Vilniaus universitetas

TARPTAUTINIŲ SANTYKIŲ IR POLITIKOS MOKSLŲ INSTITUTAS

TARPTAUTINIŲ SANTYKIŲ IR DIPLOMATIJOS MAGISTRO PROGRAMA

KRISTINA SELIVANOVAITĖ

II kurso studentė

SUVERENUS VALSTYBIŲ INTERNETAS ŽMOGAUS TEISIŲ KONTEKSTE: KINIJOS IR RUSIJOS KIBERNETINĖS ERDVĖS REGULIAVIMO LYGINAMOJI ANALIZĖ

MAGISTRO DARBAS

Darbo vadovas: Dr. Konstantinas Andrijauskas

Vilnius, 2024 m.

Magistro darbo vadovo išvados dėl darbo gynimo:

.....
.....
.....

....

(data) (v., pavardė) (parašas)

Magistro darbas įteiktas gynimo komisijai:

....

(data) (Gynimo komisijos sekretoriaus/ės parašas)

Magistro darbo recenzentas/ė:

.....

(v., pavardė)

Bakalauro/magistro darbų gynimo komisijos įvertinimas:

.....

Komisijos pirmininkas/ė:

Komisijos nariai:

PATVIRTINIMAS APIE ATLIKTO DARBO SAVARANKIŠKUMĄ

Patvirtinu, kad įteikiamas magistro darbas „Suverenus valstybių internetas žmogaus teisių kontekste: Rusijos ir Kinijos kibernetinės erdvės lyginamoji analizė“ yra:

1. Atliktas mano paties ir nėra pateiktas kitam kursui šiame ar ankstesniuose semestruose;
2. Nebuvo naudotas kitame Institute/Universitete Lietuvoje ir užsienyje;
3. Nenaudoja šaltinių, kurie nėra nurodyti darbe, ir pateikia visą panaudotos literatūros sąrašą.

Kristina Selivanovaitė

BIBLIOGRAFINIO APRAŠO LAPAS

Selivanovaitė K. ***Suverenus valstybių internetas žmogaus teisių kontekste: Kinijos ir Rusijos kibernetinės erdvės reguliavimo lyginamoji analizė:*** Politikos mokslų specialybės magistro darbas / VU Tarptautinių santykių ir politikos mokslų institutas; darbo vadovas Dr. Konstantinas Andrijauskas. – Vilnius, 2024. – 63 p.

Reikšmingi žodžiai: Suverenus internetas, interneto susiskaldymas, kibernetinė erdvė, Kinija, Rusija

Šiame darbe yra nagrinėjama Kinijos ir Rusijos formuojamas suverenus valstybių internetas siekiant išsiaiškinti, kaip Kinija ir Rusija formuluoja kibernetinio suverenumo doktriną ir ją įgyvendina praktiškai santykyje su Vakaruose vyraujančiais žmogaus teisių principais internete. Teorinėje darbo dalyje aptariama tikslingiausia tarptautinių santykių teorija, kuri padeda nagrinėti kibernetinės erdvės gilumines problemas tokias, kaip žmogaus teisės. Šiuo atveju, remiantis Nye išsiaiškinta, jog tarptautinių režimų teorija yra tikslingiausia. Empirinėje darbo dalyje pasirinkta nagrinėti *Freedom House* kasmetinius Kinijos ir Rusijos raportus, kuriuose aiškinamasi, kaip nuo 2015 m. atrodo šalių kibernetinė erdvė atsižvelgiant būtent į žmogaus teisių aspektus. Taip pat nagrinėjami Kinijos ir Rusijos pagrindiniai įstatymai dėl kibernetinės erdvės veikimo principų, kurie yra susiję su formuojamu suverenumu kibernetinėje erdvėje. Darbo pabaigoje pateikiamos išvados, kaip Kinijoje ir Rusijoje atrodo formuojama suverenaus valstybių interneto doktrina ir kaip praktiškai tai sąveikauja su Vakaruose vyraujančiu žmogaus teisių principu internete.

Turinys

Santrumpų sąrašas

1. JT – Jungtinės Tautos;
2. NVO – Nevyriausybinė organizacija;
3. EŽTK – Europos Žmogaus Teisių komitetas;
4. IT – informacinės technologijos;
5. KE – kibernetinė erdvė;
6. JAV – Jungtinės Amerikos Valstijos;
7. ES – Europos Sąjunga;
8. KLR – Kinijos Liaudies Respublika;
9. KKP – Kinijos komunistų partija;
10. JAE – Jungtiniai Arabų Emyratai;
11. ITPK – Interneto teisių ir principų koalicija

Įvadas

KE yra neatsiejama tarptautinių santykių ir diplomatijos sudedamoji dalis. Sparčiai plėtojantis internetui ir informacinėms technologijoms, KE ir internetas savaime tapo didžiųjų valstybių konfrontacijos lauku.[1]

Interneto tinklo pradinę paradigmą galime apibūdinti kaip demokratijos ir liberalizmo principais paremtą aplinką, kurioje laisvai sąveikauja multikultūrinė informacija. Barlow neoficialiu protokolu „*Kibernetinės erdvės nepriklausomybės deklaracija*“ viešai deklaravo laisvo interneto prigimtį pabrėždamas, jog skaitmeninėje erdvėje valdžios institucijoms nėra vietos ir kad tinklas neturi sienų, ypatingai – valstybės ribų, todėl privalo būti nepriklausomas.[2] Tuo tarpu Wu nagrinėjo valstybių elgesį suverenaus interneto kontekste teigdamas, kad internetas vienaip ar kitaip yra valdomas valstybės, korporacijų ir organizacijų.[3] Taip KE įgyja dviprasmiškumo statusą, viena vertus apibūdinant internetą kaip laisvą ir beribį, kurio skaitmeninės aplinkos valstybės institucijos negali apjuosti valstybės ribomis, kita vertus, teigiant, jog internetas yra valdomas ne vieno subjekto, įskaitant ir pačias valstybes. Taigi, anot Wu, tarpvalstybinis dialogas siekiant išlaikyti laisvą internetą tuo pačiu užtikrinant nacionalinį valstybės suverenitetą – būtinas.[4]

IT, socialinių ir politikos mokslų šaltiniuose pastebima sąvoka „*The Splinternet*“ – interneto skilimas, susiskaldymas, susiskaidymas. Vykstant interneto skilimui, yra grįžtama prie ryškių, KE nacionalinių sienų „aptvėrimo“, kuriomis tarsi bandoma išryškinti valstybės interneto ribą.[5] Craws interneto susiskaldymą paaiškina kaip lygiagretų interneto tinklą, kuris valdomas atskirai ir skirtingų segmentų su iš anksto nustatytomis taisyklėmis, kurios susijusios su privatumu ir kitais valdymo reguliavimo klausimais[6], arba, kitaip sakant, interneto susiskaldymo įtakotas tarptautinis interneto tinklas tampa daugiapoliu.[7] Įvairių sričių mokslininkai kalba apie iš interneto susiskaldymo kylančias grėsmes, apimančias ne tik kibernetinę erdvę, bet ir žmogaus teises bei laisvę. Hoffmann et. al. ‘„splinterneto“ problemą apibrėžia taip: „*Interneto tinklo suskaidymas sukeltų naujų iššūkių kibernetinei gynybai ir priešininkams galėtų suteikti tam tikras technines priemones, kurios pakenktų šiandieninės kibernetinės erdvės normoms,* nuspėjamumui *ir saugumui, o taip pat, tai įtakotų ir*

---

[1] Ovgu Kalkan Kucuksolak, „Cyberspace: The Fifth Domain of Escalating Security Challenges, „*International Relations & Law* 24, No.15, (2018): 25.

[2] John P. Barlow, *A Declaration of the Independence of Cyberspace,* Editions-hache, 1996.

[3] Timothy S. Wu, „Cyberspace Sovereignty? – The Internet and the International System“ *Harvard Journal of Law & Technology* 10, No. 3 (1997): 648-666.

[4] *Ibid*.

[5] Mark A. Lemley, „The Splinternet“ *Stanfort Law and Economics Olin Working Paper* 555 (2021).

[6] Clyde Wayne Crews, „One Internet Is Not Enough“, Cato Institute, žiūrėta 2024 m. kovo 1 d. https://www.cato.org/techknowledge/one-internet-not-enough .

[7] Scott Malcomson, *Splinternet: How Geopolitics and Commerce are Fragmenting the World Wide Web* (Indija: AarkMany Media, 2016), 112.

neigiamai paveiktų žmogaus teises ir padidintų skaitmeninę atskirtį.“[8] Tuo tarpu Blumberg interneto susiskaldymo kylančią grėsmę įvardija gilesniame kontekste, t. y. verslui, IT inovacijoms ir politinei ideologijai, šiuo atveju būtent demokratijai.[9] Nepaisant kylančios grėsmės tarptautinei bendruomenei dėl tinklo skilimo, manoma, jog dėl interneto vartotojų įvairovės ir interesų bei sprendimų priėmėjų reglamentų kitoniškumo, tinklo skilimas tęsis.[10]

Žvelgiant iš geopolitinės prizmės, Vašingtono, Maskvos ir Pekino jėgų vaidmuo kibernetinėje erdvėje – kritiškas. JAV kibernetinę erdvę laiko laisva ir demokratiniais principais paremta tarptautine aplinka, tuo tarpu Rusija ir Kinija vienbalsiai nepritaria jau galiojantiems Vakarų tarptautiniams principams dėl KE valdymo. Todėl, pasak JAV, tai atitinkamai kelia didelį kibernetinių atakų pavojų, kurios gali būti tokios pat destruktyvios kaip rugsėjo 11-osios išpuolis.[11] Šiuo atveju KE globalų požiūrį galime skirstyti į dviejų pasaulio hegemonų segmentus, t. y. Vakarų (JAV) – paremtas demokratija ir liberalių principų veikiamas internetas, kuriame laisvai ir decentralizuotai teka multikultūrinė informacija, ir Rytų (Kinija ir Rusija) – autoritarinis požiūris į skaitmeninę erdvę, kuri turi būti centralizuotai valdoma, brėžianti geopolitines valstybės ribas, cenzūruojama ir kontroliuojama režimo labui. Kinijos ir Rusijos potenciali KE valdymo režimų sąveika ir pasekmės gali apimti platų spektrą: nuo geopolitinės galios dinamikų, tarptautinio bendradarbiavimo iki IT poveikio.[12]

2015 m. Kinijos prezidentas Xi Jinping Pekino remiamoje pasaulinėje interneto konferencijoje į tarptautinių santykių diskursą įtraukė „interneto suvereniteto“ arba kitaip „kibernetinės erdvės suverenumo“ sąvoką, propaguodamas idėją, jog KE turi būti valdoma pagal tuos pačius principus kaip ir kitos geopolitinės sritys. Tai vienas iš Kinijos siekių nustatinėti savo primetamas normas tarptautinėje interneto tinklo valdymo srityje.[13] Xi kibernetinėje erdvėje brėžia ryškias nacionalines ribas kurdamas savitą interneto tinklą „*ChinaNet*“[14], o nuo 1996 m. Kinijoje plėtojama „Didžioji

---

[8] Stacie Hoffmann et. al., „Standardising the splinternet: how China‘s technical standarts could fragment the internet“ *Journal of Cyber Policy,* 5, No.2 (2020): 239

[9] Deborah Lynn Blumberg, „3 ways the ‚splinternet‘is damaging society“, Management Sloan School, žiūrėta 2024 vasario 25 d., https://mitsloan.mit.edu/ideas-made-to-matter/3-ways-splinternet-damaging-society .

[10] Robbie Fordyce, „What is the ‚splinternet‘? Here‘s why the internet is less whole than you might think“, The Conversation, žiūrėta 2024 vasario 25 d., https://theconversation.com/what-is-the-splinternet-heres-why-the-internet-is-less-whole-than-you-might-think-207033 .

[11] A Liaropoulos, „Exercising State Sovereignty in Cyberspace: An International Cyber-Order under Construction?“ *Journal of Information Warfare* 12, No. 2 (2013): 23.

[12] Clement Perarnaud et al., „‘Splinternets‘: Addressing the renewed debate on internet fragmentation“ *European Parliamentary Research Service* PE 729.530, (2022): 1-3.

[13] Jinghan Zeng, Tim Stevens ir Yaru Chen, „China‘s Solution to Global Vyber Governance: Unpacking the Domestic Discourse of „Internet Sovereignty““, *Politics & Policy,* 45, No.3 (2017): 434.

[14] Elizabeth C. Economy, „The great firewall of China: Xi Jinping‘s internet shutdown“, The Guardian, žiūrėta 2024 m. vasario 25 d.,https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown .

ugniasienė“, kuri oficialiai pradėjo veikti 2000 m.[15], taip pat 2006 m. patvirtintas „Auksinio skydo projektas“[16], kuris blokuoja prieigą prie daugelio užsienio naujienų[17], lėtina užsienio domenų srautą, filtruoja turinį griežtai cenzūruojant internete esančią informaciją. Tuo tarpu Rusija žengia Kinijos keliu ir, ypatingai invazijos Ukrainoje metu, imasi užsienio portalų blokavimo.[18] 2019 m. Vladimiras Putinas pasirašė įstatymą, leidžiantį kurti suverenų valstybės internetą atsijungiant nuo likusio pasaulio ir suteikiant galimybę įkalinti žmones, kurie šalies interaktyvioje erdvėje skleidžia Kremliui opozicinį naratyvą.[19] Rusijos atsijungimas nuo pasaulinio interneto nesiejamas su potencialia grėsme Vakarams, tai kelia pačių rusų laisvos informacijos sklaidos ribojimą, taip pat tai vienareikšmiškai pagreitina tarptautinio tinklo skilimą[20] bei turi įtakos Rusijos piliečių žmogaus teisėms. Būtent Kinijos ir Rusijos formuojamas suverenus valstybių internetas yra šio darbo **objektas**.

