis internetinis balsavimas nėra plačiai įdiegiamas. Norvegija išbandžiusi internetinį balsavimą 2011 m. ir 2013 m. nusprendė internetinio balsavimo atsisakyti, kadangi suvokė šio balsavimo saugumo problematiką.

Prancūzija pasiūliusi balsuoti internetu Prancūzijos piliečiams gyvenantiems užsienyje 2012 m. vykstančiuose parlamento rinkimuose, taip pat nusprendė nutraukti šią internetinio balsavimo praktiką prieš 2017 m. vyksiančius parlamento rinkimus, kadangi buvo baiminamasi kibernetinių atakų įsikišimo. O Suomija 2016 m. svarsčiusi internetinio balsavimo reglamentavimą, taip pat atsisakė tokių planų, remdamasi darbo grupės rekomendacija.

Estija šiuo atveju yra priešingas pavyzdys. Likusi Europa su pavydu stebėjo kaip Estija stiprina savo demokratinę sistemą, naudodama naujausias technologijas ir taip tapdama pirmąja Europos Sąjungos valstybe pradėjusia balsuoti internetu. Tačiau šis sėkmingas transformavimasis į pirmąją Europoje visiškai internetiniu būdu balsavusią valstybę nebuvo toks sėkmingas. Šis pavyzdys vertas dėmesio, atsižvelgiant ir į tai, jog 2007 m. Estija patyrė didžiulę kibernetinę (Microsoft EU Policy blog 2018) ataką, dėl kurios buvo uždarytos vyriausybės, bankininkystės ir žiniasklaidos svetainės. Atrodytų, kad po tokio sukrėtimo Estijos vyriausybė turėjo atsisakyti tuometinio teisinio reglamentavimo dėl internetinio balsavimo, tačiau užuot atsitraukusi nuo internetinio balsavimo, šalis išmoko vertingų pamokų ir tapo pasaulio internetinio balsavimo pioniere.

Verta paminėti, kodėl estai nusprendė įvesti internetinį balsavimą. Jų sprendimą lėmė mažas rinkėjų aktyvumas ir kova su politiniu susvetimėjimu (Madise and Martens 2006). 2005 m. gegužės mėn. Estijos parlamentas priėmė įstatymą, kuriuo reglamentavo galimybę balsuoti internetu 2005 m. spalį vyksiančiuose šalies savivaldos rinkimuose. 2007 m. vasario mėn. Estija išplėtė internetinį balsavimą nacionaliniuose parlamento rinkimuose ir galiausiai šią technologiją panaudojo per 2009 m. Europos Parlamento rinkimus (Charles 2009).

Galima manyti, kad Estijos pavyzdys, kuris dažnai yra idealizuojamas, turėjo nustatyti praktiką likusiai Europos Sąjungai, tačiau situacija yra priešinga, nes dauguma tyrimų, pagrįstų suvestiniais duomenimis, nenurodo beveik jokio internetinio balsavimo poveikio

rinkėjų aktyvumui (Henry 2003). Tai galioja ir Estijos pavyzdžiui, kadangi analizuojant rinkimų duomenis iš 234 Estijos savivaldybių, darytina išvada, kad internetinis balsavimas neturi jokios pastebimos įtakos demokratiniams rinkimams (Palities and Bochsler 2010).

Nors ir šiuo metu Estija turi nusistovėjusį internetinio balsavimo rinkimuose mechanizmą, Mičigano universiteto atlikta nepriklausoma saugumo analizė (Michigan University 2014) nurodė, kad Estijos internetinio balsavimo rinkimų sistemoje kyla daug pavojų, įskaitant programinės įrangos pažeidžiamumą ir asmens duomenų saugumo klaidas. Pažymėtina, jog Estija yra vienintelė Europos Sąjungos šalis, savo piliečiams siūlanti visuotinio balsavimo internetu galimybę, šios valstybės internetinio balsavimo sistema yra nuolat vertinama ir atnaujinama, siekiant užtikrinti, kad būtų naudojamos naujausios technologijos demokratijos pagrindams apsaugoti.

Tačiau per pastaruosius daugiau nei penkiolika metų įvykę įsilaužimai bei kišimąsi į rinkimus JAV ir Europoje, atkreipė demokratinių valstybių dėmesį į kibernetines atakas nukreiptas prieš demokratinius procesus. Atsižvelgiant į tai, Europos Sąjunga vis dar neturi vieningo požiūrio dėl internetinio balsavimo technologijų. Nors Europos Komisija deda pastangas siekdama užtikrinti, kad kiekviena valstybė narė žinotų apie galimą pavojų jų rinkimų aplinkai, tačiau valstybės narės išlieka labai atsargios.

Apibendrinant galima teigti, kad susidomėjimas rinkimų technologiniais sprendimais yra išties didelis, tačiau šiuo metu egzistuojantys internetinio balsavimo pavyzdžiai kelia daug abejonių dėl tinkamo šio instituto įgyvendinimo. Pabrėžtina, kad internetinio balsavimo Europos Sąjungos kontekste grėsmės atsveria galimas internetinio balsavimo galimybes. Tai įrodo tiek valstybių narių praktika, tiek ir bendra Europos Sąjungos viešųjų institucijų veikla bei skirtingos valstybių narių pozicijos, kurios leidžia daryti išvadą, jog šiuo laikotarpiu Europos Sąjungoje yra skeptiškai žvelgiama į bendrą internetinio balsavimo teisinio reguliavimo nustatymą valstybėse narėse.

3.3. Interneto technologijų sukelti duomenų apsaugos iššūkiai demokratijai

Visame pasaulyje vis daugiau dėmesio skiriama duomenų privatumui. 2015 m. paskelbtame Frank Pasquale darbe (Frank Pasquale 2015) pastebima, kad technologiniai algoritmai pakeitė šiuolaikinę visuomenę, nors didžiųjų duomenų problemas dekonstruoti nėra lengva. Praėjus metams po Frank Pasquale knygos išleidimo, nedaugelis galėjo nuspėti, kad algoritminiais įrankiais kartu su sudėtingų šiuolaikinių kampanijų pobūdžiu, galima manipuliuoti JAV rinkėjais 2016 m. prezidento rinkimuose.

Rusijos kišimasis į 2016 m. JAV rinkimus sukėlė susirūpinimą dėl interneto technologijų kaupiamų duomenų įtakos demokratiniams procesams. 2018 m. „Cambridge Analytica“ skandalas tapo simboliu iliustruojančiu neteisėtą kišimąsį į demokratinius rinkimus. Šis skandalas kilo 2018 m. kovo 17 d. (Lapowsky, I 2019) kuomet viename interviu pagrindinės Cambridge Analytica įmonės tyrimų direktorius paaiškino, jog psichografinis profiliavimas leido „Cambridge Analytica“ paveikti rinkėjus naudojant socialinės žiniasklaidos duomenis.

Vykstantys tyrimai JAV galiausiai atskleidė, jog maždaug 87 milijonų „Facebook“ naudotojų duomenis surinkęs tyrėjas, o vėliau juos panaudojusi įmonė, padarė didžiulę įtaką demokratiniams procesams JAV (Kang and Frenkel 2018). Po „Cambridge Analytica“ ir „Facebook“ skandalo Federalinė prekybos komisija pradėjo šio pažeidimo tyrimą.

2019 m. liepos 24 d., „Facebook“ buvo skirta rekordinė 5 milijardų dolerių bauda bei buvo priimtas Federalinės prekybos komisijos įsakymas nustatyti naujus privatumo standartus (Kang 2019) tam, kad daugiau tokie atvejai, kuomet remiantis privačių asmenų duomenimis būtų daroma įtaka demokratiniams procesams, nepasikartotų.

Cambridge Analytica“ skandalas atskleidė, kaip lengva politinėms kampanijoms panaudoti socialinės žiniasklaidos duomenis, siekiant manipuliuoti rinkėjais tam, kad jie balsuotų tam tikru būdu. Vertinant tuo metu susiklosčiusią situaciją iškyla klausimai – kokių veiksmų ėmėsi įstatymų leidėjai ir kaip pasikeitė privatumo įstatymai po „Facebook“ duomenų skandalo?

Europos Sąjunga ėmėsi pirmųjų žingsnių masinės duomenų apsaugos srityje ir dar 2016 m. priėmė Bendrąjį duomenų apsaugos reglamentą (Europos Parlamento ir Tarybos reglamentas 2016 (2016/679)) (toliau – BDAR), o po dvejų metų jis įsigaliojo ir išplėtė teises į duomenų privatumą bei nustatė griežtas taisykles, kaip įmonės turėtų tvarkyti asmens duomenis.

Europos Sąjunga priimdama šį reglamentą siekė išspręsti susiklosčiusias duomenų apsaugos privatumo problemas. Apskritai Europos Sąjunga norėjo, kad reglamentas būtų

nuosekliai priimtas visoje Europoje, būtų sustiprintos duomenų perdavimo už Europos Sąjungos ribų taisyklės ir taip būtų suteiktą asmenims daugiau galimybių valdyti savo asmens duomenis. Europos Sąjungoje BDAR pakeitė įmonių, įskaitant „Facebook“, duomenų saugojimo ir naudojimo būdus.

Pažymėtina, kad įgyvendinus BDAR vartotojai turi daug daugiau galimybių valdyti savo duomenis – svarbiausia, jie turi teisę būti pamiršti, o tai reiškia, jog šią informaciją turinti įmonė privalo ištrinti visus su tuo asmeniu susijusius įrašus. Jeigu to nepadaro, tuomet jai gresia bauda, kuri gali siekti 4 proc. įmonės pasaulinių pajamų arba 20 milijonų eurų, atsižvelgiant į tai, kuri suma didesnė. Ironiška, bet jeigu „Cambridge Analytica“ skandalo metu būtų galiojęs BDAR, tuomet Jungtinės Karalystės informacijos komisaro biuras būtų skyręs ne 500 000 svarų baudą, o 4% „Facebook“ pasaulinės metinės apyvartos. Bendra baudos suma būtų buvusi 315 milijonų eurų (Statista 2021).

BDAR yra didžiulis žingsnis stipresnės privatumo apsaugos link. Duomenų naudojimas tapo gyvybiškai svarbus šių dienų visuomenei – duomenys pakeitė naftą kaip vertingiausią pasaulio išteklį. Taigi tikimybė, jog asmens duomenimis bus piktnaudžiaujama, yra didelė, todėl asmenys turi būti apsaugoti tam tikrais teisės aktais.

Tuo tarpu, stebėtina, kad JAV neturi vieno bendro pagrindinio duomenų apsaugos teisės akto. JAV šiuo metu galioja šimtai įstatymų priimtų tiek federaliniu, tiek valstijų lygiu. Pavyzdžiui, Federalinės prekybos komisijos įstatymas (Federal Trade Commission Act (15 U.S.C. 41 et seq.) iš esmės apsaugo vartotojus nuo nesąžiningos ar apgaulingos praktikos ir užtikrina federalinį privatumą bei duomenų apsaugos taisykles. Šiame įstatyme nustatyta, jog apgaulinga praktika apima įmonės privatumo taisyklių nesilaikymą ir nesugebėjimą tinkamai užtikrinti asmeninės informacijos saugumą, be apgaulingos reklamos ar rinkodaros metodų naudojimo.

Nors nėra bendro federalinio įstatymo, turinčio įtakos duomenų apsaugai, yra keletas federalinių duomenų apsaugos priemonių sektoriui būdingų įstatymų. Pavyzdžiui, 1994 m. Vairuotojo privatumo apsaugos įstatymas (18 U.S. Code § 2721) reglamentuoja valstybės motorinių transporto priemonių departamentų surinktos asmeninės informacijos privatumą ir atskleidimą.

Pabrėžtina, kad taip pat vaiko informacija yra saugoma federaliniu lygmeniu pagal Vaikų privatumo internete apsaugos įstatymą (15 U.S. Code § 6501), kuris draudžia rinkti bet kokią informaciją iš vaikų jaunesnių nei 13 metų, prisijungusių prie skaitmeniniu įrenginių. Šis įstatymas reikalauja paskelbti privatumo pranešimus ir rinkti tėvų sutikimus, kuomet informacija iš vaikų yra renkama. Taip pat ir Vaizdo įrašų privatumo apsaugos

įstatymas (18 US Code § 2710) riboja nuomos ar pardavimo atskleidimą susijusį su vaizdo įrašų ar panašiais vaizdo, garso medžiagos įrašais, įskaitant transliacija internetu.

Kiti JAV įstatymai taip pat nustato apribojimus ir įpareigojimus įmonėms, susijusiomis su duomenų rinkimu, naudojimu, atskleidimu, sauga arba specialių kategorijų informacija, pvz., biometrinių duomenų, medicininiais įrašais, vairuotojo pažymėjimo informacija, pašto adresais, bibliotekos įrašais, televizijos žiūrėjimo įpročiais, finansiniai įrašais, mokesčių įrašais, draudimo informacija, telefono įrašais ir t.t. Kiekviena atskira JAV valstija yra priėmusi atskirus pranešimo dėl duomenų pažeidimų teisės aktus. Tačiau kai kurios valstijos yra labiau pažengusios nei kitos, kuomet yra kalbama apie asmens duomenų apsaugą.

Pavyzdžiui, Masačiusetse galioja griežti duomenų apsaugos reglamentai (The Massachusetts General Law Chapter 93H 2021 (201 CMR 17.00)), reikalaujantys, kad bet kuris subjektas, kuris gauna, saugo, prižiūri, apdoroja ar kitaip turi prieigą prie Masačiusetso gyventojo asmeninės informacijos, kuri yra susijusi su prekių ar paslaugų teikimu arba susijusia su užimtumu – a) turi įgyvendinti ir prižiūrėti išsamų rašytinį informacijos saugumo planą, apimantį 10 pagrindinių standartų,b) nurodytas subjektas privalo sukurti ir prižiūrėti oficialią informacijos saugumo programą, atitinkančią aštuonis pagrindinius reikalavimus, kurie apima reikalavimus susijusius nuo šifravimo iki informacijos saugumo mokymų.