Wang teigia, Kinijos turinio filtravimas atspindi pagrindines socialistines vertybes tiek kibernetinio, tiek ir nacionalinio saugumo atžvilgiu, nes, anot autoriaus, Xi suverenaus interneto politikos pagrindinis tikslas yra siekti ekonomikos augimo, o tam reikia vidinio šalies stabilumo per nacionalinį valstybės saugumo užtikrinimą.[21] Tuo tarpu žvelgiant į Rusiją, pastarosios argumentai dėl suverenaus valstybės interneto formavimo nėra tik vidaus politikos interesas, o atvirai nukreiptas prieš, anot Kremliaus, kylantį Vakarų KE pavojų. Costigan pabrėžia, jog Rusijos suverenus valstybės internetas „*RuNet*“ iš esmės yra nukreiptas prieš Vakarų valstybes Kremliui teigiant, jog Vakarai piktybiškai nusitaikę į Rusijos kritinę infrastruktūrą, kuriai yra iškilusi grėsmė dėl stabilumo, saugumo ir funkcinio vientisumo.[22]

Kinijos ir Rusijos argumentai dėl nacionalinio tinklo valdymo iš esmės parodo, jog Xi ir Putinas turi skirtingus požiūrius dėl KE kontroliavimo, nors valstybių veiksmai valdant skaitmeninę aplinką iš esmės turi panašumų. Abi valstybės taiko pakankamai sudėtingus būdus, jog kontroliuotų teritorinę

---

[15] Yaqiu Wang, „In China, the „Great Firewall“ Is Changing a Generation“, POLITICO, žiūrėta 2024 m. vasario 25 d., https://www.politico.com/news/magazine/2020/09/01/china-great-firewall-generation-405385 .

[16] Xiao Qiang, „How China‘s Internet Police Control Speech on the Internet‘‘, Radio Free Asia, žiūrėta 2024 m. vasario 25 d., https://www.rfa.org/english/commentaries/china_internet-11242008134108.html .

[17] Lietuvos nacionalinis radijas ir televizija, „Kinijos valdžia blokuoja užsienio žiniasklaidos portalus, kurių žurnalistai dirba šalyje“, LRT, žiūrėta 2024 m. vasario 25 d.,https://www.lrt.lt/naujienos/pasaulyje/6/1109130/kinijos-valdzia-blokuoja-uzsienio-ziniasklaidos-portalus-kuriu-zurnalistai-dirba-salyje .

[18] Lietuvos rytas, „Leidžiasi skaitmeninė Geležinė uždanga: Rusijos internetas netrukus gali tapti panašus į Kinijos internetą“, Lrytas, žiūrėta 2024 m. vasario 24 d.,https://www.lrytas.lt/it/ismanyk/2022/03/08/news/leidziasi-skaitmenine-gelezine-uzdanga-rusijos-internetas-netrukus-gali-tapti-panasus-i-kinijos-interneta-22650678#google_vignette .

[19] Nathan Hodge ir Mary Ilyushina, „Putin signs law to create an independent Russian internet“, CNN, žiūrėta 2024 m. vasario 24 d., https://edition.cnn.com/2019/05/01/europe/vladimir-putin-russian-independent-internet-intl/index.html .

[20] Lietuvos rytas, *Leidžiasi skaitmeninė Geležinė uždanga.*

[21] Anqi Wang, „Cyber Sovereignty as Its Boldest: A Chinese Perspective“ *Ohio State Technology Law Journal* 16, No. 2 (2020).

[22] Sean Costigan, „Trouble in Cyberspace: increasing crime and exporting authoritarianism, Iris Report, žiūrėta 2024 m. balandžio 8 d. https://www.iris.report/p/trouble-in-cyberspace .

kibernetinę erdvę ir jai darytų įtaką; šios strategijos taikomos ne tik vidaus politikai, bet ir tarptautiniu mastu. Deibert ir Pauly pabrėžia, jog tiek Kinijos, tiek ir Rusijos interneto politikos strategijos apima veiksmus už nacionalinių ribų, įskaitant šnipinėjimo ir dezinformacijos kampanijas; taip pat įtakoja tarptautines organizacijas, užsienio valstybes ir netgi fizinius asmenis. Todėl formuojamas suverenus valstybių internetas yra kur kas platesnis geopolitinis tikslas, kuriuo siekiama įtvirtinti savo galią ir įtaką.[23] Verta pabrėžti, kad valstybės žino, jog ideologinė konkurencija dėl tinklo veikimo suteiks valstybėms autoritetą, padėsiantį globaliu mastu formuoti IT vartojimo ir valdymo standartus, tad jei Vakarai ir Rytai toliau nepasieks vienbalsio sutarimo, tikėtina, kad pasaulinis internetas skils į du skirtingus polius: JAV ir jų sąjungininkų bei vadovaujamą Kinijos, kuriame bus daugelis Azijos, Afrikos ir kai kurios P. Amerikos šalys, taipogi Rusija.[24] Taip pat, kaip jau minėjau anksčiau, viena iš grėsmių, kylančių dėl interneto susiskaldymo, yra žmogaus teisių skaitmeninėje aplinkoje užtikrinimas. Todėl atitinkamai galime formuluoti tyrimo **problemą:** kibernetinės erdvės valdymas skyla į daug segmentų, sudarydamas daugiapolį tinklą, kuriame dalyvauja: valstybė, IT privatus verslas, organizacijos ir interneto vartotojai, kurie vienaip ar kitaip prisideda prie interneto valdymo. Tuo tarpu autoritarinės valstybės, Rusija ir Kinija, daro įtaką tinklo susiskaldymui kurdamos valstybinę interneto suverenumo politiką, o tokia kampanija, šio darbo vertinimu, kelia dvejopą grėsmę demokratijos paradigmai: žmogaus teisėms ir žmogaus teisei į laisvą prieigą prie informacijos sklaidos interneto tinkle. Atsižvelgiant į tai, kyla tyrimo **klausimas**: kaip Kinija ir Rusija formuluoja kibernetinio suverenumo doktriną ir ją įgyvendina praktiškai santykyje su Vakaruose vyraujančiais žmogaus teisių principais internete? Siekiant atsakyti į klausimą, išsikelti šie darbo **uždaviniai**:

1. Aptarti teorinį pagrindą, kuris apimtų gilesnes kibernetinės erdvės problemas, tokias kaip žmogaus teisių įgyvendinimas KE kontekste.
2. Apibrėžti suverenios valstybės interneto sampratą;
3. Išsiaiškinti, koks yra žmogaus teisių vaidmuo internete;
4. Analizuojant raportus ir remiantis įstatymais, išsiaiškinti ir palyginti Kinijos ir Rusijos formuojamo suverenaus interneto strategijas ir įgyvendinimo principus.
5. Įvertinti strategijų įtaką žmogaus teisių principams internete.

Ginamieji teiginiai:

[23] Ronald J. Deibert ir Louis W. Pauly „Mutual Entanglement and Complex Sovereignty in Cyperspace“ kn. *Data Politics: Worlds, Subjects, Rights*, ed. Didier Bigo et al. (New York: Routledge, 2019), 95-86.
[24] Cornelia Bogen, „Overcoming Modernity? How China‘s Splinternet Reinforces the Impact of Geography in Global Internet Governance“ Navigationen - Zeitschrift für Medien- und Kulturwissenschaften 23, No.2 (2023): 130.

1. Kinijos ir Rusijos suverenus internetas yra doktrina, pagal kurią konstruojama kokybiškai nauja samprata apie žmogaus teises kibernetinėje erdvėje bendrai ir kiekvienam interneto vartotojui imtinai.
2. Kinija ir Rusija formuojant suverenų valstybių internetą siekia atskirties nuo Vakarų kibernetinės erdvės laisvo interneto ideologijos, kad galėtų laisvai vykdyti autoritariniam režimui palankią veiklą bei apsisaugoti nuo užsienio įtakos veiksnių.
3. Kinijos suverenaus interneto doktrinos pagrindinis tikslas yra vidinis – ekonominės ir socialinės valstybės santvarkos palaikymas, tuo tarpu Rusijos atveju vyrauja išorinė motyvacija – Vakarų kibernetinės erdvės geopolitinis skaldymas.

Literatūros analizė: Pirmoji autorių grupė tiria, kaip atrodo Kinijos ir Rusijos kontroliuojamas bei formuojamas suverenus valstybių internetas ir koks politinis modelis yra praktikuojamas KE valdyme. Lianrui tyrime nurodoma, kad Kinijos interneto valdymas literatūroje apibrėžiamas kaip nusistovėjęs modelis dėl centralizuoto interneto turinio kontroliavimo, tam tikra prasme kuriant holistinį interneto suverenumo požiūrį, kurio pagrindinis interesas yra vidinių technologijų ekonominis augimas. Visgi, Kinijos valdžios paradigmos veikimas neatitinka interneto valdymo modelio viešo pareiškimo todėl, kad interneto tinklo kontroliavimas nebėra tik valstybės elito rankose.[25] Todėl Kinijos interneto reguliavimo monopolis iš esmės tampa konstruktyvus diaugiapolis valdymo tinklas, kuriame prisijungia ekonomiškai stiprios IT vidinės technologijų gigantės, tokios kaip *Alibaba*, *Tencent* ir *Baidu*.[26] Kita vertus, pabrėžiama, kad valdžia interneto kontroliavime balansuoja tarp technologijų nacionalizmo stiprinant partijos kontrolę ir tuo pat metu bendradarbiaujant su užsienio kapitalo technologijų įmonėmis ir įtraukiant vis daugiau veikėjų į valdymo sistemos formavimą, kas lemia Kinijos interneto valdymo dinamiškumą ir prisitaikomumą.[27] Stadnik tyrime pabrėžiama, jog Rusija neapsiriboja noru tik reguliuoti ir kontroliuoti internetą, tačiau kelia dideles ambicijas sukurti atskirą, nacionalinį „*RuNet*“ interneto segmentą, nepriklausomą nuo tarptautinės kibernetinės erdvės, bet tuo pačiu išsaugantį tam tikrą ryšį su užsienio tinklais ir įpareigojantį tarptautinį IT verslą laikytis nacionalinių Rusijos reglamentų, nustatytų KE veikimui. Atsižvelgiant į Mueller teorinę KE derinimo prie nacionalinių sienų sistemą, Rusijos ambicijos interneto ribas apibrėžti ties Rusijos valstybe yra ganėtinai didelės. Kita vertus, nors ir imasi visų priemonių, visgi ne visos svarbiausios, pavyzdžiui, visiškas IT infrastruktūros priklausymas nuo nacionalinių technologijų ir standartų, sferos jau yra pritaikytos atsijungti nuo

[25] Jia Lianrui, „Building China‘s tech superpower: State, domestic champions and foreign capital“, kn. *Power and Authority in Internet Governance: Return of the State?* ed., Blayne Haggart, Natasha Tusikov ir Jan Aart Scholte (New York: Routledge), pilnas tekstas 126-147.
[26] *Ibid,* 127.
[27] *Ibid,* 146-147.

pasaulinio interneto tinklo. Tad visiškas Rusijos suverenaus interneto kūrimas vis dar yra procese, o daugialypis santykis tarp valdžios elito, komercinio IT verslo ir pilietinės visuomenės interneto valdyme ir asimetriškas.[28]

Antroji autorių grupė nagrinėja Kinijos ir Rusijos interneto valdymą geopolitikos ir tarptautinės arenos kontekste. Kinija ir Rusija formuoja tradicinį suverenumo naratyvą tarptautinėje KE arenoje, pagrįstą nesikišimo principu[29] ir nepriklausomą politiškai ir teisiškai be užsienio įtakos išlaikant valstybės nepriklausomybės legitimumą[3031] dėl to, kad abi vyriausybės internetą suvokią kaip didelę grėsmę režimo saugumui.[32] Kinijos interneto valdymas iš esmės yra nauja Šaltojo karo interneto versija prieš JAV „informacinį imperializmą", kuriuo, anot Kinijos, yra siekiama sugriauti kitas valstybes. Taigi, inicijuodama internetinio valdymo forumus, plačiai propaguodama sukurtos Didžiosios ugniasienės šakninių serverių veikimo principą[33], 2010 m. nukreipdama interneto veikimą per vidinius serverius ir sutrikdant milžinišką interneto srautą, Kinija parodo savo siekį tapti KE geopolitine galia pertvarkant KE valdymo struktūrą ir diskursą.[3435] Kinijos interneto valdymo paradoksas taip pat siejamas su istoriniu valstybės naratyvu ir interesu į ekonomiką ir jos augimą, todėl IT srityje internetu pasikliaunama kaip įrankiu, kuris nukreiptas į vidinius ir užsienio šalies interesus, t. y. „tinklinį autoritarizmą", kuomet partija naudoja IT, kad išplėstų savo kontrolę ir priežiūrą, kartu skatindama ekonomikos vystymąsi.[36] Nocetti pabrėžia, kad Kremlius kibernetinę erdvę tarptautiniuose santykiuose naudoja kaip tam tikrą įrankį, kuriuo siekia lyderystės kibernetinio valdymo institucijų narystėje skleidžiant tradicinio suverenumo tarptautiniuose santykiuose naratyvą; tai skaldo ir kelią įtampą užsienio politikoje. Tačiau Rusijos istorija turi sąsajų su nesaugumo jausmu, kuris susijęs su vidaus politikos konteksto naratyvu, todėl geopolitinis Rusijos KE tikslas yra

[28] Ilona Stadnik, „Russia: An Independent and sovereign internet?", kn. *Power and Authority in Internet Governance: Return of the State?* ed., Blayne Haggart, Natasha Tusikov ir Jan Aart Scholte (New York: Routledge), 186-205.
[29] Charles Grant, *Russiam China and Global Governence* (London, Centre of European Reform, 2012), i.
[30] Julien Nocetti, „Contest and conquest: Russia and global internet governance" *International Affairs* 91, No. 1 (2015): 112
[31] Milton L. Mueller, „China and Global Internet Governance", kn. *Access Contested: Security, Identity, and Resistance in Asian Cyberspace"* ed., Ronald John et al. (Cambridge: The Mit Press, 2012), 181.
[32] Justin Sherman, „Chinese and Russian Efforts to Undermine the Global Internet" *Fletcher Security Review,* (2023): 22.
[33] "Šakniniai serveriai yra hierarchinio rezoliucijos proceso, kuris užtikrina domenų vardai būtų globaliai unikalūs ir suderinti IP adresai domenų pradžios taškais. Dėl interneto kilmės JAV, šakniniai serveriai, beveik visi, įsikūrė JAV." Mueller, *China and Global Internet Governance*, 186.
[34] Jinghan Zeng, Tim Stevens ir Yaru Chen, „China's Solution to Global Vyber Governance: Unpacking the Domestic Discourse of „Internet Sovereignty"", *Politics & Policy,* 45, No.3 (2017): 434.
[35] Jessica Chen Weiss ir Jeremy L. Wallace, „Domestic Politics, China's Rise, and the Future of Liberal International Order"*International Organization* 75, (2021): 635-664.
[36] Mueller, *China and Global Internet Governance*, 177-192.

informacijos revoliucija, kuri susijusi su Kremliaus nusivylimu dėl Vašingtono vienašališko globalizmo interneto tinkle.[37]

Trečioji akademikų grupė nagrinėja Rusijos ir Kinijos interneto kontrolę žmogaus teisių kontekste. Teigiama, kad jeigu būtų vykdoma tai, kas aprašyta Rusijos „suverenaus interneto“ įstatyme, iš esmės pažeistų EŽTK principus. 2020 m. pagal konvenciją buvo užfiksuoti Rusijos pažeidimai dėl interneto turinio blokavimo ir socialinių medijų kontroliavimo. Tuomet EŽTK tiesiogiai nagrinėjo bylas, susijusias su žmogaus teisių pažeidimais kibernetinėje erdvėje, tačiau tai visiškai nesustabdė Rusijos suverenaus valstybės interneto vystymo, įgyvendinant atitinkamus įstatymus, paremtus kontrole ir griežtu valstybės reguliavimu, kurie tiesiogiai prieštarauja konvencijai. Tuo tarpu autoriai teigia, kad Rusijos sistemingai plėtojami įstatymai, ypač suverenus valstybės interneto įstatymas, kuris griežtina esamą interneto reguliavimo sistemą, tiesiogiai prieštarauja Rusijos įsipareigojimams EŽTK ir ES supratimui apie interneto suverenumą.[38][39] Autorius Jiang, nagrinėdamas žmogaus teisių problemą Kinijos interneto kontroliavime, problematiką pateikia kiek kitu kampu, aptardamas vidaus ir užsienio įmonių socialinį poveikį žmogaus teisėms Kinijoje bei populiariųjų kiniškų programėlių *Alibaba ir Wechat* veikimo principą užsienio teritorijose, nurodant, kad ir užsienio naudotojai kritikuoja pastarąsias dėl jautrių paskyrų, pranešimų stebėjimo ir turinio šalinimo. Dėl šių priežasčių teigiama, kad Kinijos ekonominė pažanga visiškai nekoreliuoja kartu su politine pažanga, būtent dėl žmogaus teisių, t. y. teisė į žodžio laisvę nėra Kinijos kibernetinės erdvės aspektas.[40] Zhen teigia, kad Kinijoje plačiai paplitusią cenzūrą, daugelis užsienio valstybių vertina kaip tam tikrą valstybės vidaus problemą, kuri pažeidžia teisę į žodžio laisvę. Visgi, tarptautiniai valdymo aparatai kišimąsi į Kinijos nacionalinius reikalus bandant kažką pakeisti vertina pesimistiškai.[41]

Darbo struktūra: Pirmoje dalyje pristatomos teorijos ir jų analizė KE atžvilgiu, taip pat aiškinamasi, kuri tarptautinių santykių teorija leidžia tyrinėti žmogaus teisių principus kinetinėje erdvėje. Antroje darbo dalyje pristatomas interneto susiskaldymo fenomenas, kurio pagrindu aiškinamasi suverenaus valstybės interneto samprata. Taip pat analizuojama, kokie yra žmogaus teisių principai KE, konkrečiai internete. Trečioje darbo dalyje atliekamas empirinis tyrimas lyginant

[37] Julien Nocetti, „Contest and conquest: Russia and global internet governance“ *International Affairs* 91, No. 1 (2015): 111-130.

[38] Erik Allerson, „International Censorhsip in Russia: The Sovereign Internet Laws and Russia‘s Obligations under the European Convention on Human Rights“, *Minnesota Journal of International Laws* 31, No.1 (Pavasaris 2022): 233-258.

[39] Anna Litvinenko, „Re-Defining Borders Online: Russia‘s Strategic Narrative on Internet Sovereignty“, *Media and Communications* 9, No. 4 (2021): 5-15.

[40] Min Jiang, „Chinese Internet Business and Human Rights, *Business and Human Rights Journal* 1 (2015): 139-144.

[41] Simon K. Zhen, „Combating Censorship in China: Forcing China‘s Hand through the WTO and Collective Action:, *Cornell International Law Journal* 53, No. 4 (žiema 202): 731-798.

Kinijos ir Rusijos suverenaus valstybės interneto įgyvendinimo principus, KE įstatymus ir kaip tai atliepia žmogaus teises internete.

1. Teorinis pagrindas

Remiantis akademiniais šaltiniais ir jau atliktais tyrimais, šiame skyriuje aptariamos pagrindinės teorinės prielaidos, nagrinėjančios KE dinamišką padėtį ir jos analizės perspektyvas tarptautinių santykių kontekste. Siekiama suformuluoti teorinį pagrindą, nukreiptą į Rusijos ir Kinijos kuriamą suverenų valstybių internetą ir šios politikos poveikį žmogaus teisių principų laikymuisi skaitmeninėje aplinkoje.

Daugybė mokslinių šaltinių per įvairias perspektyvas – tokias kaip realizmo, institucializmo ir konstruktyvizmo tarptautinių santykių teorijas – nagrinėja skaitmeninę aplinką ir kibernetinį saugumą imtinai. Vis dėlto, kaip teigia Choucri „*kibernetinė erdvė sukūrė naujas sąlygas, kurioms nėra aiškaus precedento.*“[42], todėl klasikinės teorijos galimai nėra pakankamai įgalios tiksliai išaiškinti valstybių elgesio dėl KE valdymo unikalumo, taip pat šią sąlygą apsunkina faktas, kad kibernetinėje erdvėje dalyvauja ne vienas subjektas. Šios erdvės procesų kūrime, formavime, valdyme ir kontroliavime iš esmės dalyvauja daugybė polių – nuo valstybės, sprendimų priėmėjų iki privataus verslo ir eilinio interneto vartotojo. Siekiant atrasti tinkamiausią teoriją, būtina apžvelgti esminių teorijų pritaikomumą nagrinėjant skaitmeninę aplinką.

1.1. Realizmo, konstruktyvizmo ir tarptautinio režimo perspektyva

Remiantis Choucri, tarptautinių santykių realizmo teorijos esminis objektas valstybių elgsenoje yra galia ir konfliktai, o KE iš esmės suteikia prieigą ne tik valstybėms, bet, globaliu mastu, visiems interneto naudotojams, todėl šiai teorijai trūksta nuoseklaus paaiškinimo dėl valstybės veikimo skaitmeninėje aplinkoje. Tuo tarpu institucionalizmo trūkumas yra tame, kad į KE valdymą dideliu mastu prisijungia privatus verslas, o konstruktyvizmas, nors ir pabrėžia subjektyvumą, taip pat kelią tam tikrą neaiškumą sprendžiant KE iššūkius. [43] Tuo tarpu Isnarti pabrėžia, jog konstruktyvizmo teorijai svarbūs akcentai yra valstybės identitetas, kultūra ir normos, lemiančios tai, kaip valstybės ir atitinkami veikėjai elgiasi tarptautiniuose santykiuose. Todėl, anot konstruktyvistų, technologinės pažangos, sukūrusios kibernetinę erdvę, tarsi sukūrė savotišką aplinką, kurioje galima grasinti žmogiškuoju ir nacionaliniu lygmenimis. Savo ruožtu, konstruktyvizmas padeda suprasti, kaip valstybės suvokia kitų šalių interesus ir tapatybes KE atžvilgiu, kadangi kibernetinis karas yra įtakojamas konstrukcijos iš valstybės suvokimo ir tapatybės tarptautiniuose santykiuose.[44] Autorių teigimu, nagrinėjant kibernetinį saugumą, konstruktyvizmo teorija iš esmės gali padėti suvokti, kaip valstybės per kitų šalių interesus ir tapatybes traktuoja kibernetinę erdvę ir pagal tai priima tam tikrus

[42] Nazli Choucri, *Cyberpolitics in International Relations* (Lodong: The MIT Press, 2012),13.
[43] *Ibid*, 14-15.
[44] Rika Isnarti, „A Comparison of Neorealism, Liberalism, and Constructivism in Analysing Cyber War“ *Andalas Journal of International Studies* 5, No. 2, (2016): 159-161.

sprendimus, lemiančius valstybės elgesį. Kita vertus, KE tarptautiniuose santykiuose yra pakankamai nauja sfera, ypač žinant, kad skaitmeninės aplinkos valdymo veikėjai yra ne tik valstybės subjektai. Galime padaryti išvadą, jog valstybės interesai ir identitetas nėra vien tik tai, kas gali padėti išsiaiškinti valstybės elgesį ir sprendimų priėmimą interneto valdymo kontekste.

„*Vyraujančią liberalią sferą stipriai propaguoja Vakarų valstybės, tačiau jai vis labiau meta iššūkį ryžtingai nusiteikusi suverenistinė sfera, kuriai vadovauja Kinija ir Rusija bei daugelis autoritarinių ir besivystančių šalių.*“[45] Kaip teigia Alperovitch, pastarosios autoritarinės valstybės siekia išlaikyti savo didžiosios galios statusą stiprindamos pozicijas nacionalinėse valstybės ribose, tokiu būdu bandydamos sumenkinti JAV ir jų sąjungininkių reputaciją žlugdant tarptautines ambicijas.[46] Pasaulinis interneto valdymas tapo JAV ir Kinijos technologinė ir ideologinė konkurencija tarp dviejų skirtingų politinių sistemų, tačiau verta pabrėžti, kad sėkmingiausia politinė sistema nustatys KE naudojimo standartus naujajame amžiuje.[47] Tad Kinija sąmoningai imasi interneto susiskaldymo tarptautinėje arenoje vaidmens, ekonomiškai besivystančiose šalyse propaguodama cenzūrą ir stebėjimu paremtą interneto veikimo principą, kuris prieštarauja politinės opozicijos principams.[48] 2015 m. tarp Kremliaus ir Xi pasirašytas dvišalis susitarimas dėl bendradarbiavimo tarptautinio informacinio saugumo srityje iš esmės atspindi šalių bendrą požiūrį į KE valdymą ir saugumą, kuris yra skirtingas nuo Vakarų. Susitarimas apibrėžia platų kibernetinių grėsmių spektrą ir ragina kurti daugiašalį, demokratišką ir skaidrų interneto valdymo modelį, suteikiant valstybėms didesnį įsitraukimą šiame procese.[49] Atsižvelgiant į konstruktyvizmo teorijos sampratą, Rusija ir Kinija kuria vienodą suvokimą ir tarsi tapatybę tarptautiniuose santykiuose KE požiūrio kontekste bei formuojant suverenų valstybių internetą, kuris ne tik įtvirtina nacionalistinę galią, bet apima ir užsienio politikos strategiją ieškant sąjungininkių ekonomiškai besivystančiose šalyse.

Kita vertus, Nye teigia, kad konstruktyvistų teorijų rinkinys remiasi į pažintinį veiksnį, kuomet tam tikros grupės ir socialiniai judėjimai keičiasi pagal intereso suvokimą, todėl tai neteisingai apibūdina valstybę kaip subjektą, kuris vadovaujasi nacionaliniais interesais. Todėl svarbus klausimas valstybių elgsenoje dėl kibernetinės srities – kaip tie interesai suvokiami ir įgyvendinami,

---

[45] Danielle Flonk, Markus Jachtenfuchs ir Anke S. Obendiek, „Authority conflicts in internet governance: Liberals vs. Sovereigntists“ *Cambridge University Press* 9, No.2, (2020): 365.