Tuo tarpu, 2019 m. Niujorkas išplėtė pranešimų apie duomenų pažeidimus įstatymą (N.Y. Gen Bus. Law § 899–bb), įtraukdamas aiškų reikalavimą, jog subjektai sukurtų, įgyvendintų ir prižiūrėtų „pagrįstas“ apsaugos priemones, skirtas apsaugoti privačios informacijos saugumą, konfidencialumą ir vientisumą. Svarbu tai, kad šis Niujorko įstatymas (N.Y. Gen Bus. Law § 899–bb) nustato daugybę administracinių, techninių ir fizinių apsaugos priemonių. Ne išimtis ir Ilinojaus valstija, kurioje galioja išskirtinai platus Biometrinės informacijos privatumo įstatymas (Biometric Information Privacy Act. 2008 (740 ILCS 14/), kuris nustato reikalavimus verslui bei renka ar kitaip gauna biometrinę informaciją. Ilinojaus biometrinės informacijos privatumo įstatymas yra vienintelis Ilinojaus valstijos įstatymas, reglamentuojantis biometrinių duomenų naudojimą, kuris leidžia privatiems asmenims pareikšti ieškinį ir išieškoti žalą esant duomenų apsaugos pažeidimui.

Kalifornijoje jau seniai yra priimti teisės aktai dėl asmens duomenų privatumo, o 2018 m. valstija priėmė Kalifornijos vartotojų privatumo įstatymą (California Consumer Privacy Act 2018 (Assembly Bill No. 375). Šiuo 2020 m. sausio 1 d. įsigaliojusiu įstatymu buvo nustatyti nauji įpareigojimai apdraustam verslui, įskaitant reikalavimus atskleisti asmeninės

informacijos kategorijas verslui, kuris renka duomenis apie vartotojus. Taip pat buvo įvestos naujos teisės Kalifornijos gyventojams, įskaitant teisę prašyti prieigos prie asmeninės informacijos, teisę ištrinti surinktus asmeninius duomenis ir teisę atsisakyti perduoti asmeninę informaciją trečiosioms šalims. Sekdama Kalifornijos pavyzdžiu, 2021 m. pradžioje Virdžinija priėmė Vartotojų duomenų apsaugos įstatymą (Virginia Consumer Data Protection Act 2021 (SB 1392)) ir tapo antrąja valstija reglamentavusia išsamias duomenų privatumo taisykles.

Taigi nors JAV neturi bendro duomenų apsaugos reguliavimo, tačiau institucijos federaliniu lygiu dažnai nustato bendrą toną federalinio privatumo ir duomenų saugumo klausimais. Pažymėtina, jog JAV neturint bendrų teisės aktų, užtikrinančių vartotojų privatumą, atsirado keletas alternatyvių modelių, skirtų spręsti su asmens duomenų apsauga susijusias problemas. „Facebook “ ir „Google“ įdiegė vartotojų tyrimų programas, kurios tiesiogiai kompensuoja žmonėms žalą už jų savanorišką duomenų dalijimąsi (Peters 2019). Pavyzdžiui startuolis, „Ozone AI“ siūlo savo vartotojams tiesioginius, reguliarius mokėjimus už savanorišką vartotojų asmeninių duomenų perdavimą.

Deja, kol šios milžiniškos technologijų įmonės dar nėra priverstos perrašyti savo verslo modelių veikimo, tol jų tokio pobūdžio veikimas dar labiau paskatins vis didėjantį piktnaudžiavimą vartotojų duomenų privatumu. Įstatymų leidėjai turi būti suinteresuoti apsaugoti savo piliečius ir priversti interneto technologijų įmones užtikrinti, kad vartotojų duomenys būtų tvarkomi tinkamai.

Apibendrinant galime teigti, jog įstatymų leidėjai tik pradeda spręsti problemas. Pastaruoju metu vykdoma teisėkūros veikla buvo sutelkta į asmens privatumo apsaugą, reikalaujant, kad interneto technologijų platformos suteiktų vartotojams daugiau galimybių valdyti savo asmens duomenis. Atrodo, jog Europos Sąjunga yra ryški lyderė duomenų apsaugos klausimu lyginant su JAV, tačiau tinkamas duomenų apsaugos reglamentavimas toliau išlieka labai svarbus, nes netinkamas asmens duomenų tvarkymas gali sukelti žalą demokratinių valstybių sistemoms, neteisėtai manipuliuojant rinkėjų duomenimis. Pažymėtina, jog apgalvotas teisinis reglamentavimas asmens duomenų apsaugos atžvilgiu yra įrankis, kuris padėtų apsaugoti demokratinių valstybių santvarkas.

3.4. „Deepfake“ – kita didelė grėsmė demokratijai?

Naujos kartos skaitmeninė interneto technologija, kuria manipuliuojant galima generuoti labai tikroviškus vaizdo įrašus. Visa tai yra realybė, kadangi naujoji technologija pavadinimu „deepfake“ sukėlė didelį tiek mokslo, tiek politinės bendruomenės susirūpinimą dėl galimo šios technologijos naudojimo netinkamiems tikslams pasiekti – pakenkti demokratiniams procesams.

Akivaizdu, jog dirbtinio intelekto pažanga leido sukurti itin tikroviškus netikrus vaizdo įrašus, kuriuose yra vaizduojamas asmuo atliekantis veiksmus, kurių jis niekada neatliko (Bateman 2020). Populiarus ir universalus terminas, kuris dažnai vartojamas šiai technologijai apibūdinti – „deepfake“.

Šiame darbe „deepfake“ suprantamas kaip manipuliuojamas arba sintetinis garso ir/ar vaizdo įrankis, kuris atrodo autentiškai, nes turi tam tikro asmens bruožus bei atlieka veiksmus, kurie niekada tikrojo asmens nebuvo pasakyti ar padaryti. Šie veiksmai sukuriami naudojant dirbtinio intelekto metodus, įskaitant pačios interneto technologijos savarankišką mokymąsi.

Ryškūs „deepfake“ pavyzdžiai yra matomi vaizdo įrašuose, kuriuose buvęs JAV prezidentas Barackas Obama įžeidžia savo įpėdinį Donaldą Trumpą arba Donaldas Trumpas ragina Belgijos vyriausybę pasitraukti iš Paryžiaus Klimato susitarimo. Tačiau tokie vaizdo įrašai, kurie iš pirmo žvilgsnio gali pasirodyti juokingi, iš tikrųjų gali būti tik problemos ledkalnio viršūnė. Spartus šios technologijos augimas interneto technologijų tarpe gali sukelti didžiulę žalą demokratinių valstybių santvarkoms, taip paliekant jas pažeidžiamomis (Bateman 2020).

Atrodytų, jog „deepfake“ neigiamas poveikis demokratijai gali būti didesnis negu kitų interneto technologijų. Kai kurie ekspertai mano, jog prognozuojant niūresnį scenarijų, galime sulaukti ir tokio atvejo, kuomet nebegalėsime tikėti skaitmeniniu turiniu, nes viskas ką mes matysime, galimai bus manipuliatyvu (Schick 2020). Tokiu atveju turėtume situaciją, kuomet būtų destabilizuota visa visuomenė. Iš esmės „deepfake“ sukeltų neigiamą poveikį ne tik asmenų privatumui, bet ir demokratiniam valstybių valdymui bei nacionaliniam saugumui. „Deepfake“ gali būti panaudojamas kaip dezinformacijos skleidimo priemonė (Vaccari and Chadwick 2020).

Toks technologinis manipuliavimas yra naujas reiškinys, sukeliantis susirūpinimą šio technologinio įrankio esme. Žinoma vertinant „deepfake“ galime įžvelgti ir teigiamų niuansų. Daugelis žmonių, kurie yra naudoję šiuolaikinį išmanųjį telefoną fotografijai, tikriausiai yra pajutę „deepfake“ technologijų suteikiamą naudą. Dažnai visose fotografijų

programėlėse yra įdiegti grožio filtrai, kurie fotografuojant ar filmuojant automatiškai keičia vaizdus. Pažangesni „deepfake“ gali pakeisti visą veidą, modifikuoti kalbą, taip teisėtai leidžiant interneto technologijų vartotojams kurti satyrą, parodijas ar kitą interneto turinį. „Deepfake“ panaudojimo galimybės leidžia ne tik gerai praleisti laiką, bet ir užsiimti kūrybine raiška.

Tačiau vertinant „deepfake“ bendrąja prasme matyti, jog šis technologinis įrankis gali būti žalingas, ypač šiomis dienomis, kadangi gyvename dezinformacijos kampanijų laikais, kuomet dažnai pasitaiko įvairių priešiškų kampanijų nukreiptų prieš demokratijas. Galima tikėtis, jog „deepfake“ gali pakenkti demokratiniam valstybių valdymui įvairiais būdais: viešiems debatams, rinkimams, viešųjų institucijų legitimumui, mąstymui (Bennett and Livingston 2018).

Pažymėtina, jog yra galimas problematiškas manipuliavimas naujienų žiniasklaida, kadangi ji tiesiogiai susijusi su svarbiais demokratijos procesais. Pavyzdžiui, viešosiomis diskusijomis. Viešųjų diskusijų vientisumas ir kokybė yra labai svarbūs, nes tai yra pagrindinė priemonė padedanti piliečiams formuoti savo politinę nuomonę demokratinėje valstybėje svarbiais klausimais. Tačiau siekiant viešosios diskusijos kokybės, turi būti užtikrintas tam tikras bendras tikrovės pojūtis, apimantis piliečių bendrą suvokimą, kas yra viešosios diskusijos, kas jose dalyvauja ir kokias pozicijas atstovauja viešųjų diskusijų dalyviai.

Pasitelkiant „deepfake“ galima manipuliuoti visais bendros tikrovės jausmo aspektais (Yiping Xia et al. 2019). Tokios manipuliacijos gali sukelti gilumines problemas demokratiniam valstybių valdymui, kadangi pasitelkiant šį technologinį įrankį galima sukelti susiskaldymą ir poliarizaciją pačioje visuomenėje. Taip pat tai gali būti naudojama kaip politinė manipuliacija ir tikslinė propaganda, siekiant padidinti sąmokslo teorijų skaičių, nukreiptų prieš demokratinių valstybių institucijas.

„Deepfake“ taip pat gali padaryti ilgalaikę žalą viešųjų asmenų reputacijai, įskaitant politikų ir kitų išrinktų pareigūnų, taip siekiant manipuliuoti demokratiniais rinkimais. Pavyzdžiui, 2019 m. Malaizijoje plačiai paplito netikras vaizdo įrašas, kuriame yra vaizduojamas politikas, kuris neva pripažino turėjęs homoseksualių santykių su vyriausybės kabineto ministru. Netikrame vaizdo įraše taip pat kalbama apie tariamą ministro korupciją. Dėl šio „deepfake“ įrašo buvo sukeltas vyriausybės koalicijos nestabilumas (Nic Ker 2019). Tokių dezinformacijos pavyzdžių galima pastebėti ir per rinkimus JAV 2016 m. bei Prancūzijoje 2017 m. (Citron and Chesney 2019).

Taigi „deepfake“ pagalba sukurti vaizdo įrašai gali sukelti žalą demokratiniam valstybių valdymui. „Deepfake“ taip pat gali sukelti socialinį susiskaldymą, politinius

neramumus, paniką,konfliktus bei pakenkti visuomenės ir nacionaliniam saugumui. O blogiausiu atveju „deepfake“ gali sukelti smurtinius konfliktus, išpuolius prieš politikus ir galiausiai demokratinių valstybių santvarkos žlugimą. Tad kyla klausimas – ką reikėtų daryti, kad išvengti tokių grėsmių demokratiniam valstybių valdymui? Koks turėtų būti nustatytas teisinis reglamentavimas, jog nebūtų pakenkta demokratinėms santvarkoms?

Pastebėtina, jog ”deepfake“ yra dirbtinio intelekto technologijų produktas, todėl jo naudojimo taisyklės ir reglamentai yra labai svarbūs. 2021 m. balandžio mėn. Europos Komisija paskelbė pasiūlymą dėl vieningo požiūrio į dirbtinio intelekto reguliavimą (Europos Komisija 2021). Pasiūlyme buvo siūlomos įvairios galimybės, kuriomis siekiama sudaryti sąlygas patikimai ir saugiai taikyti dirbtinį intelektą, tuo pat metu gerbiant vertybes ir pagrindines Europos Sąjungos piliečių teises. Šiuo tikslu siūlomame reguliavime nustatomos suderintos dirbtinio intelekto sistemų kūrimo, pateikimo į rinką ir naudojimo taisyklės.

Savo pasiūlymu Komisija siekė uždrausti naudoti dirbtinio intelekto sistemas, kurios kelia nepriimtiną riziką Europos Sąjungos piliečių saugumui ir pagrindinėms teisėms. Dirbtinio intelekto sistemų, kurios patenka į didelės rizikos kategoriją, teikėjai, be kitų reikalavimų, būtų įpareigoti atlikti rizikos vertinimą, numatyti dokumentaciją ir žmogaus priežiūrą bei užtikrinti aukštą duomenų kokybę.