[46] Dmitri Alperovitch, „The Case for Cyber-Realism: Geopolitical Problems Don‘t Have Technical Solutions“ *Foreign Affairs* 101, No.1, (2022): 48.

[47] Bogen, *Overcoming Modernity?*, 130.

[48] Dakota Cary, „Community watch: China‘s vision for the future of the internet“, Atlantic Council, žiūrėta 2024 m. kovo 4 d., https://www.atlanticcouncil.org/in-depth-research-reports/report/community-watch-chinas-vision-for-the-future-of-the-internet/ .

[49] Elaine Korzak, „Have Russia and China Signed a Cyber Nonaggression Pact“, The Diplomat, žiūrėta 2024 m. kovo 4 d., https://thediplomat.com/2015/08/have-russia-and-china-signed-a-cyber-nonaggression-pact/ .

kuomet KE ir IT yra dinamiškai besivystančios, o valstybės vis dar stengiasi suprasti ir apibrėžti savo interesus.[50] Atsižvelgiant į tai, jog KE yra modernus ir inovatyvus galių mūšio laukas, kuriame interneto valdymo ir veikimo įrankiai – itin dinamiški, tobulėjantys sparčiau nei valstybių priimami veiksmai, galima daryti prielaidą, jog valstybės nespėja suformuluoti tikslaus KE intereso, apart esamo KE identiteto išlaikymo. Turiu omenyje tai, kad JAV toliau laikosi laisvo ir decentralizuoto interneto valdymo identiteto, tuo tarpu autoritarinės valstybės, ypač Kinija, formuoja globalų, interneto kontroliavimu pagrįstą identitetą, prie kurios prisijungia Rusija, o jų tikslas – kurti tarpvalstybinius santykius būtent tokio interneto veikimo principų kontekste.

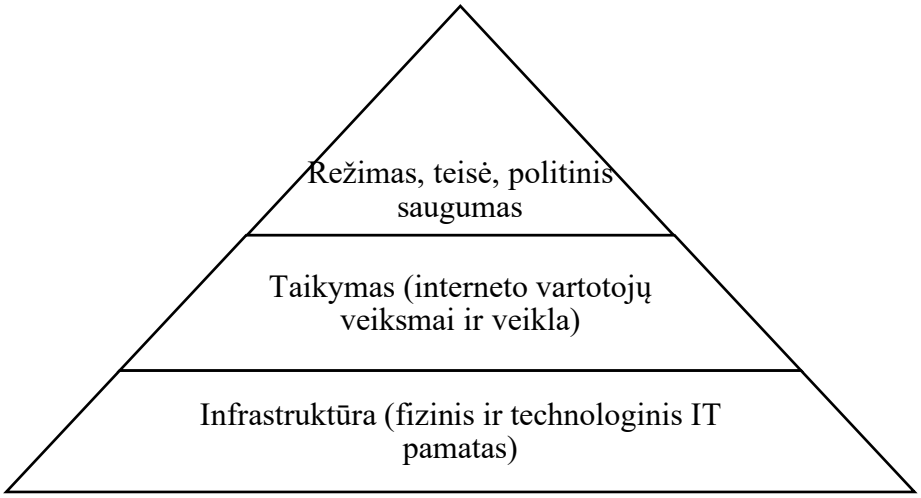
KE, nors ir kelia interneto susiskaldymo fenomeną, visgi iki šiol tebėra bendra, nepaisant to, kad apima platų spektrą skirtingų valstybių požiūrių ir valdymų. Įjos veikimo ir valdymo principą įeina daugybė skirtingų ir dinamiškų segmentų, kurie, savo ruožtu, kuria savotišką valdymo režimą. Nye interneto valdymą apibūdina kaip KE centrą,[51] nurodant valdymo struktūrą ir režimų kompleksiškumą dėl to, jog KE neturi vieno, tarptautiniu mastu priimto valdymo režimo. Veikiau interneto valdymą sudaro skirtingi fragmentai, įskaitant formalias ir neformalias normas ir institucijų, organizacijų rinkinius, kurie nustato reguliavimą per hierarchines struktūras. Nye režimo kompleksiškumo apipavidalinimas parodo platesnį diapazoną KE valdyme esančių subjektų, t. y.

1. Veikėjų ir su valdymu susijusių veiklų mastą bei veikimo principo dydį;
2. Atskiria problemas nuo techninės ryšio funkcijos ir daug platesnio režimo kompleksiškumo;
3. Parodo KE sudėtingas valdymo sritis, tuo pačiu atskleidžiant daug gilesnes problemas, tokias kaip žmogaus teisių atitinkamumas.[52]

Galima teigti, kad nors konstruktyvizmo teorija gali suteikti įžvalgų apie Rusijos ir Kinijos suverenaus interneto formavimo ypatumus per valstybės identitetą kaip socialinio modelio formavimą tarptautiniuose santykiuose, ši teorija vis dėlto neatrodo pakankamai tinkama atsižvelgiant į KE kintamumo greitį ir IT vystymąsi, kas savaime kinetinę erdvę paverčia inertiška. Nagrinėjant žmogaus teises Rusijos ir Kinijos suverenaus valstybių interneto kontekste, reikia kiek gilesnio metodologinio įrankio, kuris plačiame KE valdymo spektre iškelia ir papildo gilesnių problemų sąsają su valstybės elgesiu ir sprendimų priėmimais interneto valdymo klausimais. "*…režimo teorijos suteikia geresnių priemonių tiems pokyčiams suprasti nei pernelyg supaprastintos hegemoninio perėjimo teorijos*."[53] Atsižvelgiant į piliečio ir valstybės interesus, KE kvalifikacijos

[50] Joseph S. Nye, „The Regime Complex for Managing Global Cyber Activities" *Centre for International Governance Innovation and the Royal Institute for International Affairs* No.1 (2014): 11-12.
[51] *Ibid*, 2.
[52] *Ibid*, 5-7.
[53] *Ibid*, 15.

viršūnėje yra režimas, teisė, politinis saugumas, t. y. valstybės ideologija, kuri yra nepajudinama ir atspindi valstybės interesus interneto tinklo geopolitikos kontekste.[54]



1 lentelė. Sudarė autorė, pagal H.Yeli „A Three-Perspective Theory of Cyber Sovereignty“ lentelę (2017)

Šiame darbe siekiant giliau ištirti Rusijos ir Kinijos suverenaus valstybių interneto formavimo ir valdymo politiką kibernetinės erdvės geopolitikoje, taip pat interneto kontrolės ir žmogaus teisių sąveiką, kaip pagrindinis analizės įrankis pasirenkama režimo teorija.

1.2. Tarptautinių režimų ištakos ir samprata

Režimų teorija tarptautiniuose santykiuose atsirado reaguojant į Breton Vudso[55] sistemos žlugimą. Prognozuojant JAV hegemonijos pabaigą, kaip nurodė Keohane, tai galėjo turėti įtakos ekonominių režimų nuosmukiui.[56] Atitinkamai reaguojant į ekonominius pokyčius, tarptautinių režimų teorija atsirado nagrinėjant tarptautinę politinę ekonomiką. Pirmasis asmuo, kuris išplėtojo tarptautinių režimų teoriją, buvo tuomet jau buvęs realistas Krasner. 1983 m. atlikęs kolektyvinį tyrimų projektą apie pasaulio ekonomikos valdančiųjų institucijų santykius ir siekęs suprasti apie naujai pripažintų tarpvalstybinio bendradarbiavimo organų veiklą, Krasner tapo žinomas kaip režimo teorijos išvedėjas tarptautinių santykių srityje. Esė „Tarptautiniai režimai“ iki šiol yra svarbus įrankis, nagrinėjantis JAV sistemos valdymą.[57]

Tarptautiniai režimai yra svarbūs geopolitikos elementai, apimantys pakankamai platų spektrą sudedamųjų tarptautinių santykių srityje, įskaitant pagrindinius: nuomonę, principus, taisykles ir normas, sprendimų priėmėjų procedūrų rinkinius, kuriuose tarpusavyje sąveikauja veikėjų tarpusavio

[54] Hao Yeli, „A Three-Perspective Theory of Cyber Sovereignty“ *Institute for National Strategic Security, National Defence University* 7, No.2 (2017): 112-114.
[55] Po Antrojo pasaulinio karo įsigalėjusi tarptautinė monetarinė, fiksuotų valiutios kursų sistema
[56] Benjamin J. Cohen, *International Political Economy: An Intelectual History* (New Jersay: Princeton University Press, 2008), 68.
[57] *Ibid*, 96.

lūkesčiai. Verta pabrėžti, jog režimo valdomas elgesys – ilgalaikis, kadangi režimo principai ir funkcija yra grindžiami naudos siekimo principu, kuris skatina įsipareigojimą ir bendradarbiavimą. Kitaip sakant, pagrindinis režimo principas – abipusiškumas, t. y. valstybės ar kiti tarptautiniai veikėjai yra pasirengę paaukoti trumpalaikę intereso naudą tam, kad užtikrintų ilgalaikę tarpusavio naudą ir bendradarbiavimą siekiant, jog kiti tarptautinių santykių veikėjai priimtų tokį patį ar panašų sprendimą remiantis bendrai sutartomis taisyklėmis ir normomis.[58] Analizuodamas režimų teorijas, Krasner išskyrė pagrindines kategorijas, kurios lemia režimo atsiradimą atsižvelgiant į valstybių interesus: 1. Egoistiškumas ir savo interesų siekimas: režimo formavimas spontaniškai arba derybomis, kuriuose režimas formuojamas pagal nubrėžtus susitarimus, tačiau bet kokiu atveju su tikslu siekti savo interesų ir maksimizuoti naudą; 2. Politinės galios siekimas: režimas naudojamas kaip įrankis geopolitinei galiai įtvirtinti, tą galią suvokiant kaip tarptautinio gėrio užtikrinimą Galia taip pat naudojama kaip konkretus sistemos veikėjų vertybių padidinimas, apimanti skirtingų tikslų skatinimą, kuriuo siekiama individualios galios, kuri tarnauja konkretiems interesams; 3. Normų ir principų vienodumas: t. y. kuomet formuojančių režimą dalyvių interesai bei principai yra vienodi. 4. Naudojimas ir įprotis: iš esmės tai nėra traktuojamas kaip režimo atsiradimo kintamasis, veikiau jis papildo prieš tai jau minėtas priežastis.[59]

Young tarptautinius režimus apibūdina kaip specializuotus susitarimus, reguliuojančius konkrečias veiklas, išteklius arba priskirtas geografines sritis, apimančias tik specifinę tarptautinės arenos dalį. Režimo formavime ir vykdyme dalyvaujant formalioms valstybės institucijoms, privačioms organizacijoms ar kitiems neformaliems subjektams, iš esmės visi, nepriklausomai nuo priklausomybės viešajam ar privačiam sektoriui, privalo laikytis nustatytų režimo reglamentų, o sėkmingas režimo įgyvendinimas priklauso nuo kelių proceso etapų. Young pabrėžia, jog tai yra svarbus akcentas norint nagrinėti tarptautinių režimų veiksmus.[60] Kita vertus, režimas kuria tam tikrą tarpvalstybinę priklausomybę, dėl kurios valstybės tampa jautrios ir pažeidžiamos prieš išorės veiksmus, t. y. veikiančias jėgas, kurios kartais gali veikti prieš jų valią. Dėl šios priežasties, formuojant užsienio politiką tarptautinio režimo kontekste valstybė negali nepaisyti neformalių veikėjų ir nacionalinių politikos procesų bei sprendimų priėmėjų poveikio.[61]

---

[58] Stephen D. Krasner, „Structural causes and regime consequences: regimes as intervening variables: kn. *International regimes*, ed. Stephen D. Krasner (New York: Cornell University Press, 1983): 2-3.
[59] *Ibid*, 11-18 psl.
[60] Oran R. Young, *International Cooperation: Building Regimes for Natural Resources and the Environment* (New York: Cornell University Press (1989): 12-15.
[61] Hidetaka Yoshimatsu, „International Regimes, International Society, and Theoretical Relations“ *The International Centre for the Study of East Asian Development, Kitakyushu* 98, No.10 (1998): 12.

1.3. Tarptautinis režimas kibernetinės erdvės kontekste

Yoshimatsu teigia, kad valstybės, kurios išlaiko nepriklausomybę, įgauna įsipareigojimą atitinkamai išlaikyti ekonominę ir visuomenės sektoriaus kontrolę, tokiu būdu atsiribojant nuo išorės kontrolės. Tad, jeigu tarptautiniai režimai sustiprina valstybės kontrolę tarsi užkirsdami kelią užsienio įtakai, valstybės randa racionalų bendrą interesą ir sistemingai laikosi režimo principo.[62] Atitinkamai Rusija ir Kinija, formuodamos suverenų valstybių internetą, turi bendrą interesą – išlaikyti valstybės suverenitetą, išlaikyti partijos kontrolę nacionaliniu lygmeniu bei užkirsti kelią užsienio įtakai kibernetinėje erdvėje ir vidaus interneto veikimo principams. Kitaip sakant, Kremliaus ir Xi požiūris į skaitmeninę aplinką sutampa: dvišalis bendradarbiavimas ir interesas nukreiptas prieš Vakarų interesą, jis skatina valstybes imtis vienodų ar bent jau panašių interneto kontrolės principų ir laikytis dvišalio abipusiškumo, kas savaime suteikia valstybėms nacionalinį stuburą ir politinio režimo legitimumą ne tik vidaus politikoje, bet ir tarptautinėje arenoje. Galima teigti, kad dvišalis bendradarbiavimas formuojant KE režimo principą yra ne tik orientuotas į vidaus politiką, bet ir apima užsienio politiką įgalinant autoritarinio režimo ideologiją platesniu mastu, tokiu būdu užtikrinant Rytų hegemoniją interneto veikimo ir kontrolės kontekste.