Svarbu pažymėti, kad šiame pasiūlyme nurodyta, jog yra leidžiama naudoti „deepfake“, tačiau tuo pačiu yra suformuluoti kai kurie minimalūs reikalavimai, ypač susiję su skaidrumo įpareigojimais. „Deepfake“ kūrėjai privalo pažymėti savo turinį taip, kad visiems būtų aišku, jog jie susiduria su manipuliuojama filmuota medžiaga. Pasiūlyme (Europos Komisija 2020) numatoma, kad sistemos, kurios yra sukurtos arba manipuliuoja garso ir vaizdo turiniu, kuris yra labai panaši kopija į egzistuojančius asmenis, objektus, vietas ar kitus subjektus, ar įvykius ir kuris asmeniui klaidingai atrodytų autentiškas arba teisingas, „deep fake“ naudotojai turi atskleisti, kad turinys buvo dirbtinai sukurtas arba manipuliuojamas.

Tačiau pasiūlymo 52 straipsnio 3 dalyje taip pat nustatyta, kad ši ženklinimo prievolė netaikoma, kai naudojimas yra leidžiamas pagal įstatymą, siekiant nustatyti, užkirsti kelią, tirti nusikalstamas veikas, arba kai tai būtina siekiant pasinaudoti teise į saviraiškos laisvę, teise į meno ir mokslo laisvę. Nors įpareigojimas ženklinti padirbtus produktus galėtų būti pirmasis žingsnis siekiant sumažinti galimą neigiamą poveikį, šios priemonės pobūdis ir taikymo sritis lieka neaiški. Pasiūlyme nėra nenumatytos jokios priemonės prieš tuos naudotojus, kurie neatitinka 52 straipsnio 3 dalyje nustatytų skaidrumo reikalavimų.

Pasiūlyme tarp bausmių nenurodoma, ar yra baudžiama už 52 straipsnio 3 dalies reikalavimų nevykdymą ir jeigu baudžiama, tai kokia apimtimi.

2022 m. sausio 20 d. Europos Parlamentas ratifikavo Skaitmeninių paslaugų įstatymo pataisas (Europos Parlamento pataisos 2022 (P9_TA(2022)0014)), kurios turėtų įsigalioti 2023 m. Šios pataisos tiesiogiai susijusios su „deepfake“ platinimu internete. Atkreiptinas dėmesys į pataisose priimtą naują 30a straipsnį, kuriame nurodyta: „Kai labai didelė interneto platforma sužino, kad dalis turinio yra sukurtas arba manipuliuojamas vaizdo, garso ar vaizdo įrašo turinys, kuris pastebimai panašus į egzistuojančius asmenis, objektus, vietas ar kitus subjektus ar įvykius ir sudaro klaidingą įspūdį, kad asmuo yra autentiškas arba tikras (sintetinė vaizdo sankaita), paslaugos teikėjas pažymi turinį taip, kad būtų informuojama, jog turinys yra neautentiškas, ir kad būtų aiškiai matoma paslaugų gavėjui.“

Taip pat šiuo atveju svarbus ir 63 straipsnis, kuris daugiausia susijęs reklamos platformų skaidrumo didinimu. Tekstas skamba taip: „Be to, labai didelės interneto platformos turėtų ženklinti visą žinomą sintetinę vaizdakaitą, garso įrašus ar kitus failus;“. Panašu, Europos Sąjunga priimta tokį teisinį reglamentavimą ruošiasi augančiai„deepfake“ praktikai, taip stengdamasi apsaugoti savo demokratinę santvarką.

Tuo tarpu, JAV Nacionalinės gynybos leidimo įstatyme (United States National Defense Authorization Act 2021 (H.R.4350)) yra įtrauktos nuostatos, sprendžiančios didėjančią „deepfake“ atvejų problemą. Minėtas JAV Nacionalinės gynybos leidimo įstatymas tapo įstatymu, kuris reikalauja Valstybės saugumo departamento ateinančius penkerius metus pateikti metines ataskaitas dėl „deepfake“ situacijos. Įstatyme nurodyta, jog ataskaita turėtų apimti visą galimą technologijų žalą, įskaitant užsienio kampanijų įtaką, sukčiavimą ir žalą konkrečioms gyventojų grupėms.

Tai iš esmės išplėtė „deepfake“ ataskaitos apimtį. Be to, nurodytas įstatymas įpareigoja JAV vidaus saugumo departamentą ištirti „deepfake“ kūrimo technologiją ir galimus aptikimo bei mažinimo sprendimus. Galiausiai, įstatyme reikalaujama, kad JAV gynybos departamentas išnagrinėtų galimybę priešiškiems subjektams sukurti netikrą turinį, kuriame būtų vaizduojamas JAV karinis personalas.

2020 m. JAV buvo priimtas kitas įstatymas – Konkurencinių tinklų rezultatų nustatymo aktas (Identifying Outputs of Generative Adversarial Networks Act 2020 (H.R. 4355 (116th)). Pagal šį įstatymą Nacionalinis mokslo fondas turi tirti „deepfake“ autentiškumo priemones, o Nacionalinis standartų ir technologijų institutas remtis standartais, susijusių su „deepfake“. Šis įstatymas nurodo abiems agentūroms sukurti būdus, kaip dirbti su privačiu sektoriumi, „deepfake“ identifikavimo galimybių srityje.

Pažymėtina, jog Ilinojaus universiteto teisės apžvalgos straipsnyje (Prajakta Pradhan 2020) nurodoma, kad kelios valstijos taip pat priėmė apsaugą ir draudimus, susijusius su „deepfake“. Teksasas buvo pirmasis, uždraudęs „deepfake“, siekdamas apsisaugoti nuo neigiamos įtakos 2019 m. rinkimams. Tuo tarpu Kalifornijos įstatymai draudžia kurti vaizdo ir garso įrašus ar vaizdus, kuriuose per 60 dienų nuo rinkimų buvo pavaizduoti politikai, primenantys tikrą filmuotą medžiagą. Nurodytame straipsnyje teigiama, jog draudimai prieš „deepfake“ gali susidurti su JAV pirmosios pataisos iššūkiais. Tad net jeigu dabartiniai JAV įstatymai atlaikytų Pirmosios pataisos iššūkį, jurisdikcijos nebuvimas „deepfake“ kūrėjams sumažintų jų veiksmingumą. Todėl draudimai dėl „deepfake“ gali būti taikomi tik esant kelioms konkrečioms aplinkybėms, įskaitant žalą demokratijai.

Nors galėtų atrodyti, kad „deepfake“ žala demokratiniam valstybių valdymui neturėtų būti didelė, tačiau tenka prisiminti šio technologinio įrankio žalą Ukrainos karo įvykių kontekste. Kuomet informacinėje erdvėje pasirodė Ukrainos prezidento Volodymyro Zelenskio “deepfake” įrašas, kuris pasklido akimirksniu. Vaizdo įraše buvo pasirinkta kapituliacijos žinutė siekiant sumenkinti ukrainiečių visuomenės norą priešintis agresoriui. „Deefake“ kūrėjai tikėjosi, jog taip pavyks apgauti ukrainiečių karius bei įnešti chaosą Ukrainos demokratiniams procesams (Independent 2022). Pažymėtina, kad greitai pasklidęs “deepfake” buvo efektyviai demaskuotas – jį pašalino socialiniai tinklai, faktų tikrintojai skubiai paneigė tariamus Ukrainos prezidento žodžius. Nepaisant to, įrašas toliau sėkmingai sklido rusiškoje informacinėje erdvėje. Nors nurodytas vaizdo įrašas buvo sukurtas gan mėgėjiškai, negalima atmesti daugelio ekspertų nuogąstavimų, jog ateityje galima tikėtis itin kokybiškų „deepfake“ atvejų, kuomet politikai ar kiti asmenys turintys įtaką demokratiniams valstybių procesams taptų naujos formos dezinformacijos aukomis.

Apibendrinant galima daryti išvadą, kad „deepfake“ technologija greitai vystosi ir tobulėja. Šis interneto technologinis įrankis gali sukelti didžiulę grėsmę demokratinių valstybių santvarkoms. Todėl pastaraisiais metais “deepfake” yra laikomi savotišku rytojaus dezinformacijos simboliu, o įvairūs ekspertai pranašauja niūrią informacinės erdvės ateitį. „Deepfake” nėra tik smagūs dainuojančių garsenybių įrašai ir „prastumti laiką“ padedančios veidų keitimo aplikacijos. Tai yra realią dezinformacijos grėsmę keliantys įrankiai ateityje galintys kelti didelį pavojų demokratiniams procesams. Ši technologija griauna senas kategorijas – kas yra tikra, o kas yra dirbtina? Kadangi „deepfake“ tampa vis svarbesnis, ateinančiais dešimtmečiais priprasime prie tokių patirčių, tačiau tam, kad demokratija būtų saugi, reikia platesnio ir detalesnio teisinio reglamentavimo tiek JAV, tiek Europos Sąjungoje.

IV. Interneto technologijų galimybės demokratiniam valstybės valdymui

Demokratiją apibrėžti nėra lengva. Taip yra todėl, kad demokratija - daugelio skirtingų elementų rinkinys – elementų, kuriuos suprantame kaip demokratiją derinys arba visuma. Šiame kontekste nenuostabu, jog egzistuoja daugybe skaitmeninės demokratijos apibrėžimų. Vieniems tai reiškia skaitmeninių priemonių naudojimą informacijai teikti ir reklamuoti. Kiti skaitmeninę demokratiją apibūdina kaip technologinį informacijos ir komunikacijos būdą, kuris gali išplėsti, ir pagilinti dalyvavimą demokratiniuose procesuose, o kiti kalba apie skatinimą, įgalinimą suteikiantį piliečiams galimybę tiesiogiai priimti sprendimus naudojant internetines priemones.

Nors literatūroje nėra sutartų skaitmeninės demokratijos apibrėžimų, tačiau šiame darbe skaitmeninę demokratiją apibrėžiame kaip demokratijos praktiką naudojant skaitmenines priemones ir technologijas.

Pabrėžtina, kad galime išskirti „minimalistinius“ ir „maksimalistinius“ skaitmeninės demokratijos apibrėžimus. Pirmuoju minimalistiniu skaitmeninės demokratijos apibrėžimu daugiausia dėmesio yra skiriama piliečių prieigos prie vyriausybės informacijos suteikimui ir sąlygų bendrauti su vyriausybe sudarymui – pavyzdžiui, internetinės konsultacijos. Pastarasis skaitmeninės demokratijos būdas suteikia daugiau dalyvavimo demokratiniuose procesuose, taip leidžiant piliečiams bendrauti su valdžios organų pareigūnais ir siūlyti savo sprendimus dėl to, kaip jie bei jų vietos bendruomenės turėtų būti valdomi (Cammaerts and Carpentier 2007).

Demokratinės naujovės šiuo metu yra įtraukusios daugybę piliečių į demokratinius procesus ir suteikusios jiems įvairias galimybes – teikti peticijas (We The People JAV), teikti pasiūlymus (Your Priorities in Reykjavik), bendradarbiauti su valdžios atstovais (Estonian Citizens’ Assembly) arba atlikti užduotis, iki šiol priklausiusias valstybės tarnautojams (Peer to Patent). Šie pavyzdžiai įrodo, jog demokratiniuose procesuose remiantis interneto technologijų pagalba galima įtraukti piliečius ir taip sukurti kolaboracinę (bendradarbiavimo) demokratiją (Noveck 2009).

Nors šiandien skaitmeninės platformos apibūdinamos kaip „XX pirmojo amžiaus pradžios organizacinė forma“, kuriomis yra monopolizuojamas duomenų rinkimas (Stark and Pais 2021), internetinės platformos būdamos tarpininkės tarp demokratinės valdžios ir demokratinės valstybės piliečių, tapo privačiomis valstybių valdytojomis (Helberger 2020), turinčiomis didelį poveikį demokratijos procesams, įskaitant ir piliečių nuomonės formavimą susijusi su demokratinėms valstybėms svarbiais klausimais. Ankstyvos viltys,

kad internetas automatiškai sukurs demokratiją subliuško. Nepaisant to, galima įžvelgti ir teigiamų interneto technologijų aspektų demokratinių valstybių atžvilgiu.

Pastebėtina, kad tiek privatus, tiek viešasis piliečių bendravimas internete turi netiesioginį poveikį politiniams sprendimams. Diskusijose, kurios vyksta internete, dažnai dalyvauja savarankiškos bendruomenės, kaip pavydžiui„Reddit“, kuri nepatenkaį socialinės žiniasklaidos didžiųjų bendrovių įtakos sferą. Bendra tokių forumų savybė yra ta, kad jie nėra oficialiai reglamentuojami. Tad kuomet tokie politiniai pokalbiai išauga, jie gali tapti socialiniais judėjimais.

Internetiniai socialiniai tinklai gali būti įgalinančiomis platformomis padedančiomis asmenims ir mažumoms pasiekti auditorijas, didinti sąmoningumą ir sukurti didžiulius judėjimus. Kaip pavyzdžiui: „Metoo“ ar „BlackLivesMatter“. Minėtojo judėjimo „Metoo“ grotažymė #metoo, žyminti seksualinio priekabiavimo patirtis, per 2017 m. metus „Twitter“ platformoje buvo panaudota 19 milijonų kartų (Pew Research Center 2018) Pabrėžtina, kad judėjimai yra prisitaikantys prie interneto platformų vartotojų. Tai rodo aukštas įsitraukimas, kuris įmanomas tik per internetinę socialinę žiniasklaidą.

Konstatuotina, jog socialinė žiniasklaida ne tik leidžia koordinuoti socialinius judėjimus, ji taip pat gali nukreipti vartotojus į oficialias svetaines, skirtas politiniam dalyvavimui. Tyrimas rodo, jog apie 50 proc. Jungtinės Karalystės vyriausybės peticijų svetainės lankytojų atkeliavo per Facebook (40 proc.) ir Twitter (10 proc.) platformas. (S. A. Hale et al. 2018). Tai rodo, jog socialinės žiniasklaidos platformos padeda platinti reikšmingą informaciją, kuria demokratinės valstybės piliečiai gali išreikšti savo politinę nuomonę. Pažymėtina, kad socialinės žiniasklaidos platformų suteikiama lengva prieiga yra labai svarbus veiksnys, lemiantis aktyvesnį dalyvavimą demokratiniuose procesuose.

Tuo tarpu kitame spektro gale galime įžvelgti tiesioginį visuomenės dalyvavimą, kuris yra oficialiai pripažįstamas, valdomas ir reglamentuojamas, pavyzdžiui: referendumai, svarstomieji susirinkimai ir t.t. Pasinaudojant interneto technologijomis galima surasti ir kitų piliečių dalyvavimo formų, formuojančių politiką. Pavyzdžiui, peticijos pasirašymą internetu ar prisijungimą prie bendrų grupinių ieškinių, ginant savo pilietines teises.

Galima sutikti, jog yra pavyzdžių, kuomet skaitmeninė demokratija gerai veikia ir pačiose Europos Sąjungos valstybėse. Interneto technologijų priemonės vis dažniau naudojamos siekiant atgaivinti ir pagerinti piliečių dalyvavimą priimant demokratinius sprendimus. Mažėjant rinkėjų aktyvumui ir mažėjant partijos narių skaičiams (Pascal Delwit 2011) piliečiai pereina prie internetinio politinio įsitraukimo. Daugelis Europos piliečių nors ir nėra apotiški politikai, tačiau naudojasi naujais būdais, kurie padėtų

išgirsti jų nuomonę svarbiais klausimais. Tai svarbu, kadangi skaitmeninis dalyvavimas demokratiniuose procesuose yra paprastas, prieinamas ir gali pasiekti plačią auditoriją.

Europos Sąjungoje dažnai vadinama e–demokratija suteikia daugybę labai skirtingų internetinio įsitraukimo galimybių, įskaitant e–iniciatyvas, e–konsultacijas, dalyvavimą biudžeto sudaryme ir elektroninį balsavimą. Daugelis Europos šalių pradėjo taikyti šias priemones, tam, kad pasiektų daugiau piliečių ir pasinaudotų taip vadinamąja minios išmintimi. Šių interneto technologijų dėka Europos demokratija yra plėtojama su tikslu ją padaryti skaidresnę ir labiau įtraukiančią Europos Sąjungos piliečius dalyvauti sprendimų priėmimo procesuose.

Pavyzdžiui, 2014 m. Paryžiaus miesto vienas iš prioritetų buvo padidinti miesto bendradarbiavimą, leidžiantį paryžiečiams kartu teikti naujus pasiūlymus miestui irprisidėti prie kuriamų projektų. Paryžiaus miesto valdžia siekdama užmegzti tvirtesnius santykius su miestiečiais, nedelsdama pradėjo įgyvendinti viso Paryžiaus dalyvaujamojo biudžeto sudarymo projektą, apimantį visus politikos klausimus.

Paryžiaus miestas pasiūlė penkiolika projektų, kurie galėtų būti finansuojami iki 20 milijonų eurų. Ši iniciatyva leido miestiečiams balsadėžėje arba internetu balsuoti ir nuspręsti į kuriuos projektus Paryžiaus miesto valdžia turėtų investuoti. Paryžiečiai ir vietos valdžia šį eksperimentą laikė sėkmingu. Todėl buvo nuspręsta šį projektą tęsti skiriant tam dar daugiau lėšų. Pažymėtina, jog per dvejus metus miestiečių dalyvavimo lygis demokratiniuose procesuose labai išaugo – nuo maždaug 40 000 rinkėjų 2014 m. iki 92 809 2017 m. rinkėjų (Paris Budget Participatif 2017).

„ Paris Budget Participatif “ yra oficiali platforma, leidžianti paryžiečiams nuspręsti, kaip išleisti 5 proc. Paryžiaus miesto biudžeto, kuris sudaro apie 500 milijonų eurų. Be to, Paryžiaus miesto valdžia yra pristačiusi dar dvi e-demokratijos platformas – „ Paris Petitions “ elektroninėms peticijoms ir „Idée Paris “ elektroninėms konsultacijoms. Tad dabar Prancūzijos sostinės gyventojai turi daugybę technologinių įrankių, kuriuose gali išreikšti savo nuomonę ir taip prisidėti prie savo miesto plėtros.

Tuo tarpu Suomijoje pati vyriausybė į Suomijos politinę sistemą įtraukė tiesioginės demokratijos elementą. Suomijos valdžia priimdama 2012 m. Piliečių iniciatyvos aktą (Citizens Initiative Act 2012 (12/2012)) leido piliečiams teikti iniciatyvas parlamentui internetiniu būdu. Reikalavimai, kurie buvo nustatyti yra labai paprasti: bet kuris pilietis, kuris turi balsavimo teisę, gali pasiūlyti įstatymo projekto iniciatyvą, kuri pakeičia esamus teisės aktus arba sudaro visiškai naują įstatymo projektą. Iniciatyvos turi surinkti 50 000 parašų per šešis mėnesius popieriuje arba internetu. Tuomet Suomijos parlamentas tokį

projektą svarstys. Parlamentarai privalo svarstyti parašus surinkusias iniciatyvas, jas priimdami arba atmesdami.

Netrukus po Piliečių iniciatyvos akto (Citizens Initiative Act 2012 (12/2012)) priėmimo, buvo sukurta internetinė platforma Avoinministerio.fi, kurioje galima diskutuoti, reklamuoti ir balsuoti už piliečių iniciatyvas. Tam, jog būtų lengviau surinkti 50 000 parašų, Suomijos teisingumo ministerija atidarė oficialią internetinę sistemą (www.kansalaisaloite.fi), skirtą pareiškimams teikti.

Konstatuotina, kad ir kitos pilietinių technologijų nevyriausybinės organizacijos visoje Europoje kuria ir eksperimentuoja su įvairiomis skaitmeninėmis priemonėmis, siekdamos atgaivinti Europos Sąjungos demokratiją. Tai apima tokias iniciatyvas kaip „Science For You“ (SCiFY) Graikijoje, „ Netwerk Democratie “ Nyderlanduose ir „ Citizens Foundation “ Islandijoje.

Nors šios iniciatyvos daro teigiamą poveikį Europos demokratijos kokybei, didžioji dalis oficialios Europos Sąjungos politikos dėmesį skiria technologijų milžinų galios suvaržymui, o ne teigiamam skaitmeninio dalyvavimo skatinimui.

Per pastaruosius metus tik iš trijų Europos Sąjungos programų buvo finansuoti darbai, tiesiogiai susiję su skaitmenine demokratija: 700 000 eurų paketas pagal Teisių, lygybės ir pilietybės programą (Rights, Equality and Citizenship Programme 2014–2020), 1,6 milijonų eurų pagal Erasmus+ ateities bendradarbiavimo projektus (Erasmus+ 2015) bei 5 milijonų eurų akademiniams tyrimams pagal programą „ Horizontas 2020“ (Horizon 2020). Šios investicijos daugiau nei 1 trilijono eurų bendro Europos Sąjungos biudžete yra tik lašas jūroje.

Tačiau žvelgdama į ateitį, Europos Komisija pasiūlė 9,2 milijardo eurų vertės Skaitmeninės Europos programą (European Commission. EU budget 2018), kurioje 2021–2027 m. numatyti penki prioritetai: superkompiuteriai, dirbtinis intelektas, kibernetinis saugumas, skaitmeniniai įgūdžiai ir platesnis skaitmeninių technologijų naudojimas, daugiausia viešajam administravimui ir paslaugoms. Tačiau pasiūlyme akivaizdžiai nėra įtraukta skaitmeninė demokratija.

Skeptikai šį sprendimą kritikuoja ir nerimauja, kadangi apie skaitmeninę demokratiją Europoje plačiai kalba populistiniai judėjimai. Kritikai teigia, jog tokį sprendimą lėmė stiprus Europos Sąjungos institucijų nepasitikėjimas tiesioginės demokratijos procesais. Pavyzdžiui, referendumais, kurie per pastarąjį dešimtmetį sukėlė sukrėtimų visai Europos demokratinei sistemai.

Europos Sąjungos kontekste galima įžvelgti požiūrį, jog skaitmeninės grėsmės gali užgožti galimybes. Nors atrodytų, kad skaitmeninės technologijos galėtų sumažinti žmonių

nusivylimą tradicine politika, tačiau vadindama šiuolaikinė dezinformacija ir interneto technologijų mažinama asmeninė laisvė kelia grėsmę demokratiniams procesams. Todėl šiuo metu Europos Sąjungos institucijos skiria daug dėmesio neigiamiems skaitmeninių priemonių aspektams suvaldyti.

Politikos formuotojų susirūpinimas yra iš dalies pagrįstas ir jie teisūs kritiškai žvelgdami į skaitmeninės demokratijos praktiką. Skaitmeniniai įrankiai nėra be trūkumų. Pabrėžtina, jog skaitmeninis dalyvavimas gali išties pakenkti demokratiniams procesams, jeigu interneto technologijų priemonės yra prastai įdiegiamos. Tuomet piliečių lūkesčiai nėra tinkamai įgyvendinami.

Tinkamas interneto technologijų galimybių įgyvendinimas yra labai svarbus – priešingu atveju skaitmeninės priemonės gali pakenkti demokratinei santvarkai. Tačiau minėti pavyzdžiai – Prancūzijoje ir Suomijoje – rodo, kad e– dalyvavimo platformos yra naudojamos papildyti, o ne pakeisti esamus demokratinius įrankius. Tad jeigu sprendimus priimantys demokratinių valstybių valdžios organai atsižvelgia į skaitmeninio balsavimo rezultatus, tuomet skaitmeninės priemonės gali būti labai sėkmingos, stiprinant piliečių dalyvavimą demokratiniuose procesuose.

Galiausiai reikia suprasti, kad realybė yra tokia, jog skaitmeninė demokratija jau egzistuoja, nesvarbu, ar vyriausybės yra pasirengusios ją įdiegti, ar ne. Esminiai klausimai yra tokie – ar panaudojus interneto technologijas galima atgaivinti „sergančias“ Europos demokratines institucijas bei demokratinius procesus ir ar šiuo metu toks e–demokratijos įdiegimas visoje Europos Sąjungoje nesugriautų pačios Europos demokratijos? Tai yra klausimai į kuriuos turi atsakyti tiek Europos Sąjungos institucijos, tiek Europos Sąjungos piliečiai.

Taigi interneto technologijos nėra pačios demokratijos problema. Internetinės platformos gali ir turėtų būti panaudotos demokratijai skatinti ir mūsų demokratinių procesų kokybei gerinti. Nors galima įžvelgti daugybę galimų piktnaudžiavimų rinkimų procesais, tačiau pastebime ir teigiamų interneto technologijų savybių demokratiniams procesams: informacijos sklaida, efektyvesnis tiesioginis ir netiesioginis piliečių atstovavimas, sklandesnis valdžios organų įsiklausymas į piliečių nuomonę. Tad šiuo metu vertinant Europos Sąjungos bei valstybių narių viešųjų institucijų praktiką darome išvadą, jog interneto technologijos vis dėlto gali suteikti demokratiniams procesams teigiamų pokyčių. Tačiau tokius pokyčius reikia vertinti labai atsargiai.

V. Lietuvos demokratinė teisinė sistema

Lietuvos Respublika būdama Europos Sąjungos nare bei pasaulinės rinkos dalyve interneto technologijų atžvilgiu yra glaudžiai susijusi su interneto technologijų įmonėmis ir vyraujančiomis tarptautinėmis grėsmėmis bei galimybėmis. Interneto technologijų grėsmių ir galimybių Lietuvos demokratiniams procesams tyrime svarbu atsižvelgti į Lietuvoje galiojantį teisinį reglamentavimą bei viešųjų institucijų pozicijas.

Nors atrodytų, kad per pastaruosius dešimtmečius Lietuvos institucijos, kurias ankstesnės kartos laikė būtinomis formuojant demokratišką valstybę vis dar veikia, ačiau šiuo atveju kyla esminiai klausimai – ar Lietuvoje yra pakankamas teisinis reglamentavimas interneto technologijų grėsmėms suvaldyti? Kokios yra galimos interneto technologijų galimybės Lietuvos teisinėje sistemoje?

Konstitucinio teismo jurisprudencijoje (Lietuvos Respublikos Konstitucinio Teismo 2000 m. vasario 23 d. nutarimas. Valstybės žinios, Nr. 17-419) nurodoma, kad Konstitucijos 1 straipsnyje ne tik įtvirtinti pamatiniai Lietuvos valstybės principai (Lietuvos valstybė yra savarankiška, nepriklausoma valstybė; Lietuvos valstybės valdymo forma yra respublika), bet ir (interpretuojant terminą „demokratinė“) tai, jog „valstybės valdžia turi būti organizuota demokratiškai, šalyje turi būti demokratinis politinis režimas.

Konstatuotina, jog Lietuvoje egzistuojant demokratinei santvarkai, turime suprasti, kad šią santvarką reikia nuolat prižiūrėti ir puoselėti, taip ją stiprinant ir išsaugant taisyklėmis pagrįstą tvarką. Siekiant, kad Lietuvos teisinė sistema atlaikytų interneto technologijų keliamas grėsmes turime tobulinti egzistuojantį teisinį reglamentavimą.