Denardis teigia, jog klausimas „*kas turėtų valdyti internetą, Jungtinės Tautos ar bet kokia kita pavaldi organizacija iš esmės neturi jokios prasmės, veikiau reikia aiškintis kokia valdymo forma yra veiksmingiausia kiekviename konkrečiame kontekste.*“[63] Tuo tarpu Nye pabrėžia, jog KE valdymas yra labai sudėtingas, kadangi tarptautiniu atžvilgiu valstybės nesutaria dėl vieningos ir centralizuotos KE valdymo formos. Be visa to, KE valdymą sudaro daugybė atskirų normų, reglamentų, principų, kurie savo ruožtu formuojami skirtingų valstybių, institucijų ir organizacijų., Tai sudaro daugiapolį KE neapibrėžtumą valdymo klausimais, egzistuojantį tarpusavyje sąveikaujant decentralizuotiems režimams, kurie sudaro režimų kompleksiškumą.[64] Tuo tarpu Valeri interneto kontroliavime pabrėžia du pagrindinius veikėjus, t. y. valstybę ir privatų verslą, nurodant, jog tobulėjant informacinėms technologijoms ir internetui, atsiranda vis naujų interneto tinklo grėsmių, kurias valstybė yra neįgali išspręsti, todėl privataus verslo dalyvavimas formuojant KE režimo formavimą – būtinas.[65] Autorius taip pat pabrėžia, kad atvira architektūra, visuotine ir lanksčia prieiga paremtas Atvirasis ryšio infrastruktūros modelis yra būtinas norint užtikrinti tarptautinį informacijos režimą, o toks principų

[62] *Ibid.*

[63] Laura Denardis, *The Global War for Internet Governance* (New Haven and London: Yale University Press, 2014), 226.

[64] Nye, *The Regime Complex For Managing Global Cyber Activities*, 7-9.

[65] Ian Hosein ir Johan Eriksson, „International policy dynamics and the regulation of dataflows: bypassing domestic restrictions“ kn. *International Relations and Security in the Digital Age* sud. Johan Eriksson ir Giampriero Giacomello (New York: Routledge, 2007), 157.

derinys režimo formavime savaime skatina technologinę ir politinę sinergiją.[66] Kita vertus, formuojantis daugiapolei geopolitinei skaitmeninės aplinkos valdymo sistemai, galimybė užtikrinti laisvumu paremtą tarptautinį informacijos režimą tampa komplikuota, kadangi suverenaus valstybės interneto valdymo sistema neatitinka atviros prieigos principo.

Remiantis moksliniais šaltiniais nagrinėjančiais KE, galima įžvelgti, jog konstruktyvizmas, kaip teorija, gali padėti išaiškinti valstybių elgesį skaitmeninės erdvės valdymo kontekste. Tačiau teorija neapima gilesnio konteksto, tokio kaip žmogaus teisės. Tuo tarpu tarptautinio režimo teorija sudaro kur kas platesnį ir gilesnį diapazoną KE valdyme žmogaus teisių kontekste dėl to, jog teorija apima neformalius, bet valstybės politikoje dalyvaujančius subjektus bei pačią valstybę, kurie yra svarbūs dedamieji nagrinėjant valstybės KE valdymo principus tarptautinėje arenoje. Šiuo atveju, nagrinėjant Rusijos ir Kinijos suverenų valstybės internetą žmogaus teisių kontekste tarptautiniai režimai padeda suprasti, kokie yra valstybių lūkesčiai ir kokios yra dvišalės abipusiškumo normos atskleidžiant sudėtingas valdymo sritis, kurios atspindi gilesnes problemas, t. y. žmogaus teisių atitinkamumą.

2. Kibernetinės erdvės susiskaldymas ir žmogaus teisės

Antroje darbo dalyje siekiama ištyrinėti interneto susiskaldymo procesą ir aiškiai apibrėžti suverenaus interneto koncepciją. Be to, reikia išanalizuoti pagrindinius žmogaus teisių chartijos principus KE siekiant išryškinti esmines žmogaus teises interneto tinkle tam, kad būtų galima įvertinti ir atsakyti į iškeltą tyrimo klausimą.

2.1. Interneto susiskaldymas teorijoje

KE dabartinę situaciją apibūdinantis autorius siekia parodyti interneto inovatyvumą teigiant, jog dabartinė interneto stadija nuo laisvo ir nepriklausomo tinklo tapo dideliu geopolitikos iššūkiu. Formuojant tradicines valstybių sienas, buvusi vieninga ir anarchiška KE skyla, atitinkamai sudarant sąlygas valstybių interesų konfliktui.[67] Pasaulio ekonomikos forumo baltajame popieriuje interneto susiskaldymas įvardijamas kaip didelė geopolitikos problema, kurią skirtingos suinteresuotos šalys traktuoja ne vienodai:

1. Techninis susiskaldymas – interneto pagrindo, kaip techninių standartų nesuderinamumas, kuris užtikrina sklandų sistemos veikimą.

[66] Lorenzo Valeri, „Public-private cooperation and information accurance: a liberal institutionalist approach“kn. *International Relations and Security in the Digital Age* sud. Johan Eriksson ir Giampriero Giacomello (New York: Routledge, 2007), 137–142.
[67] Scott, *Splinternet: How Geopolitics and Commerce are Fragmenting the World Wide Web*, 108-140.

2. Vyriausybinis susiskaldymas – nacionalinė valstybių politika kontroliuojant arba reguliuojant interneto veikimo principą, apimant duomenų lokalizavimą, domenų blokavimą, cenzūravimą, kas savaime trikdo globalų duomenų srautą KE ir apriboja informacijos laisvę.

3. Komercinis susiskaldymas – skirtingi nacionaliniai teisės aktai, apimantys elektroninę prekybą ir duomenų srautus*[68] sukeliant papildomas finansines išlaidas ir iššūkius tarptautinių kompanijų veiklai.

4. Visuomenės perspektyva – prieigos prie informacijos izoliavimas, apribojant interneto vartotojo galimybes gauti, kurti ir platinti informaciją.[69] Interneto susiskaldymo problema tampa ne tik politinė, tačiau iš esmės apimanti ekonominę ir socialinę visuomenę, kurioje interneto fragmentacija kelia iššūkius ir apriboja interneto vartotojo laisvę į informaciją. Todėl teoriškai interneto susiskaldymas kelia interesų konfliktus ne tik tarp skirtingų politinių ideologijų, bet ir tarp verslo subjektų, IT užtikrinančių pamatinį interneto tinklo veikimą bei apskritai tarptautinės visuomenės, kuri skaitmeninėje aplinkoje vienaip ar kitaip kuria bendrą, multikultūriškumu paremtą aplinką.

Remiantis JT teigimu, interneto susiskaldymas kelia vis daugiau rizikų visuose lygmenyse, nes techninis susiskaldymas gali sugriauti dabartinį, saugų ir stabilų interneto tinklą, o tai turi didžiulį poveikį kibernetiniam saugumui. Tačiau valstybių siekimas suderinti techninius tarptautinius tinklo veikimo standartus ir protokolus ir bet kokie savavališki ir vienašaliai bandymai sugadinti pagrindinius interneto veikimo komponentus stiprina jau vyksiantį interneto susiskaldymą, kas savaime kelia pavojų tarptautiniam saugumui.[70]

Galima teigti, kad tarptautinėje arenoje valstybės brėžia griežtas nacionalines ribas, kurios apima skirtingus, nuo valstybės identiteto ir vertybių, apimančius reglamentus. Šie principai iš esmės apima visas KE dalyvaujančias kategorijas, kurios savo ruožtu vienaip ar kitaip yra susijusios su valstybės elgsena ir sprendimų priėmimais dėl interneto valdymo, tačiau dinamiška geopolitinė KE etika kelia pavojų tarptautiniam saugumui.

2.2. Interneto susiskaldymas praktikoje

Tam, kad geriau įvertintume ir apsibrėžtume suverenaus valstybės interneto koncepciją, reikia išsiaiškinti, kaip šiandien atrodo interneto skilimo fenomenas globaliu mastu. Tam, kad šis uždavinys būtų įvykdytas, išskyriau keletą, mano manymu, pagrindinių kategorijų, kuriose matomi ryškiausi

[68] Taip pat, pridėčiau skirtingas duomenų apsaugos supratimo ir reglamentų skirtumas.

[69] William J. Drake, Vinton G. Cerf ir Wolfgang Kleinwachter, „Future of the Internet Initiative White Paper: Internet Fragmentation: An Overview“, *World Economic Forum*, (2016): 7-8.

[70] Samuele Dominioni, „Internet Fragmentation and Cybersecurity“, The United Nations Institute for Disarmament Research, (2023): 12.

interneto susiskaldymo veiksniai, apimantys tarptautinę areną ir už kuriuos yra vienaip ar kitaip atsakingi valdžios sprendimų priėmėjai.

2.2.1. Duomenų saugumas

Dabartinis internetas yra vienašališkas monopolis JAV atžvilgiu, tuo tarpu kitos šalys yra tik interneto vartotojos.[71] Kita vertus, plėtojantis IT ir apimant vis platesnį spektrą duomenų ir informacijos KE, daugybė valstybių imasi priemonių tam, kad interneto tinklas būtų saugus ir, atsižvelgiant į valstybes vertybes, užtikrinantis interneto veikimo principus. Šiuo atveju, Rusija ir Iranas perkelia duomenų serverius į savo šalis, tuo tarpu Kinija, Vietnamas, Nigerija ir Pakistanas nustatė duomenų lokalizavimo reikalavimus.[72]

Pastarąjį dešimtmetį, IT privatūs verslai bei vyriausybės renkami asmeniniai duomenys internete sparčiai išaugo.[73] Atsižvelgiant į tai ES ir Kalifornija ėmėsi atitinkamų veiksmų, kurie užtikrintų piliečių saugumą ir apskritai informuotų interneto vartotojus apie asmeninių duomenų rinkimą, naudojimą ir laikymą. ES pasirašė „Bendrąjį duomenų apsaugos reglamentą“, kuris nuo 2018 m. įpareigoja, įskaitant ir trečiąsias šalis, renkant bet kokią informaciją apie ES piliečius, įskaitant ir fizinis asmenis, užtikrinti surinktų duomenų saugumą, atitinkamai juos tvarkyti bei pranešti, kodėl ir kokie privatūs duomenys yra renkami.[74] Vakaruose tais pačiais metais Kalifornija pristatė „Kalifornijos vartotojų privatumo įstatymą“, suteikiantį teisę matyti, kokia asmeninė informacija yra renkama, prašyti ją ištrinti, gauti prieigą prie informacijos apie duomenis renkančią įmonę arba kuriai duomenys buvo perteikti arba parduoti, ir įpareigojantį įmones neperduoti informacijos trečiosioms šalims.[75]

2021-iais m. Kinija paskelbė KLR duomenų saugumo įstatymą, kuris yra taikomas ne tik vidaus duomenų tvarkymui, bet ir apima ekstra teritorinį pasiekiamumą.[76] įstatymo 2-uoju straipsniu nurodoma, kad įstatymas taikomas duomenų tvarkymo veiklai ir saugumo taisyklėms vykdomoms šalies teritorijoje, tačiau už žemyninės Kinijos teritorijos vykdoma duomenų tvarkymo veikla, kuri kenkia Kinijos nacionaliniam saugumui, viešajam interesui arba piliečių ir organizacijų teisei ir

---

[71] Xui Li ir Xin Yang, Co-governed Sovereignty Network: Legal Basis and Its Prototype & Applications with MIN Architecture (Singapore: The Springer, 2021), XI.

[72] Article19, „Sovereign Internet Networks and Net Neutrality“, Article19, žiūrėta 2024 m. kovo 24 d. https://www.article19.org/reader/global-expression-report-2018-19/global-analysis/global-analysis-2/digital/sovereign-internet-networks-and-net-neutrality/ .

[73] Freedom Online Coalition, „Openess, Accessibility and Inclusion – Human Rights Online in the 2020“ (pranešimas konferencijoje Freedom Online: 2021: 10th Anniversary of the Freedom Online Coalition, Lapkričio 30 d. – Gruodžio 3 d., 2021) 10.

[74] Duomenų apsaugos tarnyba, „GDPR įstatymas Lietuvoje – kaip prisitaikyti organizacijoms?“, Duomenų apsaugos tarnyba, žiūrėta 2024 vasario 16 d. https://dat.lt .

[75] Issie Lapowsky, „California Unanimously Passes Historic Privacy Bill“, WIRED, žiūrėta 2024 m. vasario 27 d. https://www.wired.com/story/california-unanimously-passes-historic-privacy-bill/ .