Tačiau neramina tai, jog daugelis Lietuvos gyventojų, t. y. net 71 proc., toleruotų ir ne taip gerai veikiančią demokratiją, jei šalyje būtų užtikrinta stipri ekonomika (Pew Research Center 2011). Minėtas tyrimas taip pat rodo, jog per dvidešimtmetį nuo nepriklausomybės atkūrimo Lietuvoje gerokai sumažėjo remiančių daugiapartinę sistemą, rinkos ekonomiką ir apskritai demokratiją. O teikiančių pirmenybę demokratijai, o ne stipriam lyderiui respondentų yra beveik tik puse.

Būtina pastebėti, kad svarbiausia užduotis Lietuvos institucijoms – užtikrinti tinkamą demokratinės sistemos būseną. Kadangi demokratija savaime negimsta – dažnai ją reikia sukurti, o Lietuvos teisinė sistema nėra išimtis.

5.1. Interneto technologijų grėsmės Lietuvos teisinei sistemai

Šiuo metu Lietuvoje galiojantis rinkimų kampanijų organizavimo, finansavimo, priežiūros ir atsakomybės už rinkimų proceso pažeidimus reglamentavimas yra vienas griežčiausių Europos Sąjungoje. Lietuvos Respublikos politinių kampanijų finansavimo ir finansavimo kontrolės įstatyme (Lietuvos Respublikos politinių kampanijų finansavimo ir finansavimo kontrolės įstatymas 2004 (Žin Nr. IX–2428)) yra nustatyti gana griežti politinės reklamos reikalavimai. Minėtame įstatyme nurodyta, kad politinė reklama turi būti pažymėta nurodant lėšų šaltinį, taip aiškiai atskiriant politinę reklamą nuo kitos skleidžiamos informacijos. Taip pat politinė reklama, nepažymėta pagal teisės aktų reikalavimus arba pažymėta nesilaikant teisės aktų reikalavimų, laikoma paslėpta politine reklama ir yra draudžiama. Už jos skleidimą taikoma įstatymų nustatyta atsakomybė.

Tačiau vertinant dabartinį teisinį reglamentavimą politinės reklamos atžvilgiu interneto technologijų socialiniuose tinkluose, matome, kad atskirai nėra išskiriamas teisinis reglamentavimas socialinių tinklų atžvilgiu. Atrodytų, jog politinės reklamos socialiniuose tinkluose šiuo metu sureguliuoti neįmanoma, nes socialinis tinklas „Facebook“ vis dar nedeklaruoja savo reklamos įkainių, kurie turėtų būti vienodi visiems politinės reklamos užsakovams.

Pabrėžtina, jog viešoje erdvėje dar 2020 m. rugsėjo mėn. pasirodė Interneto žiniasklaidos asociacijos raginimas (15min. 2020) Lietuvos Respublikos vyriausiąją rinkimų komisiją imtis priemonių dėl politinės reklamos socialiniuose tinkluose. Interneto žiniasklaidos asociacija nurodė, kad pirma, reikia įpareigoti politines partijas ir fizinius rinkimų kampanijos dalyvius deklaruoti vieną socialinių tinklų paskyrą, kurioje būtų skelbiama informacija bei kurios matomumas galėtų būti didinamas komerciniu reklamos pirkimu. O antra, remiantis finansinio skaidrumo principu, turi būti nustatytas teisinis reglamentavimas, kuomet politinės partijos ir fiziniai rinkimų kampanijos dalyviai turėtų būti įpareigoti visus mokėjimus, susijusius su socialiniais tinklais (ypač rinkiminiu laikotarpiu) vykdyti tik iš vienos, Lietuvos Respublikos vyriausiajai rinkimų komisijai deklaruotos banko sąskaitos.

Gali būti manoma, jog Interneto žiniasklaidos asociacijos pasiūlymas padėtų užtikrinti rinkimuose dalyvaujančių kandidatų ir partijų finansinį skaidrumą, ir atskaitomybę visuomenei, taip apsaugant Lietuvos demokratiją, tačiau praktikoje toks reguliavimas vis dar nėra įgyvendinamas.

Tarptautinių socialinių tinklų kontrolė remiantis Lietuvos teisiniu reglamentavimu yra stebėtinai sunkiai įgyvendina, kadangi Lietuvos Respublikos vyriausioji rinkimų komisija

neturi kompetencijos įpareigoti didžiąsias interneto technologijų įmones keisti taisykles politinės reklamos atžvilgiu. Tačiau galima teigti, jog tokie Interneto žiniasklaidos asociacijos raginimai yra teigiami atsižvelgiant į politinės kampanijos dalyvių atskaitingumo klausimus.

Nors šiuo metu į tokį Interneto žiniasklaidos asociacijos raginimą Lietuvos Respublikos Vyriausioji rinkimų komisiją teisiniais veiksmais nesureagavo. Tačiau reikia atkreipti dėmėsį, kad apskritai siekdama reglamentuoti bendrus reikalavimus interneto technologijų bendrovėms, Lietuva būdama Europos Sąjungos nare turėtų spręsti šį klausimą Europos Sąjungos lygiu kartu su kitomis Europos Sąjungos valstybėmis. Bendros politinės reklamos socialiniuose tinkluose klausimas yra tarptautinio pobūdžio, kurį galėtų iškelti Lietuvos atstovai Europos Sąjungos institucijose.

Taigi augant socialinių tinklų svarbai ir naudojimo mastui, siūlytina apsvarstyti teisės aktų, susijusių su politine reklama, tobulinimą, daugiau dėmesio skiriant reklamos socialiniuose tinkluose sklaidos ir finansavimo skaidrumui. Pavyzdžiui, įpareigojant politines partijas pateikti išsamesnes finansines ataskaitas, kuriose būtų išskirtos lėšos reklamai socialiniuose tinkluose, sąskaitos bei sutartys sudarytos su socialiniais tinklais, ir už kurias būtų atsiskaitoma iš vienos Lietuvos Respublikos vyriausiajai rinkimų komisijai deklaruotos banko sąskaitos.

Dabartiniame Politinių partijų ir politinių kampanijų finansavimo ir finansavimo kontrolės įstatyme (Lietuvos Respublikos politinių kampanijų finansavimo ir finansavimo kontrolės įstatymas 2004 (Žin Nr. IX–2428)) nėra atskirai apibrėžiama politinė reklama internete ar socialiniuose tinkluose. Taip pat nėra įtrauktas trečiųjų asmenų vaidmuo politinėje kampanijoje. Įstatymas palieka landų, kurios neleidžia užtikrinti pakankamų politinės reklamos sklaidos ir finansavimo skaidrumo. Tai yra teisinio reglamentavimo spraga, kadangi būtent pasinaudojant šiomis įstatymo landomis būtų galima pakenkti Lietuvos teisinei santvarkai.

Tuo tarpu tiriant Lietuvos teisinę situaciją dezinformacijos ir kibernetinio saugumo atžvilgiu turime įvertinti, kad prieš 2019 m. Lietuvoje vykusius savivaldybių tarybų ir merų, Respublikos Prezidento ir Europos Parlamento rinkimus buvo sustiprintos Lietuvos institucijų pastangos pasirengti galimam poveikiui iš kitų šalių. Tai paskatino užsienio šalyse užfiksuoti precedentai (2016 m. JAV prezidento rinkimai, 2017 m. Prancūzijos prezidento rinkimai) bei suintensyvėjusi Rusijos dezinformacijos veikla, kuri išaugino konfrontaciją tarp Rusijos ir Vakarų šalių.

Ypač didelis dėmesys buvo skiriamas kibernetiniam saugumui. Nors kibernetinių incidentų per visus trejus Lietuvoje vykusius 2019 m. rinkimus nebuvo daug. Buvo stebima

tipinė potencialiai kenkėjiška veikla (pvz., Lietuvos Respublikos vyriausiosios rinkimų komisijos serverių perimetro skenavimas, ieškant pažeidžiamų vietų), tačiau esminių incidentų ar ypatingai didelio kibernetinių išpuolių suaktyvėjimo nepastebėta. Svarbu paminėti, jog Lietuvos Respublikos Seimo ir Respublikos Prezidento rinkimų metu buvo blokuota daugiau negu 900 IP adresų (Nacionalinio kibernetinio saugumo centras 2019). Taip pat Lietuvos Respublikos vyriausioji rinkimų komisija užfiksavo keletą atvejų, susijusių su galimos kenkėjiškos programinės įrangos naudojimu asmeniniuose kompiuteriuose.

Žvalgybos priemonėmis buvo vykdomas ir politinio kišimosi į rinkimus stebėjimas. Lietuvos Respublikos valstybės saugumo departamento ir Antrojo operatyvinių tarnybų departamento parengtoje grėsmių vertinimo ataskaitoje (Lietuvos Respublikos Valstybės saugumo departamentas, Antrasis operatyvinių tarnybų departamentas prie Krašto apsaugos ministerijos 2020) nurodoma, kad 2019 m. savivaldybių tarybų rinkimuose Rusija siekė, jog jai lojalūs politikai išlaikytų savo pozicijas savivaldybėse. Tokia veikla nėra nauja – tautinių mažumų rinkėjų segmentai vis dar yra santykinai jautriausia visuomenės grupė, kuriai bandoma daryti įtaką iš Rusijos. Tai susiję ir su Rusijos informacinės erdvės naudojimosi įpročiais, kai kuriais atvejais – su ribota integracija į Lietuvos visuomenę ir dėl to kylančiu nesaugumo jausmu. Tuo tarpu Lietuvos Respublikos Prezidento rinkimų metu nebuvo pastebėta aktyvių Rusijos ar kitų užsienio šalių kišimosi pastangų.

Kaip nurodoma žvalgybos tarnybų 2020 m. parengtame vertinime (Lietuvos Respublikos Valstybės saugumo departamentas, Antrasis operatyvinių tarnybų departamentas prie Krašto apsaugos ministerijos 2020) 2019 rinkimų kampanijų metu plataus masto bandymų paveikti rinkimų rezultatus nebuvo, sistemingų bandymų manipuliuoti visuomenės nuomone taip pat nenustatyta. Pastebima, kad rinkimų laikotarpiu Rusijos propagandistai labiau orientavosi į šmeižto kampanijas prieš Rusijos valdžios veiksmus aktyviausiai kritikuojančius Lietuvos politikus.

Galima matyti, jog 2020 m. rugsėjo mėn. buvo parengti Lietuvos Respublikos kibernetinio saugumo įstatymo (Lietuvos Respublikos kibernetinio saugumo įstatymas 2014 (Žin Nr. XII–1428)) ir Lietuvos Respublikos administracinių nusižengimų kodekso pakeitimo įstatymo (Lietuvos Respublikos administracinių nusižengimų kodekso 12, 79, 124, 136, 146, 477, 502 ir 548 straipsnių pakeitimo įstatymas 2021 (Žin Nr. XIV–182)) projektai, numatantys Lietuvos rinkos subjektams galimybę produktus, procesus ir paslaugas sertifikuoti pagal Europos kibernetinio saugumo sertifikavimo schemas bei įteisinanti RIS spragų atskleidimo modelį.

Tad galima teigti, jog Lietuvos Respublikoje teisinis reglamentavimas kibernetinio saugumo bei dezinformacijos atžvilgiu yra nuolat tobulinimas. Įstatymų leidėjas, tiek viešosios institucijos deda ryškias pastangas, siekdamos užkardyti dezinformacijos ir kibernetinių atakų žalą Lietuvos demokratinei sistemai.

Kita vertus tiriant asmenų duomenų aspektus Lietuvoje, turime pabrėžti, jog asmens duomenys Lietuvos demokratinių rinkimų metu Lietuvos Respublikos vyriausioji rinkimų komisija tvarko vadovaujantis BDAR (Europos Parlamento ir Tarybos reglamentas 2016 (2016/679)). Valstybinė duomenų apsaugos inspekcija 2019 m. vasario 27 d. yra išleidusi rekomendaciją apie asmens duomenų tvarkymą rinkimų metu, kuri yra skirta asmens duomenis tvarkančioms politinėms partijoms, kandidatams, visuomeniniams rinkimų komitetams, tačiau pabrėžtina, jog šiuo atveju atskiro ir plataus teisinio reguliavimo šiuo klausimu nėra.

Atskiro teisinio reguliavimo Lietuvos teisinėje sistemoje nėra ir dėl „deepfake“ keliamų grėsmių. Matoma, kad tiriant Lietuvoje galiojančių įstatymų teisinę bazę šio darbo tyrimo metu nebuvo rasta galiojančių norminių teisės aktų, kuriuose būtų paminėta ar sureguliuota „deepfake“ problematika Lietuvos teisinėje sistemoje. Taip pat šiuo momentu Lietuvoje nėra teismų sprendimų ar nutarčių, kuriuose būtų paminėtas ar išaiškintas šis interneto technologinis įrankis. Pažymėtina, kad „deepfake“ yra grėsmė Lietuvos demokratinei santvarkai, kuri negali būti ignoruojama.

Taigi Lietuvoje galiojantis teisinis reguliavimas interneto technologijų grėsmių Lietuvos demokratijai atžvilgių – nepakankamas, nes Lietuvos įstatymų leidėjas nėra tinkamai sureguliavęs ne tik politinės reklamos sklaidos ir finansavimo skaidrumo klausimų, bet ir vis dažnėjančių interneto technologijų grėsmių – „deepfake“. Ir nors Lietuvoje vyraujantis teisinis reglamentavimas susijęs su kibernetiniu saugumu ar duomenų apsauga yra tobulinamas, įstatymų leidėjas ir viešosios institucijos vis dar palieka spragų teisiniame reglamentavime, kuriomis pasinaudojant būtų galima pakenkti Lietuvos demokratinei santvarkai.

5.2. Interneto technologijų galimybės Lietuvos teisinei sistemai

Lietuvos Respublikos teisiniame reglamentavime susijusiame su interneto technologijų institutu turime įžvelgti ir šio instituto galimas galimybes Lietuvos teisinei santvarkai. Pabrėžtina, jog viešojoje erdvėje Lietuvos Respublikos vyriausioji rinkimų komisija 2021 m. priėmė sprendimą (LRT 2021) pradėti internetinio balsavimo informacinės sistemos galimybių studijos pirkimo procedūras. Tačiau tenka pastebėti, kad idėja įteisinti balsavimą internetu viešojoje erdvėje svarstoma jau daugiau nei penkiolika metų.

Lietuvos Seime anksčiau keliskart buvo teikti projektai dėl balsavimo internetu, bet jie nebuvo priimti. Internetinio balsavimo šalininkai dažnai nurodo, kad internetinis balsavimas Lietuvoje leistų padidinti rinkėjų aktyvumą, o kritikai nuogąstauja, kad balsavimo internetu sistema gali tapti lengvu kibernetinių atakų taikiniu, jomis gali būti siekiama pakeisti rinkimų rezultatus. Tad keliami klausimai dėl internetinio balsavimo – toli gražu ne naujiena Lietuvos teisiniame gyvenime.

Balsavimo internetu rinkimuose ir referendumuose koncepcija, kurioje buvo suformuluoti balsavimo internetu įvedimo tikslai, pagrindiniai balsavimo principai, aprašyta balsavimo internetu schema bei numatyta, kad turi būti pakeisti Savivaldybių tarybų rinkimų, Seimo rinkimų, Prezidento rinkimų, Rinkimų į Europos Parlamentą, Referendumo įstatymai, juose įteisinant balsavimą internetu kaip alternatyvų balsavimo būdą, buvo numatyta dar 2006 m. Lietuvos Respublikos Seimo nutarime (Lietuvos Respublikos Seimo nutarimas 2006 (Žin Nr. X–912)).

Svarbu paminėti, kad buvo parengti rinkimų įstatymų pakeitimai net kelis kartus – 2008 m. sausį, 2009 m. gruodį, 2010 m. birželį, 2014 m. gegužę buvo teikiami Lietuvos Respublikos Seimui, tačiau nesėkmingai. Lietuvos Respublikos Seimas įstatymų projektus grąžindavo iniciatoriams tobulinti.

Pirmą kartą parengtas Lietuvos Respublikos balsavimo internetu pagrindų įstatymo projektas po pateikimo Lietuvos Respublikos Seimui 2016 m. kovo 22 d. posėdžio metu buvo grąžintas iniciatoriams tobulinti. O 2018 m. kovo 6 d. užregistravus Balsavimo internetu pagrindų įstatymo projektą (Balsavimo internetu pagrindų įstatymo projektas 2018 (Žin XIIP–3879(2)) nebuvo priimtas.

2018 m. gegužės 25 d. Lietuvos Respublikos Seimo kanceliarijos Teisės departamentas pateikdamas išvadą (Teisės departamento išvadą 2018 (Žin Nr. XIIP–3879(2)) įvertino šio projekto atitiktį Konstitucijai, įstatymams, teisėkūros principams bei teisės technikos taisyklėms.

Išvadoje Lietuvos Respublikos Seimo kanceliarijos Teisės departamentas atkreipė dėmesį į tai, kad 2012 m. kovo 15 d. priimtu Konstitucinių įstatymų sąrašo konstituciniu įstatymu Seimas yra įsipareigojęs patvirtinti Rinkimų kodekso patvirtinimo, įsigaliojimo ir įgyvendinimo konstitucinį įstatymą ir Referendumo konstitucinį įstatymą (Konstitucinių įstatymų sąrašo konstitucinio įstatymo 2 straipsnio 1 dalies 5 ir 6 punktai). Taigi praktika, leidžianti nurodytų konstitucinių įstatymų sferai priskirtus klausimus reglamentuoti paprastu įstatymu, taip išvengiant Konstitucijoje numatytos ypatingos konstitucinių įstatymų priėmimo ir keitimo tvarkos, būtų ydinga.

Svarbu, kad Teisės departamentas nurodė ir tai, jog projekto nuostatos bei jų imperatyvumas yra diskutuotini. Balsavimas internetu nuotoliniu būdu vyksta nekontroliuojamoje rinkėjo pasirinktoje aplinkoje. Tai reiškia, kad rinkimų komisijų nariai ir kiti valstybės įgalioti asmenys negali įsitikinti balsavimo slaptumu bei rinkėjo laisva valia, tuo labiau negali to užtikrinti. Reikalavimai dėl balsavimo slaptumo ir rinkėjo laisvos valios balsavimo internetu metu negali būti užtikrinami, todėl balsavimas internetu niekada negalėtų atitikti minėtų imperatyvių projekto nuostatų.

Taip pat Lietuvos Respublikos Seimo kanceliarijos Teisės departamentas nurodo, kad projekte nėra nustatoma įstatymo įsigaliojimo data, todėl įstatymas, jeigu jis būtų priimtas, įsigaliotų Teisėkūros pagrindų įstatymo 20 straipsnio 1 dalyje (Lietuvos Respublikos teisėkūros pagrindų įstatymas 2012 (Žin Nr. XI–2220)) nustatyta tvarka – kitą dieną jį oficialiai paskelbus Teisės aktų registre. Nuo šios datos įstatymas turėtų būti taikomas. Tačiau diskutuotina, ar projektu teikiamo įstatymo, kuris sudarytų teisines prielaidas sukurti, įdiegti, palaikyti ir atnaujinti balsavimo internetu sistemą, priėmimas neturėtų vykti lygiagrečiai su rinkimų ir referendumo įstatymų pakeitimais.

Lietuvos teisinėje sistemoje pateikti įstatymų projektai yra kritiškai vertinami, tačiau šiuo metu vykstančios diskusijos dėl interneto balsavimo reglamentavimo vėl įgauna naujų gyvybės ženklų, bet svarbu atkreipti dėmesį, kad Lietuvos Respublikos vyriausioji rinkimų komisija priėmusi sprendimą pradėti internetinio balsavimo informacinės sistemos galimybių studijos pirkimo procedūras bei taip siekdama išsiaiškinti internetinio balsavimo įdiegimo Lietuvoje galimybes, suteikia daugiau peno diskusijoms dėl šio internetinio balsavimo instituto reglamentavimo.

Konstatuotina, kad rinkimų organizavimui informacinės technologijos Lietuvoje naudojamos jau gana seniai ir plačiai: Lietuvos Respublikos vyriausioji rinkimų komisija turi elektroninius rinkėjų sąrašus, rinkėjai gali internetu gauti ir atsispausdinti rinkėjo pažymėjimą, rinkimų apygardos turi interneto ryšį, rinkimų rezultatai pateikiami nuolat atnaujinamoje Lietuvos Respublikos vyriausios rinkimų komisijos interneto svetainėje.

Šiuo metu Lietuvoje naudojamas kol kas tik popierinis balsavimas. Nors Lietuvos Respublikos vyriausiosios rinkimų komisijos įstatymo 3 straipsnio 15 punkte (Lietuvos Respublikos vyriausiosios rinkimų komisijos įstatymas 2002 (Žin Nr. IX–985) nustatyta, kad ši institucija rūpinasi rinkimų technologijų tobulinimu galutinis sprendimas dėl internetinio balsavimo reglamentavimo Lietuvoje priklauso nuo įstatymų leidėjo – Lietuvos Respublikos Seimo.

Teigtina, jog Lietuvos teisinėje trūksta teisinio reglamentavimo, kuris apribotų interneto technologijų grėsmes demokratiniams procesams. Lietuvoje nėra pakankamai skiriamas dėmesys politinės reklamos socialiniuose tinkluose kontrolės reglamentavimui. Galima pastebėti, kad kibernetinėje, duomenų apsaugos bei kovos su dezinformacija sferoje Lietuvos teisinė sistema yra pažengusi, dabartinis teisinis reglamentavimas nėra pakankamas tam, jog galėtume kalbėti apie saugų internetinio balsavimo įdiegimą Lietuvos teisinėje sistemoje.

Apibendrinant galima teigti, kad vertinant Lietuvos teisinį reglamentavimą interneto technologijų galimybių atžvilgiu, pastebime, jog internetinio balsavimo įteisinimas Lietuvoje išgyvena sudėtingą laikotarpį. Galima sutikti, rinkimai yra viena svarbiausių moderniosios atstovaujamosios demokratijos procedūrų – jie sudaro galimybę piliečiams netiesiogiai per savo išrinktus atstovus dalyvauti valstybės valdyme. Tačiau klaidinga būtų teigti, kad kiekviena interneto technologija demokratinės valstybės atžvilgiu yra sveikintina, nes kiekvieną tokią idėją turime vertinti atsargiai, ypač stebint bendrą situaciją Europos Sąjungoje. Tad internetinio balsavimo galimybė Lietuvos demokratijai yra rizikinga. Šiandien tai yra vienas iš populiariausių siūlymų, neva padedantis spręsti mažėjančio dalyvavimo rinkimuose problemą, bet tai gali sukelti didžiulę žalą Lietuvos Respublikos demokratiniams procesams, o galbūt ir pačiai Lietuvos demokratinės santvarkos egzistencijai.

IŠVADOS

1. Specialiojoje literatūroje demokratinė valstybė apibrėžiama kaip valstybė, kuri turi ne tik konstituciškai įteisintą demokratiją kaip politinio valdymo formą, bet ir, kurios procedūrų realus įgyvendinimas atitinka demokratinių valstybių bruožus: demokratinių piliečių teisių ir laisvių pripažinimas, politinis pliuralizmas, valdžių padalijimo principo realus įgyvendinimas, parlamento funkcionavimas bei politinės ideologijos laisvumas. Interneto technologijos specialiojoje literatūroje yra suprantamos kaip interneto įrankis, leidžiantis asmenims dalintis internetu tam tikra informacija ir bendrauti iš bet kurios pasaulio vietos, kurioje yra interneto ryšys.
2. Pozityvus požiūris į interneto technologijas, kuris ypač vyravo pirmaisiais plėtros dešimtmečiais keičiasi ir kelia susirūpinimą, kai yra atsižvelgiama į demokratijos ir interneto technologijų sąveiką. Esminė problematika interneto technologijų ir demokratinių valstybių santykyje:
   2.1. Nėra nustatytas bendras teisinis reglamentavimas skirtas kovai su dezinformacija internete. Europos Sąjunga, o ypač JAV per daug pasitiki gera interneto technologijų bendrovių valia. Dabartinis teisinis reguliavimas (dokumentai ir strategijos) nustato svarbius įsipareigojimus interneto technologijų įmonėms, tačiau šių teisinių idėjų įgyvendinimas nėra pakankamas, nes iki šiol nėra reglamentuotos bendros ir visuotinai taikomos teisės normos skirtos kovai prieš dezinformaciją internete. Dėl šios priežasties skaitmeninėms platformoms yra suteikiama per didelė veiksmų laisvė. Tai kelia grėsmę tiek atskirų valstybių, tiek visos Europos Sąjungos demokratinėms santvarkoms.
   2.2. Internetinio balsavimo problematika demokratinių valstybių santvarkoms atsispindi Europos Sąjungos viešųjų institucijų ir Europos Sąjungos valstybių narių teisiniame reglamentavime bei pozicijose. Dėl šios priežasties, kad egzistuoja galimas išorės subjektų kišimasis į demokratinių valstybių valdymo procesus, internetinis balsavimas galėtų būti įdiegiamas nebent kiekvienos Europos Sąjungos valstybės narės iniciatyva atskirai, taip administruojant rinkimų rezultatus decentralizuotai, nes bendrai Europos Sąjungoje yra skeptiškai žvelgiama į centralizuotą internetinio balsavimo teisinio reguliavimo nustatymą valstybėse narėse.
   2.3. Duomenų apsaugos reglamentavimo problematika atsispindi JAV, kadangi šioje valstybėje nėra nustatytas bendras duomenų apsaugos teisinis

reglamentavimas. Tuo tarpu Europos Sąjungoje duomenų apsaugos klausimas buvo išspręstas dar 2016 m. Reikia pabrėžti, kad tinkamas šio instituto reglamentavimas ir įgyvendinimas išlieka itin svarbus demokratinėms santvarkoms, nes tik tinkamai tvarkant demokratinės valstybės piliečių duomenis galima išvengti manipuliavimo rinkėjų duomenimis, kuriais naudojantis ne kartą buvo siekiama neteisėtai kištis į valstybių demokratinius procesus.

2.4. „Deepfake“ yra kylanti grėsmė demokratinių valstybių santvarkose. Šis interneto technologijų įrankis gali pakenkti demokratiniam valstybių valdymui įvairiais būdais: viešiems debatams, rinkimams, viešųjų institucijų legitimumui, mąstymui, o tai turi neigiamą įtaką patikimos informacijos srautui ir demokratinių valstybių funkcionavimui. „Deepfake“ problematikai kol kas yra skiriama nepakankamai dėmesio teisiniame reglamentavime.

3. Interneto technologijos gali būti įgalinančios platformos, padedančios visiems asmenims pasiekti auditorijas, didinti sąmoningumą ir sukurti didžiulius judėjimus. Nors įvairios įstatymų leidėjų ar viešųjų institucijų iniciatyvos daro teigiamą poveikį demokratijos kokybei, didžioji dalis teisinio reglamentavimo yra nukreipta į technologijų milžinų galios suvaržymą, o ne teigiamą skaitmeninio dalyvavimo skatinimą.
4. Lietuva interneto technologijų atžvilgiu yra glaudžiai susijusi su interneto technologijų įmonėmis ir vyraujančiomis tarptautinėmis interneto technologijų grėsmėmis bei galimybėmis. Lietuvoje galiojantis teisinis reguliavimas interneto technologijų grėsmių Lietuvos demokratijai atžvilgiu – nepakankamas. Be to internetinio balsavimo reglamentavimo idėja Lietuvos demokratijai yra rizikinga, nes tai gali sukelti didžiulę žalą Lietuvos demokratiniams procesams.