[76] George Qi, „China Finalizes Data Security Law“, Greenberg Traurig, žiūrėta 2024 m. kovo 20 d. https://www.gtlaw.com/en/insights/2021/7/china-finalizes-data-security-law .

interesams, turi būti ginama pagal įstatyme nurodoma atsakomybę.[77] Tais pačiais metais Kinija taip pat išleido įstatymą, iš esmės lygiavertišką ES duomenų saugos įstatymui, ,,KLR asmens informacijos apsaugos įstatymas“[78], kurio esmė yra tokia pati, kaip ir BDAR. 2014m. Putinas pasirašė duomenų apsaugos įstatymą, kuris veikiau siejamas su duomenų lokalizacija, turint omenyje tai, kad šiuo įstatymu įpareigojama visas Rusijos ir užsienio bendroves, nepriklausomai iš kokios pasaulio vietos yra vykdoma veikla, turinčias bet kokius asmens duomenis apie Rusijos piliečius, saugoti šią informaciją būtent Rusijoje.[79]

Pasaulio duomenų apsaugos geopolitinę padėtį būtų galima suskirstyti:

Griežta duomenų apsauga	Tvirta duomenų apsauga	Vidutinė duomenų apsauga	Ribota duomenų apsauga
Kanada, JAV, Meksika, Europa, Kinija, Indija, Australija, Tanzanija ir t. t.	Argentina, Urugvajus, Japonija, Pietų Azijos valstybės ir t. t.	Rusija, daugelis pietų Afrikos valstybių, Brazilija ir kitos pietų Amerikos valstybės ir t. t.	Keletas Afrikos, pietų Amerikos, centrinės Azijos valstybių, Iranas.

2 lentelė. Sudarė autorė, remiantis https://www.dlapiperdataprotection.com žemėlapiu.

Galima teigti, kad JAV, Europa ir Kinija yra tarp regionų, kurie įgyvendina itin griežtus duomenų apsaugos įstatymus, didelį dėmesį skiriant tam, kad būtų užtikrintas asmeninių duomenų saugumas ir privatumas. Tuo tarpu kitos valstybės implementuoja apsaugos reglamentus, tačiau jie nėra tokie griežti. Kita vertus, tai parodo geopolitinį duomenų apsaugos reglamentų dinamiškumą ir skirtingus geopolitinius interesus KE kontekste, kuris prisideda prie interneto susiskaldymo veiksmo ir daugiapolinio valdymo.

2.2.2. Turinio filtravimas

Valstybės turi galios valdyti teritorinį interneto turinį,[80] kuris apima, bet neapsiriboja temomis apie valdžią, ypač opozicijos, arba kritiką, nukreiptą prieš dabartinę valstybės politiką, seksualumą, kultūrą ar religiją, jeigu valdžios elitas mano, kad tema yra pakankamai jautri. 2007 m. atliktas pirmasis tyrimas dėl interneto turinio filtravimo parodė, jog net 25 iš 41 šalių filtruoja turinį, susijusį

[77] People‘s Republic of China, *Data Security Law of the People‘s Republic of China*, China, žiūrėta 2024 m. kovo 31 d. http://www.bi168.cn/thread-37794-1-1.html .

[78] China Briefing, ,,The PRC Personal Information Protection Law (Final): A Full Translation, China Briefing, žiūrėta 2024 m. kovo 20 d. https://www.china-briefing.com/news/the-prc-personal-information-protection-law-final-a-full-translation/ .

[79] Justin Sherman, ,,Russia is weaponizing its data laws against foreign organizations“, The Brooking Institution, 2024 m. kovo 21 d. https://www.brookings.edu/articles/russia-is-weaponizing-its-data-laws-against-foreign-organizations/ .

[80] P. W. Singer ir Allan Friedman, *Cybersecurity and Cyberwar what Everyone needs to know* (New York: Oxford University Press, 2014), 176.

su prieš tai įvardintomis temomis. Tuo tarpu Iranas, Kinija ir Saudo Arabija ne tik cenzūruoja turinį, bet ir blokuoja didelį kiekį užsienio domenų, Pietų Korėja tikslingai filtruoja temą apie Šiaurės Korėją, o šalys, įvardintos kaip vykdančios esminį politiškai motyvuotą filtravimą, buvo Birma, Kinija, Iranas, Sirija, Tunisas ir Vietnamas.[81]

Naujausiame atliktame tyrime dėl turinio filtravimo nurodoma, jog Šiaurės Korėjos, Kinijos ir Irano piliečiai negali naudotis Vakarų socialine žiniasklaida, tuo tarpu esama žiniasklaida yra griežtai cenzūruojama ir kuriama pagal vyriausybės nurodymus. Taip pat šiose valstybėse blokuojamos pranešimų siuntimo programėlės iš užsienio, priverčiant gyventojus naudotis jau esamomis programėlėmis, tarkim Kinijoje „*WeChat*“,*[82] kurios galimai yra griežtai kontroliuojamos. Antroje vietoje pagal turinio filtravimą yra Irakas, Mianmaras, Pakistanas ir Turkmėnistanas čia informacijos srautas nėra visiškai uždraustas ar blokuojamas, trečioje vietoje – Rusija Saudo Arabija, JAE. Pastaraisiais metais Rusija užblokavo daugybę užsienio svetainių, socialinės žiniasklaidos kanalų ir susirašinėjimo programėlių, tačiau įdomus faktas yra tas, kad Rusijoje vyksta diskusijos, raginančios legalizuoti vakarietiškų filmų ir TV laidų piratavimą. Taip pat nurodoma, kad, lyginant su praėjusiais metais, šalių, filtruojančių turinį, atsirado kur kas daugiau, t. y. šįmet nustatyta 50, tuo tarpu praėjusiais metais buvo 27 valstybės. Tyrime buvo nagrinėjami apribojimai, susiję su socialine ir politine žiniasklaida / programėlėmis ir pornografija.[83]

Atsižvelgus į šiuos tyrimus, matomas vis didesnis valstybių, kontroliuojančių interneto turinį, įsitraukimas. Tačiau galima teigti, kad šalių turinio filtravimas daugiausiai susijęs su politiškai jautriomis temomis, todėl valstybės, siekdamos išsaugoti ar sustiprinti savo politinę valdžią, linkusios filtruoti ir cenzūruoti turinį, kuris gali pakenkti politikos įvaizdžiui ar netgi kelti grėsmę valstybės legitimumui.

2.2.3. Socialinių tinklų politika

Morozov yra gerai žinomas kaip laisvo interneto skeptikas ir plačiai kvestionuojantis KE ir IT geopolitinius principus, įskaitant privataus IT verslo veiklą. Remiantis Morozov, tiek autoritarinės, tiek ir demokratinės valstybės, KE siekia „informacinio suvereniteto“ nuo JAV IT kompanijų, kurios turi artimą ryšį su JAV vyriausybe. Šiuo atveju strategine interneto pramonės šaka laikoma: interneto paieškos domenai, socialiniai tinklai ir netgi elektroninis paštas, todėl užsienio valstybės, siekdamos

[81] Harvard University, „Survey of Government Internet Filtering Practices Indicates Increasing Internet Censorship“, Berkman Klein Center For Internet & Society at Harvard University, žiūrėta 2024 m. kovo 22 d. https://cyber.harvard.edu/newsroom/first_global_filtering_survey_released .

[82] „WeChat“ yra „Weixin“atitikmuo, tačiau svarbu pabrėžti skirtumus: „WeChat“ skirtas visiems vartotojams už žemyninės Kinijos teritorijos, o „Weixin“ skirtas žemyninės Kinijos Liaudies Respublikos vartotojams. Technologiškai jie neturėtų priklausyti bendrai technologinei sistemai ir serveriams.

[83] Paul Bischoff, „Internet Censorship 2024: A Global Map of Internet Restrictions“, Comparitech, žiūrėta 2024 m. kovo 22 d. https://www.comparitech.com/blog/vpn-privacy/internet-censorship-map/ .

apsaugoti internetą nuo užsienio kontrolės, kuria vietinę alternatyvą. Teigiama, jog Iranas svarsto uždrausti „*Gmail*“ bei sukūrė vietinę socialinio tinklo „*Facebook*“ alternatyvą. Tuo tarpu Turkija, esanti artima JAV sąjungininkė, planuoja kiekvienam valstybės piliečiui suteikti vyriausybės valdomą elektroninio pašto adresą tam, kad sumažintų priklausomybę nuo JAV IT paslaugų tiekėjų.[84]

Iš esmės geopolitinis IT karas tampa vis ryškesnis, ypatingai tarp Kinijos ir JAV, kuomet valstybės varžo ar/ ir blokuoja IT ryšio segmentus, kontroliuodamos informacijos suverenumą, arba, kaip Kinija, formuodama suverenų valstybių internetą. Šiuo atveju JAV imasi griežto naratyvo dėl Kinijos įmonės „*ByteDance*“ valdomos programėlės „*TikTok*“ nurodydama, jog nepardavus jos kitam valdytojui, JAV užblokuos platformą.[85] Tuo tarpu Kinijoje per pastarąjį dešimtmetį buvo užblokuoti bene populiariausi Vakarų socialiniai tinklai, tokie kaip „*Facebook*“, „*Twitter*“ ir „*Instagram*“, įskaitant daugianacionalinę paieškos sistemą „*Google*“.[86] Kinijoje blokuojami kone visi Vakaruose paplitę ir populiarūs socialiniai tinklai ar susirašinėjimo programėlės dėl įvairių politinių, socialinių, kultūrinių ir ekonominių priežasčių. KKP naudoja griežtą cenzūrą dėl to, kad išlaikytų kontrolę, ir bet kokį turinį, susijusį su keliama grėsme – blokuoja. Politinės perspektyvos atžvilgiu, nurodoma, jog turinys, kuris kritikuoja vyriausybę ar skatina demokratiją ir žmogaus teises, arba kuriame kalbama partijai jautriu naratyvu, t. y. Tiananmeno aikštės protestai, Tibeto ir Xinjiang regionų problematika, yra griežtai nepageidaujamas Kinijos KE. Socialinių ir ekonomikos aspektų atžvilgiu, socialinių tinklų cenzūravimu Kinijoje siekiama socialinio stabilumo, palaikant tradicines vertybes, todėl temos apie LGBT nėra leidžiamos, o ekonominiu aspektu, blokuodama užsienio svetaines ir programėles, Kinija tiesiog skatina vietinių IT įmonių populiarumą.[87]

Rusijos socialinių tinklų blokavimas ir cenzūravimas maksimizavosi Rusijos invazijos Ukrainoje metu. Daugelis prieš tai jau minėtų, Vakaruose populiariausių socialinės medijos platformų Rusijoje buvo užblokuotos, bet populiariausia video platforma „*Youtube*“ ir susirašinėjimų programėlė „*Telegram*“ kol kas neužblokuotos.[88] Iš esmės Rusijoje nuo 2022 m. sausio mėn. iki 2023

---

[84] Evgeny Morozov, „Freedom.gov: Why Washington‘s support for online democracy is the worst thing ever to happen to the Internet“, Foreign Policy, žiūrėta 2024 m. kovo 23 d.https://web.archive.org/web/20110913073036/http://www.foreignpolicy.com/articles/2011/01/02/freedomgov?page=0,1 .

[85] Lietuvos nacionalinis radijas ir televizija, „JAV siekia uždrausti „TikTok“: kaip tai atsilieps Europai?“„ LRT, žiūrėta 2024 m. kovo 23 d. https://www.lrt.lt/naujienos/mokslas-ir-it/11/2225454/jav-siekiama-uzdrausti-tiktok-kaip-tai-atsilieps-europai .

[86] Li Yuan, „A Generation Grows up in China Without Google, Facebook or Twitter“, The New York Times, žiūrėta 2024 m. kovo 26 d. https://ir.westcliff.edu/wp-content/uploads/2018/08/A-Generation-Grows-Up-in-China-Without-Google-Facebook-or-Twitter.pdf .

[87] Rob Binns, „Websites banned in China: Access, alternatives and unblocked sites“, Independent Advisor, žiūrėta 2024 m. kovo 26 d. https://www.independent.co.uk/advisor/vpn/websites-banned-in-china .