PASIŪLYMAI

1. Siūlytina Lietuvos Respublikos įstatymų leidėjui keisti Lietuvos Respublikos politinių kampanijų finansavimo ir finansavimo kontrolės įstatymą (Lietuvos Respublikos politinių kampanijų finansavimo ir finansavimo kontrolės įstatymas 2004 (Žin Nr. IX–2428)) išskiriant atskirą teisinį reglamentavimą socialinių tinklų atžvilgiu. Siūloma įstatymų leidėjui nustatyti teisinį reglamentavimą kuriuo būtų:
   1.1. įpareigojamos politinės partijos ir fiziniai rinkimų kampanijos dalyviai deklaruoti vieną socialinių tinklų paskyrą, kurioje būtų skelbiama informacija, bei kurios matomumas galėtų būti didinamas komerciniu reklamos pirkimu.
   1.2. įpareigojamos politinės partijos ir fiziniai rinkimų kampanijos dalyviai vykdyti visus mokėjimus tik iš vienos, Lietuvos Respublikos vyriausiajai rinkimų komisijai deklaruotos banko sąskaitos, susijusius su socialiniais tinklais.
2. Siūlytina nustatyti teisinį reguliavimą dėl „Deepfake“ keliamo instituto grėsmių reguliavimo. Nurodant galimas šio instituto pasekmes ir rekomendacijas Lietuvos valstybinėms institucijoms – kaip reaguoti į šio kylančio interneto technologijų įrankio grėsmes.
3. Siūlytina atsisakyti internetinio balsavimo idėjos Lietuvoje nacionaliniu lygmeniu įvertinant tai, jog internetinio balsavimo reglamentavimas būtų rizikingas Lietuvos demokratijai. Atsižvelgiant į tai siūlytina Lietuvos didžiosiose savivaldybėse įgyvendinti dalyvaujamojo biudžeto sudarymo projekto nustatymą remiantis Paryžiaus miesto pavyzdžiu. Taip pateisinant dalies Lietuvos visuomenės lūkesčius dėl interneto technologinių įrankių įdiegimo Lietuvos demokratinėje santvarkoje.

LITERATŪROS SĄRAŠAS

Norminiai teisės aktai:

Lietuvos Respublikos teisės aktai:

1. Lietuvos Respublikos vyriausiosios rinkimų komisijos įstatymas 2002 (Valstybės žinios 2002, Nr. IX–985).
2. Lietuvos Respublikos Vyriausybės nutarimas 2003 (Valstybės žinios, 2003 Nr. 24–1002).
3. Lietuvos Respublikos politinių kampanijų finansavimo ir finansavimo kontrolės įstatymas 2004 (Valstybės žinios, 2004 Nr. IX–2428).
4. Lietuvos Respublikos Seimo nutarimas 2006 (Valstybės žinios, 2006 Nr. X–912).
5. Lietuvos Respublikos teisėkūros pagrindų įstatymas 2012 (Valstybės žinios, 2012 Nr. XI–2220).
6. Lietuvos Respublikos kibernetinio saugumo įstatymas 2014 (Valstybės žinios, 2004 Nr. XII–1428).
7. Balsavimo internetu pagrindų įstatymo projektas 2018 (Valstybės žinios, 2018 XIIP–3879(2)).
8. Teisės departamento išvadą 2018 (Valstybės žinios, 2018 Nr. XIIP–3879(2)).
9. Lietuvos Respublikos administracinių nusižengimų kodekso 12, 79, 124, 136, 146, 477, 502 ir 548 straipsnių pakeitimo įstatymas 2021 (Valstybės žinios, 2021 Nr. XIV–182).

Europos Sąjungos teisės aktai:

10. Act concerning the election of the representatives of the Assembly by direct universal suffrage 1976 (No. L 278, 8.10.1976).
11. Charter of Fundamental Rights of the European Union 2000 (2000/C 364/01).
12. Europos Tarybos sprendimas 2002 m. birželio 25 d. ir rugsėjo 23 d. iš dalies keičiantis prie Sprendimo 76/787/EAPB, EEB, Euratomas pridėtą Aktą dėl atstovų į Europos Parlamentą rinkimų remiantis tiesiogine visuotine rinkimų teise (Eurotomas, 2002/772/EB).
13. Europos Sąjungos veikimo sutartis 2012 (OJ C 326, 26.10.2012).

14. 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 *(*OJ L 119, 4.5.2016).
15. European Parliament amendments on the proposal for a regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC (COM(2020)0825 – C9–0418/2020 – 2020/0361(COD)).
16. Europos Parlamento ir Tarybos reglamento pasiūlymas dėl bendrosios skaitmeninių paslaugų rinkos (Skaitmeninių paslaugų aktas), kuriuo iš dalies keičiama Direktyva 2000/31/EB (COM(2020) 825 final 2020/0361(COD)).
17. European Parlament proposal for a regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC (COM(2020)0825 – C9–0418/2020 – 2020/0361(COD)).
18. European Commission Proposal for a Regulation Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) (COM(2021) 206 final 2021/0106(COD)).

Jungtinių Amerikos Valstijų teisės aktai:

19. United States Constitution. The First Amendment (Amendment I) 1791 (USA–010).
20. Communications Decency Act 1996 (47 U.S.C. § 230).
21. The Internet Tax Freedom Act 1998 (ITFA; P.L. 105–277).
22. Federal Trade Commission Act 2006 (15 U.S.C. 41 et seq.).
23. Biometric Information Privacy Act 2008 (740 ILCS 14/).
24. United States Code 2011 (18 U.S.C. § 2710).
25. United States Code 2011 (18 U.S.C. § 2721).
26. United States Code 2011 (15 U.S.C. § 6501).
27. California Consumer Privacy Act 2018 (Assembly Bill No. 375).
28. New York General Business Law 2020 (§ 899–bb).
29. Identifying Outputs of Generative Adversarial Networks Act 2020 (H.R. 4355 (116th).
30. The Massachusetts General Law Chapter 93H 2021 (201 CMR 17.00).

31. Virginia Consumer Data Protection Act 2021 (SB 1392).
32. United States National Defense Authorization Act 2021 (H.R.4350).

Vokietijos Federacinės Respublikos teisės aktai:

33. Network Enforcement Act 2017 (2017/127/D).

Suomijos Respublikos teisės aktai:

34. Citizens Initiative Act 2012 (12/2012)).

Specialioji literatūra:

35. Beetham, D. 1992, *Liberal Democracy and the Limits of Democratization*. Political Studies, special issue vol. 40, p. 40.
36. Street, J. 1997, *Remote Control? Politics, Technology and Electronic democracy*. European Journal of Communication.
37. Lietuva. Lietuvos teisės universitetas 2002, *Lietuvos Konstitucinė teisė.* Lietuvos teisės universitetas, Vilnius.
38. Henry, S. 2003, *Can remote internet voting increase turnout?* ASLIB Proc.
39. Gibson, R. K., Nixon, P. G., Ward, S. J. 2003, *Political Parties and the Internet Net Gain?* Routledge, New York.
40. Lietuva. Mykolo Romerio Universitetas 2004, *Informacinių technologijų teisė.* Mykolo Romerio universitetas, Vilnius.
41. Garrone, P. 2004, *Fundamental and political rights in electronic elections*. Routledge, New York.
42. Šileikis, E. 2005, *Alternatyvi Konstitucinė teisė.* Teisinės informacijos centras, Vilnius.
43. Auer, A., Mendez, M. 2005, *Introducing e–voting for the European Parliament elections: the constitutional problems'*. In A. H. Trechsel & F. Mendez (Eds.), The European Union and e–voting: addressing the European Parliament's Internet voting challenge. Routledge, New York.
44. Madise, U., T. Martens. 2006, *E–voting in Estonia 2005. The first practice of the country–wide binding Internet voting in the world*. DBLP, Trier.

45. Cammaerts, B. and Carpentier, N. 2007, *Reclaiming the media. Communication rights and democratic media roles*. Bristol/Chicago: Intellect.
46. Vaišvila, A. 2009, *Teisės teorija.* Justicia, Vilnius.
47. Noveck, B., 2009. *Wiki Government: How Technology Can Make Government Better, Democracy Stronger, and Citizens More Powerful*. Washington: Brookings Institution Press.
48. Bochsler, D. 2009, *Can the Internet Increase Political Participation? An Analysis of Remote Electronic Voting's Effect on Turnout*. DISC working papers, 2009/9. Central European University. [interaktyvus; žiūrėta: 2022 m. kovo 20 d.]. Prieiga per internetą: https://core.ac.uk/download/pdf/11869589.pdf
49. Charles, A. 2009, *The Electronic State: Estonia's New Media Revolution*. Journal of Contemporary European Research, Vol. 5, No. 1, p. 97–113. [interaktyvus; žiūrėta: 2022 m. kovo 20 d.]. Prieiga per internetą: http://www.jcer.net/ojs.index.php/jcer/article/view/122/127
50. Lietuva. Mykolo Romerio Universitetas 2009, *Teisė ir demokratija. Demokratija Lietuvoje: tarp Vakarų ir Rytų (1990–2007m.)*. Mykolo Romerio universitetas, Vilnius.
51. Pasquale, F. 2011, *Still in Decline? Party Membership in Europe*. Editions de l'Université de Bruxelles.
52. Boulianne, S. 2015, *Social media use and participation: a meta–analysis of current research*. London: Routledge.
53. Rousseau, J. 2015, *Visuomenės sutartis.* Vaga, Vilnius.
54. Pasquale, F. 2015, *The Black Box Society: The Secret Algorithms that Control Money and Information*. Book Gallery. 96.
55. Lietuva. Mykolo Romerio Universitetas 2016, *Interneto ir technologijų technologijų teisė.* Mykolo Romerio universitetas, Vilnius.
56. Abdurashid, S. 2016, *Voter Turnout Trends around the World*. International Institute for Democracy and Electoral Assistance.
57. Garton Ash, T. 2016, *Free Speech: Ten Principles for a Connected World*. WorldLondon: Atlantic Books.
58. King, G., Pan, J., Roberts,. M. 2017, *How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument*. American Political Science review.
59. Lietuva. Mykolo Romerio Universitetas 2017, *Lietuvos Konstitucinė teisė.* Mykolo Romerio universitetas, Vilnius.

60. Flynn. D. J., Nyhan, B., Reifler., J. 2017, *The Nature and Origins of Misperceptions: Understanding False and Unsupported Beliefs About Politics*. Political Psychology.
61. Buning, C. 2018, *A multi–dimensional approach to disinformation: report of the independent High level Group on fake news and online disinformation. Luxembourg.* Publications Office of the European Union.
62. Bennett. W., Livingston, S. 2018, *The Disinformation Order: Disruptive Communication and the Decline of Democratic Institutions*. European Journal of Communication. Social Media + Society.
63. Vosoughi, S., Roy, D., Aral, S. 2018, *The spread of true and false news online.* Science, vol 359(6380)).
64. Meškauskaitė, L. 2018, *Žiniasklaidos teisė.* Registrų centras, Vilnius.
65. Hale, S.A., John, P., Margetts, H., Yasseri. T. 2018, *How digital design shapes political participation: A natural experiment with social information*. PLOS ONE.
66. Colomina, C. 2019, *Real and Virtual Threats: Europe's Vulnerability to Disinformation. Researcher*. CIDOB.
67. Citron K., Chesney, R. 2019, *'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*. University of California Berkeley School of Law.
68. Aleksynaitė, G. 2019*, Socialinių tinklų atsakomybė už jų vartotojų skelbiamą informaciją*: magistro darbas. Socialiniai mokslai, teisė (01S). Vilniaus universitetas, Vilnius.
69. Xia, Y., Lukito, J., Zhang, Y., Wells, C., Kim, S., Tong, C. 2019, *Disinformation, Performed: Self–Presentation of a Russian IRA Account on Twitter.* Information, Communication & Society.
70. Ker, Nic. 2019, *Is the Political Aide Viral Sex Video Confession Real or a Deepfake*?. Malay Mail.
71. Bateman, J. 2020, *Deepfakes and Synthetic Media in the Financial System: Assessing Threat Scenario*. Carnegie Endowment for International Peace.
72. Matonis, G. 2020, *Garbės ir orumo gynimas socialiniuose tinkluose*: magistro darbas. Socialiniai mokslai, teisė (01S). Vilniaus universitetas, Vilnius.
73. Kornbluh, K. ir Goodman E. 2020, *Safeguarding Digital Democracy. Digital Innovation and Democracy Initiative Roadmap*. The German Marshall Fund of the United States DIDI Roadmap.

74. Madiega, T. 2020, *Reform of the EU liability regime for online intermediaries: Background on the forthcoming digital services act*. European Parliamentary Research Service.
75. Pradhan, P. 2020, *AI DeepfakesThe Goose Is Cooked?* University of Illinois Law Review.
76. Helberger, N. 2020, *The Political Power of Platforms: How Current Attempts to Regulate Misinformation Amplify Opinion Power*. Digital Journalism.
77. Schick, N. 2020, *Deep Fakes and the Infocalypse*. Octopus Publishing Group.
78. Vaccari, C., Chadwick, A. 2020, *Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception. Uncertainty, and Trust in News*. Sage journals. [interaktyvus; žiūrėta: 2022 m. kovo 20 d.]. Prieiga per internetą: https://journals.sagepub.com/doi/full/10.1177/2056305120903408
79. Helm, R. and Nasu, H. 2021, *Regulatory responses to 'fake news' and freedom of expression: Normative and empirical evaluation*. Human Rights Law Review.
80. Stark, D. and Pais, I. 2021, *Algorithmic Management in the Platform Economy*. Sociologica.