[88] Robert McMahon, „Russia is Censoring News on the War in Ukraine. Foreign Media Are Trying to Around That“, The Council on Foreign Relations, žiūrėta 2024 m. kovo 26 d. https://www.cfr.org/in-brief/russia-censoring-news-war-ukraine-foreign-media-are-trying-get-around .

m. vasario mėn. užblokuoti 494 domenai, į kuriuos patenka tarptautinės žmogaus teisių svetainės, Rusijos žmogaus teisių tinklalapiai ir nepriklausomų naujienų žiniasklaidos svetainės.[89]

2.2.4. Interneto teisių suvaržymas

Interneto valdyme valstybės galia iš esmės yra teritoriškai susieta, o efektyviausiai veikia per fizinę interneto valdymo pusę, t. y. vyriausybės gali panaudoti savo galią per fizinį turtą, kurį galima konfiskuoti, biurus, kuriuos galima uždaryti, ir asmenis, kuriuos galima persekioti ar net įkalinti, jei jie nepaklus interneto kontroliavimo reglamentams. Šiuo atveju geriausias to pavyzdys yra interneto paieškos įmonės, kurios sutiko su Kinijos partijos nurodymu pašalinti visas nuorodas į 1989 m. vykusius protestus Tianmen aikštėje tam, kad galėtų išlaikyti verslą Kinijoje. [90]

JT žmogaus teisių ataskaita nurodo, kad kibernetinėje erdvėje vis daugėja žmogaus teisių pažeidimų dėl teisės į žodžio laisvę. Tai pasireiškia per valstybių galią nutraukti internetą, kas daro didelę žalą kasdieniam žmonių gyvenimui. Tai dažniausiai įgyvendinama protestų, didėjančios politinės įtampos, įskaitant politinių rinkimų metu, kas savaime laikoma demokratijos paradigmos katastrofa. 2021 m. atliktas tyrimas parodė, kad internetas buvo nutrauktas Čade, Kongo Respublikoje, Irane, Nigeryje, Ugandoje ir Zambijoje, ekspertams pažymint, jog tokia veika dažniausiai siejama su bandymu nuslėpti sunkius žmogaus teisių pažeidimus. Mianmare interneto prieiga buvo nutraukta per karinį perversmą, siekiant sukurti „skaitmeninę diktatūrą“, o tai turėjo didelį poveikį žmogaus teisėms, įskaitant teisę į saugumą, sveikatą, švietimą, maistą, pastogę, išgyvenimą ir žodžio laisvę.[91]

Turkijos interneto įstatymo pakeitimai ir Turkijos interneto reguliavimo institucijos sprendimai sustiprino šalyje vykstančią žmogaus teisių ribojimo tendenciją, kadangi vyriausybei buvo suteikta *carte blanche*, t. y. visiška veiksmų laisvė neribotai prieigai prie ryšio duomenų be teismo sprendimo. Taip pat vyriausybė įkalino politinius oponentus dėl siekiamybės slopinti pliuralizmą ir apriboti politinių diskusijų laisvę KE.[92] 2019-2020 m. per vykusius Honkongo protestus prieš vyriausybės pateiktą įstatymo projektą, miesto pareigūnai svarstė galimybę dalinai ar netgi visiškai blokuoti

[89] Roskomvsoboda, „How Internet censorship changed in Russia during the 1st year of military conflict in Ukraine“, Open Observatory of Network Interference, žiūrėta 2024 m. kovo 27 d. https://ooni.org/post/2023-russia-a-year-after-the-conflict/ .

[90] Singer Friedman, *Cybersecurity and Cyberwar what Everyone needs to know*, 176.

[91] United Nations, „Activists: Internet shutdowns violate human rights“, United Nations, žiūrėta 2024 m. kovo 26 d. https://www.ohchr.org/en/stories/2022/08/activists-internet-shutdowns-violate-human-rights .

[92] Katitza Rodriguez ir Hilal Temel, „Turkey Doubles Down on Violations of Digital Privacy and Free Expression, „Electronic Frontier Foundation, žiūrėta 2024 m. kovo 28 d. https://www.eff.org/deeplinks/2020/11/turkey-doubles-down-violations-digital-privacy-and-free-expression .

internetą tam, kad protestuotojai negalėtų naudotis svarbiais, internetu plintančiais organizaciniais įrankiais.[93]

Interneto teisių suvaržymai vis dažniau pasitaiko įvairiose šalyse, jie tiesiogiai pažeidžia žmogaus teises, ypač žodžio ir informacijos laisvę, bet ir atspindi valdžios galios ir naudos siekimą. Suvaržymai ne tik riboja piliečių teises, bet skatina interneto susiskaldymą, sukurdami daugiapoles kibernetines erdves, aptvertas valstybių sienomis, kuriose skirtingos taisyklės taikomos vyriausybėms, tarptautinio verslo subjektams ir visuomenei, kuri naudojasi internetu. Tai iš esmės keičia interneto , kaip atviros, multikultūrinės platformos prigimtį ir paradigmą.

2.3. Suverenaus valstybių interneto samprata

„*Kurdamos ir plėsdamos tam tikrus tinklus, vyriausybės itin sumaniai formuoja kibernetinės erdvės formą ir pobūdį, siekdamos strateginių ar politinių tikslų.*[94] Atitinkamai, galima teigti, kad valstybės formuoja KE veiklą pagal savo interesus. Tačiau čia yra būtina išskirti interneto suvereniteto sampratą.

Kibernetinėje erdvėje vyrauja dvi suvereniteto formos, t. y. duomenų suverenitetas – tokie duomenys, kaip intelektinė nuosavybė, finansinė ar asmeninė informacija turi būti reglamentuojama pagal tos geografinės vietovės galiojančią teisinę sistemą, įskaitant tai, jog informacija turi būti tvarkoma pagal tos vietovės įstatymus, iš kurios informacija atkeliauja.[95] Tuo tarpu skaitmeninio suvereniteto sąvoką pirmą kartą paminėjo Xi 2015 m. vykusioje pasaulinėje interneto konferencijoje: „*Pagarba kibernetiniam suverenitetui. Suverenios lygybės principas, įtvirtintas JT Chartijos, yra viena iš pagrindinių šiuolaikinių tarptautinių santykių normų. Ji apima visus valstybių santykių aspektus, įskaitant kibernetinę erdvę*.“[96] Segal teigia, kad Kinija tiesiogiai propaguoja kibernetinį suverenitetą, kaip tam tikrą interneto valdymo principą, oponuojantį JAV skatinamą tarptautinį atvirumu ir saugumu pagrįstą internetą.[97] Todėl interneto suvereniteto sąvoka istoriškai siejama su nedemokratinėmis valstybėmis, kurios tai naudoja kaip tam tikrą įrankį ne tik prieš demokratinę JAV interneto ideologiją, bet ir tam, kad pagrįstų decentralizuotą skaitmeninės aplinkos valdymo procesą, kuriame dalyvauja daug suinteresuotų šalių.[98] Nors ir daugelyje valstybių galima

---

[93] James Griffiths, „Blocking social media would be ‚the end of the open internet of Hong Kong‘. It also wouldn‘t work“, CNN, žiūrėta 2024 m. kovo 28 d. https://edition.cnn.com/2019/08/29/tech/hong-kong-internet-block-emergency-powers-intl-hnk/index.html .

[94] Mainwaring, *Always in control?*, 8.

[95] Cloudfare, „What is data sovereignty“, Cloudfare, žiūrėta 2024 m. kovo 29 d. https://www.cloudflare.com/en-gb/learning/privacy/what-is-data-sovereignty/ .

[96] Xi Jinping, *Remarks by H.E. Xi Jinping President of the People's Republic of China At the Opening Ceremony of the Secong World Internet Conference*(Wuzhen, 2015 m. gruodžio 16 d.) 2.

[97] Adam Segal, „China‘s Alternative Cyber Governance Regime, *Council on Foreign Relations* (2020): 3.

[98] Internet Society, „Navigating Digital Sovereignty and Its Impact on the Internet:, Internet Society, (2022): 5.

įžvelgti suverenaus interneto koncepcijos pritaikymą interneto valdymo procesuose, visgi teigiama, jog nėra vieno naratyvo, kuris galėtų apibūdinti geopolitinę suvereniteto politiką KE.[99]

Atsižvelgiant į tyrimą, suverenų valstybių internetą galime apibrėžti kaip skirtingų valstybių skirtingą interneto valdymą, kuris neturi vieno bendro naratyvo, kaip valstybės formuoja suverenumą KE. Tačiau ryškiausi interneto suverenumo formavimo principai įžvelgiami Kinijoje, iš kurios šis naratyvas ir kilo. Tuo tarpu Rusijos suverenus valstybės internetas aiškiai apibrėžiamas noru visiškai atsiriboti nuo Vakarų skaitmeninės aplinkos, tačiau matome, kad tam tikrų socialinių medijų , kaip ,,*Youtube*“, išlaikymas, visgi nėra visiškas Rusijos atsiribojimas nuo tarptautinės KE. Todėl galima teigti, kad sąvoka ,,suverenus valstybės internetas” yra labai dinamiška ir gali būti traktuojama skirtingai, atsižvelgiant į konkrečios valstybės sprendimų priėmimą ir elgesį interneto valdymo kontekste.

2.4. Žmogaus teisės

1948 m. JT žmogaus teisių chartija priėmė pirmąjį universalų visuotinį žmogaus teisių deklaracijos dokumentą, kuris įtvirtina ir bendrai apibūdina žmogaus teises.[100] JT žmogaus teisių komiteto generalinio komentaro Nr. 34, 19 straipsnyje teigiama, kad valstybės turi garantuoti teisę į saviraiškos laisvę, įskaitant teisę ieškoti, gauti ir skleisti visų rūšių informaciją ir idėjas, nepaisant sienų

, taip pat saugoti visas išraiškos formas ir jų sklaidos priemones, įskaitant elektronines ir internetines.[101] Kita vertus, tame pačiame straipsnyje pabrėžiamos specialios pareigos ir atsakomybė, kurios yra numatytos įstatyme: a) pagarba kitų teisėms ar reputacijai; b) nacionalinio saugumo arba viešosios tvarkos *ordre public,* arba visuomenės sveikatos ar moralės apsauga. Todėl tai nurodo, kad teisė į informaciją turi būti suderinta su kitomis žmogaus teisėmis, įskaitant ir žmogaus teisių apsaugą internete.[102] Verta pabrėžti, jog kibernetinis saugumas laikomas viena iš pagrindinių žmogaus teisių problemų, kadangi pastaruoju metu užfiksuojama vis daugiau pažeidimų per informacines technologijas dėl kibernetinio saugumo trūkumo.[103]

---

[99] *Ibid*

[100] Rima Varnienė, ,,Visuotinė žmogaus teisių deklaracija“, Visuotinė Lietuvių Enciklopedija, žiūrėta 2024 m. kovo 31 d. https://www.vle.lt/straipsnis/visuotine-zmogaus-teisiu-deklaracija/ .

[101] United Nations, *United Nations International Covenant on Civil and Political Rights, General comment No.34: Article 19: Freedoms of opinion and expression*, Geneva, 11-29 July, 2011, https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf (žiūrėta 2024 m. kovo 31 d.).

[102] Australian Human Rights Commission, ,,Background paper: Human rights in cyberspace“, Australian Human Rights Commission, (2013): 3.

[103] Deborah Brown, ,,It‘s Time to Treat Cybersecurity as a Human Rights Issue“, Human Rights Watch, žiūrėta 2024 m. kovo 31 d. https://www.hrw.org/news/2020/05/26/its-time-treat-cybersecurity-human-rights-issue .

2.4.1. Žmogaus teisės kibernetinėje erdvėje

Kvestionuojant interneto valdymą, diskusija sukasi apie dvi pagrindines sąvokas, t. y. "laisvą internetą" ir "interneto suverenitetą". Pirmoji sąvoka sufleruoja apie laisvą interneto tinklą, skatinantį pilietines ir politines teises, tuo tarpu antroji pabrėžia valstybių kontrolę, įtvirtinant tradicinę tarpvalstybinę valdymo struktūrą. Žmogaus teisių kontekste skirtingų ideologijų diskusija – labai svarbi, apimanti laisvę išraiškai ir privatumą, o interneto suvereniteto atveju apimanti valstybės mechanizmus, skirtus riboti laisvą internetą bei stebėti interneto vartotojus.[104] Tačiau ITPK išleido bukletą „Žmogaus teisių chartija ir interneto principai", kuriame aprašytos žmogaus teisės internete: [105]

UNIVERSALUMAS IR LYGYBĖ Visi žmonės gimsta laisvi ir lygūs į orumą ir teisę, kurie turi būti gerbiami, saugomi ir įgyvendinami internetinėje aplinkoje.	LAISVĖ IR SAUGUMAS Kinetinėje ertmėje teisė į gyvybę, laisvę ir saugumą turi būti gerbiama, saugoma ir įgyvendinama. Ši teisė negali būti pažeidžiama arba naudojama tam, kad pažeistų kitų teisę.
TEISĖS IR SOCIALINIS TEISINGUMAS Internetas – erdvė, skirta propaguoti, apsaugoti ir įgyvendinti žmogaus teisių apsaugą ir socialinę pažangą bei teisingumą. Kiekvienas privalo gerbti kitų asmenų teises internetinėje aplinkoje.	ĮVAIROVĖ Kultūrinė ir kalbinė įvairovė internete turi būti skatinama, o techninė ir politinė naujovės turėtų būti skatinamos, kaip raiškos įvairovė.
PRIEINAMUMAS Visi turi lygias galimybes pasiekti ir naudotis saugiu ir atviru internetu.	INTERNETO LYGYBĖ Kiekvienas privalo turėti atvirą prieigą prie interneto turinio be jokių apribojimų, diskriminacijos, turinio filtravimo, komercinės ar politinės ir kitų priežasčių.

[104] David P. Fidler, „Cyberspace and human rights", Elgar Online, (2018): 111.

[105] Internet Rights and Principles Dynamic Coalition UN Internet Governance, *the charter of human rights and principles for the internet* 4 (2014).