Teismų praktika:

Europos Žmogaus Teisių Teismo praktika:

81. *Yildirim v Turkey* (2012) Europos Žmogaus Teisių Teismas. Nr. 3111/10.

Jungtinių Amerikos Valstijų teismų praktika:

82. *See Reno v. ACLU* (1997) Jungtinių Amerikos Valstijų Aukščiausiasis Teismas 521 U.S. 844.

Lietuvos Respublikos Teismų praktika:

83. Lietuvos Respublikos Konstitucinio Teismo 2000 m. vasario 23 d. nutarimas. Valstybės žinios, Nr. 17-419.
84. Lietuvos Respublikos Konstitucinio Teismo 2002 m. rugsėjo 19 d. nutarimas. Valstybės žinios, Nr. 93-4000.

85. Lietuvos Respublikos Konstitucinio Teismo 2011 m. birželio 21 d. nutarimas. Valstybės žinios, Nr. 76-3672.
86. Lietuvos Respublikos Konstitucinio Teismo 2012 m. gruodžio 19 d. nutarimas. Valstybės žinios, Nr. 152-7779.
87. Lietuvos Respublikos Konstitucinio Teismo 2014 m. liepos 11 d. nutarimas. Valstybės žinios, Nr. 10117.

Kita praktinė medžiaga:

88. Perry Barlow, 1996. Declaration of the Independence of Cyberspace. [interaktyvus; žiūrėta: 2022 m. kovo 20 d.]. Prieiga per internetą: https://www.eff.org/cyberspace–independence
89. Pew Research Center, 2011. Buvusioje Sovietų Sąjungoje mažėja pasitikėjimas demokratija ir kapitalizmu. [interaktyvus; žiūrėta: 2022 m. kovo 20 d.]. Prieiga per internetą: https://www.pewresearch.org/global/2011/12/05/chapter–1–views–of–democracy/
90. Europos Tarybos Ministrų Kabineto rekomendacijos CM/Rec(2012)4 dėl žmogaus teisių apsaugos, teikiant socialinių tinklų paslaugas.
91. Rights, Equality and Citizenship Programme, 2014-2020. rieiga per internetą: https://ec.europa.eu/justice/grants1/programmes-2014-2020/rec/index_en.htm
92. Erasmus+, 2015. Erasmus+ anual report. [interaktyvus; žiūrėta: 2022 m. kovo 20 d.]. Prieiga per internetą: https://erasmus-plus.ec.europa.eu/sites/default/files/erasmus-plus-annual-report-2015.pdf
93. World Economic Forum, 2016. Values and the Fourth Industrial Revolution: Connecting the Dots Between Value, Values, Profit and Purpose. [interaktyvus; žiūrėta: 2022 m. kovo 20 d.]. Prieiga per internetą: https://www.weforum.org/whitepapers/values–and–the–fourth–industrial–revolution–connecting–the–dots–between–value–values–profit–and–purpose
94. Michigan University, 2017. Independent Report on E–voting in Estonia. [interaktyvus; žiūrėta: 2022 m. kovo 20 d.]. Prieiga per internetą: https://estoniaevoting.org
95. Microsoft EU Policy blog, 2017. From Submarines to Cyber: Estonia's Innovation Journey. [interaktyvus; žiūrėta: 2022 m. kovo 20 d.]. Prieiga per internetą: https://blogs.microsoft.com/eupolicy/2017/11/29/submarines–cyber–estonias–innovation–journey/

96. Cabannes, Y. 2017. Participatory Budgeting in Paris: Act, Reflect, Grow. . [interaktyvus; žiūrėta: 2022 m. kovo 20 d.]. Prieiga per internetą: https://budgetparticipatif.paris.fr/bp/plugins/download/PB_in_Paris.pdf
97. Europos Komisijos Bendras komunikatas Europos Parlamentui, Europos Vadovų Tarybai, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui dėl veiksmų plano prieš dezinformaciją. JOIN(2018) 36 final, 2018 m. gruodžio mėn. [interaktyvus; žiūrėta: 2022 m. kovo 20 d.]. Prieiga per internetą: https://ec.europa.eu/info/sites/default/files/eu–communication–disinformation–euco–05122018_en.pdf
98. European Commission, 2018. Independent High level Group on fake news and online disinformation, A multidimensional approach to disinformation. [interaktyvus; žiūrėta: 2022 m. kovo 20 d.]. Prieiga per internetą: https://op.europa.eu/en/publication–detail/–/publication/6ef4df8b–4cea–11e8–be1d–01aa75ed71a1/language–en
99. European Commission. EU budget: Commission proposes €9.2 billion investment in first ever digital programme. [interaktyvus; žiūrėta: 2022 m. kovo 20 d.]. Prieiga per internetą: https://ec.europa.eu/commission/presscorner/detail/en/IP_18_4043
100. The New York Times, 2018. Cambridge Analytica and Facebook: The Scandal and the Fallout So Far. [interaktyvus; žiūrėta: 2022 m. kovo 20 d.]. Prieiga per internetą: https://www.nytimes.com/2018/04/04/us/politics/cambridge–analytica–scandal
101. Julian King: Democracy is under threat from the malicious use of technology. The EU is fighting back. [interaktyvus; žiūrėta: 2022 m. kovo 20 d.]. Prieiga per internetą:https://www.theguardian.com/commentisfree/ 2018/jul/28/democracy–threatened malicious–technology–eu–fighting–back
102. Michelle Ma, 2018. The Impact of Technology on Democracy. [interaktyvus; žiūrėta: 2022 m. kovo 20 d.]. Prieiga per https://www.wsj.com/articles/the–impact–of–technology–on–democracy–1541943796
103. Ian Bogost, 2018. *Europe's Smack to Google May Only Be the Beginning*. [interaktyvus; žiūrėta: 2022 m. kovo 20 d.]. Prieiga per https://www.theatlantic.com/technology/archive/2018/07/europe–google–antitrust–fine/565505/
104. Kang, C., Frenkel, S. 2018, Facebook says Cambridge Analytica harvested data of up to 87 million users. The New York Times. [interaktyvus; žiūrėta: 2022 m. kovo 20 d.]. Prieiga per internetą: https://www.nytimes.com/2018/04/04/technology/mark–zuckerberg–testify–congress.html

105. Pew Research Center, 2018. How social media users have discussed sexual harassment since #MeToo went viral. [interaktyvus; žiūrėta: 2022 m. kovo 20 d.]. Prieiga per internetą: https://www.pewresearch.org/fact–tank/2018/10/11/how–social–media–users–have discussed–sexual–harassment–since–metoo–went–viral
106. Nacionalinio kibernetinio saugumo centras, 2019. Nacionalinio kibernetinio saugumo būklės ataskaita 2019. [interaktyvus; žiūrėta: 2022 m. kovo 20 d.]. Prieiga per internetą: https://www.nksc.lt/doc/NKSC_ataskaita_2019.pdf;
107. Lapowsky, I. 2019, How Cambridge Analytica sparked the great privacy awakening. Wired. [interaktyvus; žiūrėta: 2022 m. kovo 20 d.]. Prieiga per internetą: https://www.wired.com/story/cambridge–analytica–facebook–privacy–awakening/
108. Kang, C. 2019, F.T.C. approves Facebook fine of about $5 billion. The New York Times. [interaktyvus; žiūrėta: 2022 m. kovo 20 d.]. Prieiga per internetą: https://www.nytimes.com/2019/07/12/technology/facebook–ftc–fine.html
109. Peters, J. 2019, Facebook launches new market research app after shutting down its controversial VPN service. The Verge. [interaktyvus; žiūrėta: 2022 m. kovo 20 d.]. Prieiga per internetą: https://www.theverge.com/2019/11/25/20982367/facebook–viewpoints–new–market–research–app–study–survey–rewards
110. Europos Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui dėl Europos demokratijos veiksmų plano COM/2020/790). [interaktyvus; žiūrėta: 2022 m. kovo 20 d.]. Prieiga per internetą: https://eur–lex.europa.eu/legal–content/LT/TXT/PDF/?uri=CELEX:52020DC0790&from=EN
111. LR Valstybės saugumo departamentas, Antrasis operatyvinių tarnybų departamentas prie Krašto apsaugos ministerijos, 2020.Grėsmių nacionaliniam saugumui vertinimas 2020. [interaktyvus; žiūrėta: 2022 m. kovo 20 d.]. Prieiga per internetą: https://www.vsd.lt/wp–content/uploads/2020/02/2020–Gresmes–LT–.pdf
112. European Commission, 2020. Horizon 2020. [interaktyvus; žiūrėta: 2022 m. kovo 20 d.]. Prieiga per internetą: https://ec.europa.eu/info/research–and–innovation/funding/funding–opportunities/funding–programmes–and–open–calls/horizon–2020_en
113. 15min, 2020. Interneto žiniasklaidos asociacija ragina VRK imtis priemonių dėl politinės reklamos socialiniuose tinkluose. [interaktyvus; žiūrėta: 2022 m. kovo 20 d.]. Prieiga per internetą: https://www.15min.lt/naujiena/aktualu/lietuva/interneto–

ziniasklaidos–asociacija–ragina–vrk–imtis–priemoniu–del–politines–reklamos–socialiniuose–tinkluose–56–1374364?copied

114. European Commision, 2021. Code of Practice on Disinformation. Prieiga per internetą: https://digital–strategy.ec.europa.eu/en/policies/code–practice–disinformation

115. LRT, 2021. Postūmis siekiant internetinio balsavimo: nuspręsta pirkti galimybių studiją, paruoštas įstatymo projektas. [interaktyvus; žiūrėta: 2022 m. kovo 20 d.]. Prieiga per internetą: https://www.lrt.lt/lituanica/aktualijos/751/1568100/postumis–siekiant–internetinio–balsavimo–nuspresta–pirkti–galimybiu–studija–paruostas–istatymo–projektas

116. Statista, 2021. [interaktyvus; žiūrėta: 2022 m. kovo 20 d.]. Prieiga per internetą: https://www.statista.com/statistics/268604/annual–revenue–of–facebook/#:~:text=In%202021%2C%20Meta's%20(formerly%20Facebook,in%20the%20previous%20fiscal%20year.

117. Global Social Media Stats, 2022. [interaktyvus; žiūrėta: 2022 m. kovo 20 d.]. Prieiga per internetą: https://datareportal.com/social–media–users#:~:text=Kepios%20analysis%20shows%20that%20there,of%20the%20total%20global%20population

SANTRAUKA

Šiandieniniame pasaulyje interneto technologijos suteikia galimybių kiekvienam iš mūsų. Tačiau tiriant interneto technologijų įtaką demokratiniam valstybių valdymui galime pastebėti, kad interneto technologijos sudaro sąlygas skleisti populizmą ir dezinformaciją. Interneto technologijos gali būti panaudotos prieš demokratiją nukreiptiems tikslams įgyvendinti. Matomas populizmo augimas visame pasaulyje sutapo su interneto technologijų sukelta revoliucija. Tad pastebėtina, kad internetinė aplinka yra palanki dezinformacijos ir poliarizacijos kampanijoms, kurių pagalba galima sugriauti senąją tvarką, panaudojant naujus manipuliavimo įrankius – interneto technologijas. Tai turi būti sustabdyta, pasitelkiant tinkamą teisinį reglamentavimą. Kadangi šiuo metu galiojantys įstatymai yra nepakankami ir išsamiai neapibrėžiantys interneto technologijų poreikių demokratijos atžvilgių. Šiuo laikotarpiu galiojančius įstatymus reikia tobulinti, siekiant atsverti interneto technologijų sukeliamą žalą į naudos pusę. Tokios interneto technologijų galimos grėsmės kaip dezinformacija internete, internetinio balsavimo nepatikimumas, duomenų apsaugos problemos bei „deepfake“ iššūkiai gali sukelti didžiulę žalą demokratiniam valstybių valdymui.

Atsižvelgiant į tai, darbo tema yra aktuali tiek teisiniu, tiek socialiniu aspektu, kadangi yra pastebimas didelis visuomenės naudojimasis socialiniais tinklais, su iššūkiais susiduriančios valstybių demokratijos ir egzistuojantis itin aukštas teisinio neapibrėžtumo lygis – visa tai leidžia pagrįsti šio darbo iškeltą hipotezę interneto technologijos demokratiniam valstybės valdymui sukelia daugiau grėsmių negu suteikia galimybių.

SUMMARY

In today's world, internet technology offers opportunities to every one of us. However, when studying the impact of Internet technologies on the democratic governance of states, we can observe that Internet technologies facilitate the spread of populism and disinformation. Internet technologies can be used for anti-democratic purposes. The visible growth of populism around the world coincided with the revolution brought about by Internet technology. Thus, it should be noted that the online environment is conducive to disinformation and polarization campaigns, which can disrupt the old order by using new manipulation tools - Internet technologies. This must be stopped through appropriate regulation, because the current laws are insufficient and do not fully define the requirements for Internet technology in terms of democracy. Existing laws need to be improved to actually materialise the benefits of Internet technology. Potential threats from online technologies such as online misinformation, the unreliability of online voting, data protection issues and the challenges of deepfake can cause great damage to democratic governance.

In this context, the topic of the work is relevant from both a legal and a social point of view, as there is a high level of public use of social networks, challenging democracies and a high level of legal uncertainty posing more threats than opportunities.