IŠRAIŠKA IR ASOCIACIJA	STANDARTAI IR REGLAMENTAS
Kiekvienas turi teisę siekti, laisvai gauti ir skleisti informaciją internete be cenzūros ar kitokio kišimosi. Visi taip pat turi teisę laisvai bendrauti internete, socialiniuose tinkluose politiniais, kultūriniais ar kitais tikslais.	Interneto architektūra, ryšiai, sistemos, dokumentai ir duomenys grindžiami atvirais standartais, kurie užtikrina visišką sąveiką ir vienodas sąlygas visiems.
PRIVATUMAS IR DUOMENŲ APSAUGA	VALDYMAS
Kinetinėje ertmėje visi turi teisę į privatumą: laisvę nuo sekimo, duomenų šifravimo bei galimybę prie interneto jungtis anonimiškai. Taip pat kiekvienas žmogus turi teisę į duomenų apsaugą, įskaitant asmens duomenų rinkimo kontrolę, saugojimą, tvarkymą, šalinimą ir atskleidimą.	Žmogaus teisės ir socialinis teisingumas turi būti teisinis ir normatyvinis pagrindas, kuriuo grindžiama interneto veikla ir valdymas. Tai turi vykti skaidriai ir daugiašaliu būdu, remiantis atvirumo, įtraukimo, skaidrumo principais, dalyvavimu ir atskaitomybe.

3 lentelė. Sudarė autorė, remiantis Internet Rights&Coalition, „The Charter of Human Rights and Principles for the internet". (2014)

JT generalinis sekretorius Guterres pabrėžė, jog visuomenė yra stipresnė, kai yra galimybė atlikti reikšmingą vaidmenį politiniame, ekonominiame ir socialiniame gyvenime, tokiu būdu prisidedant prie politikos formavimo ir užtikrinant teisę į laisvą mintį. Tačiau plintant represiniams įstatymams, didėja ribojimai laisvės sklaidai, todėl naujos IT, nors ir padėjo plėstis visuomenės tinklams, bet taip pat suteikė galimybes valdžiai kontroliuoti ir apriboti žiniasklaidos laisvę, remiantis saugumo pretekstais, , o tai paveikia žmogaus teisių užtikrintumą.[106] KE kontroliavimas, skirtingai nuo visuotinės žmogaus teisių chartijos, neturi visuotinio tarptautiniu mastu pripažinto reglamento, todėl yra svarbu išsiaiškinti, kaip žmogaus teisės koreliuoja valstybės interneto kontekste.

JT straipsnio A/70/174 str.[107] 3-o str. 13 dalyje nurodoma: „*Valstybės, užtikrindamos informacinės ir ryšių technologijos saugų naudojimą, turi gerbti žmogaus teises [...] dėl teisės į privatumą skaitmeniniame amžiuje, kad būtų užtikrinta visiška pagarba žmogaus teisėms, įskaitant teisę į saviraiškos laisvę*."[108], atitinkamai užtikrinant žmogaus teises internete.[109] Vykstant interneto susiskaldymui dėl skirtingo valstybių ideologinio požiūrio, imantis veiksmų dėl KE valdymo valstybės lygmenyje, savaime susiformuoja skirtingas žmogaus teisių konteksto interpretavimas

[106] Antonio Guterres, „The Highest Aspiration: A Call to Action for Human Rights", United, Nations, (2020): 8.

[107] „Vyriausybinių ekspertų grupė dėl pokyčių informacijos ir telekomunikacijų srityje tarptautinio saugumo kontekste"

[108] Note by Secretary-General, „Group of Government Experts on Developing in the Field of Information and Telecommunications in the Context of Internatonal Security", United Nations General Assembly, 2015, *United General Assembly*, liepos 22d., 2015, 8.

[109] United Nations, *Report of the Secretary-General: Roadmap for Digital Cooperation* (United Nations, 2020),14.

interneto atžvilgiu. Šiuo atveju, tarkim Kinija, naudojasi kibernetiniu saugumu kaip priedanga tam, kad galėtų kontroliuoti ir toliau apriboti interneto veikimą ir teises šalies viduje."[110]

Tuo tarpu JAE Mansoor, taikus žmogaus teisių aktyvistas, už įrašus socialinėje erdvėje, kurie nesąžiningai teismo buvo pripažinti kaip įžeidinėjantys valstybę ir menkinantys jos prestižą, buvo nubaustas kalėti.[111] Iš esmės kibernetinėje erdvėje žmogaus teisėms gali kilti įvairių grėsmių, tarkim, interneto cenzūravimas arba tam tikrų domenų blokavimas pažeidžia įvairias teises, įskaitant prieigos prie informacijos ribojimą, draudimą žodžio ir nuomonės internete laisvei, taip pat draudimą naudotis įvairiomis socialinėmis ir kultūrinėmis teisėmis.[112] Atsižvelgiant į *Freedom House* organizacijos pateiktą statistiką, iš 70 šalių nepriklausomas internetas identifikuojamas tik 17, tuo tarpu dalinai laisvas apima 32 valstybes, o 21 šalyje internetas yra kontroliuojamas, todėl laikomas nelaisvu; Kinija iš esmės užima pirmąją vietą, surinkdama tik 9 balus laisvo interneto skalėje, Rusija 21.[113]

Šiuo atveju svarbu pabrėžti, kad skaitmeninis suverenumas yra siejamas būtent su valstybėmis, kurių politinė ideologija yra antidemokratiška, kurios internetą traktuoja kaip dar vieną įrankį, skirtą įgalintį politinį režimą. Remiantis *Freedom House* tyrimais, autoritarinėse valstybėse interneto laisvės suvaržymas apima šiuos kriterijus:

Interneto turinio filtravimas ir blokavimas, įskaitant socialinę mediją.
Politinio, socialinio ar religinio turinio platinimo kriminalizavimas.
Atsakomybės taikymas interneto paslaugų tiekėjams, kurie talpina arba neblokuoja neteisėto turinio.
Svetainių ar interneto paslaugų teikėjų priverstinis uždarymas.
Vartotojų atjungimas nuo interneto.
Rengiamos kibernetinės atakos prieš interneto svetaines, kurias valdo arba naudoja politiniai oponentai, disidentai ir nevyriausybinės organizacijos (pvz. žmogaus teisių
Interneto veiklos stebėjimas.
Manipuliavimas internetiniais ryšiais per vyriausybę palaikančius komentatorius ir dezinformacijos skleidimas.
Fiziniai išpuoliai, įskaitant žmogžudystes, prieš vyriausybę kritikuojančius interneto vartotojus.

[110] Brown, *It's Time to Threat Cybersecurity*.

[111] European Centre for Democracy and Human Rights, „In the shadow of the Burj Khalifa: the case of Ahmed Mansoor and the whitewashing of the United Arab Emirates, European Centre for Democracy and Human Rights, žiūrėta 2024 m. kovo 31 d. https://www.ecdhr.org/?p=1650 .

[112] Begum Burak, „Human Rights Violations in Cyberspace: Internet Censorship and Online Surveillance in Turkey" *Cyberpolitik Journal* 6, No. 12 (2022): 205.

[113] Freedom House, „Freedom on the Net 2023: The Repressive Power of Artificial Intelligence", Freedom House (2023): 24-27.

4 lentelė. Sudarė autorė, remiantis David P. Fidler, „Cyberspace and human rights“. (2018)[114]

Galima teigti, kad KE ir interneto veikimas apima platų spektrą žmogaus teisių, įskaitant nefizinius žmogaus teisių pažeidimus, kaip atjungimas nuo interneto, stebėjimas, propagandos ir dezinformacijos skleidimas, turinio cenzūravimas ir blokavimas. Tačiau žmogaus teisės kibernetinėje erdvėje taip pat apima ir fizinį žmogaus teisių pažeidimą, t. y. įkalinimą už valstybei kenkiančio naratyvo skleidimą ar net fizinį išpuolį ir žmogžudystę.

Apibendrinant – KE, suverenus valstybių internetas ir žmogaus teisės turi stiprią sąsają, turint omenyje, kad konstruktyviai internetas, kaip vienas objektas, savaime atrodo yra beribis ir neturintis valstybės ribų. Tačiau kita vertus, kiekviena teritorija, įskaitant ir ES, rengia įstatymus, kurie apsaugotų piliečius ir jų asmeninius duomenis visame pasaulyje. Tačiau atliepiant į kitas valstybes, interneto valdymo procesas apima kur kas daugiau fragmentų, kurie yra skirti ne tik apsaugoti valstybės piliečio informaciją, bet veikiau yra nukreipti į valstybės interesus. Šiuo atveju tokios valstybės, nepaisydamos žmogaus teisių paradigmos į žodžio ir informacijos laisvę, imasi formuoti suverenų valstybių internetą ieškodamos pasiteisinimų dėl centralizuoto interneto valdymo, kuris pažeidžia žmogaus teises, tačiau tampa įrankis valdžios galiai nacionalinėse ribose. Taip pat tokio naratyvo pagalba valstybės KE geopolitikos kontekste brėžia kibernetinio saugumo ir nacionalinės valstybės saugumo siekius, tuo pačiu ieškodamos sąjungininkių plečiant interneto kontroliavimu paremtą ideologinį mąstymą. Tad tai savaime atspindi problemos kompleksiškumą tarp laisvo interneto paradigmos ir suverenaus valstybės interneto formavimo žmogaus teisių kontekste.

3. Kinijos ir Rusijos suverenus valstybių internetas žmogaus teisių kontekste

3.1. Metodologija

Trečiojoje darbo dalyje atliekama Rusijos ir Kinijos KE suverenaus interneto formavimo lyginamoji analizė. Lyginama, kaip ir kokius aspektus žmogaus teisių kontekste interneto valdymas apima nuo 2015 m., nes tuomet Kinijos vyriausybė pirmą kartą oficialiai paminėjo suverenumą kibernetinėje erdvėje, o Rusija pradėjo formuoti idėjas apie suverenų valstybės internetą. Taip pat svarbus faktas, kad tais pačiais metais Kinija ir Rusija pasirašė dvišalę bendradarbiavimo sutartį dėl KE saugumo užtikrinimo, todėl tyrime į tai taip pat yra atsižvelgiama.

Empirinės darbo dalies laikotarpis yra nuo 2015 m. iki 2024 m. Remiantis pirminiais šaltiniais, t. y. kasmetiniai *Freedom House*, „Laisvė internete“ raportai apie Rusijos ir Kinijos valstybes. Raportuose išskiriama tematika, apimanti KE ir žmogaus teises, taip pat empirinėje dalyje nagrinėjami šalių įstatymai, turintys sąsajos su KE valdymo procesais minėtose valstybėse.

[114] *Special Rapporteur's Report* (n 17); *Freedom House* (n 20); *Freedom House* (n 22) cituota iš David P. Fidler, „Cyberspace and human rights“ *Elgar Online* (2018): 102.

Atsižvelgiant į tarptautinių režimų teoriją, režimo formavimui ir veikimo principui svarbu reglamentai, protokolai, sprendimų priėmimas, įstatymai bei pačios normos, kurios sąveikauja su valstybės interesais ir lūkesčiais. Šiuo atveju Rusijos ir Kinijos valstybių lūkestis KE kontekste – išlaikyti nacionalinį suverenitetą. Toliau svarbu išsiaiškinti, kaip valstybės, per kibernetinę erdvę formuodamos suverenų valstybių internetą, atsiriboja nuo išorės kontrolės ir sąveikauja su žmogaus teisėmis.

Klausimą reikia nagrinėti dviem aspektais: apsibrėžiant pagrindines tematikas, kurios vyrauja kalbant apie Rusijos ir Kinijos KE valdymą, t. y. kokios tendencijos dominuoja sprendimų priėmėjų darbotvarkėje, o antrasis – žmogaus teisių ir laisvių pažeidimo mastas, vyraujantis kibernetinėje erdvėje.

Pirmoji aspekto analizė svarbi tuo, kad sukonkretinamas tyrimo laukas ir išsiaiškinami pagrindiniai KE valdymo principai, apsibrėžiant esmines detales, į kurias svarbu atkreipti dėmesį kalbant apie suverenaus interneto formavimą žmogaus teisių kontekste Rusijos ir Kinijos atveju. Tai turi įtakos antrajam tyrimo laukui, kuriame plačiau, bet išsamiau analizuojama Rusijos ir Kinijos interneto kontrolė, bei suverenaus valstybių interneto mastas ir įtaka žmogaus teisėms.

3.2. Lyginamoji analizė

Rusijos ir Kinijos KE kontrolė atrodo labai panaši, tačiau, remiantis *Freedom House* raportais, galima įžvelgti skirtingą valstybių elgesį vienais ar kitais klausimais. Šiame skyriuje bendrai aptariami formuojamo suverenaus valstybės interneto ypatumai minimose valstybėse, apibendrinant atitikimus ir skiriamuosius bruožus tam, kad būtų galima išskirti svarbiausius segmentus, susijusius su žmogaus teisėmis KE. Šie skirtumai ir panašumai bus plačiau aptariami kituose poskyriuose bei remiantis minėtais raportais atliekama analizė siekiant atsakyti į tyrimo klausimą.

Remiantis minėtais raportais išskiriamos pagrindinės tematikos, kurios yra plačiausiai aptarinėjamos ir dažnai kartojasi ne vienerius metus.

Rusijos KE praktiniame valdyme išryškinamos įstatymų pataisos, kurios koreliuoja su interneto kontroliavimu. Taip pat pabrėžiamos vis didesnės valdžios galimybės implementuoti prieigą prie interneto vartotojų asmens duomenų. Akivaizdūs žurnalistų, žmogaus teisių aktyvistų, socialinių tinklų vartotojų areštai, precedento neturinčios atakos prieš socialinę žiniasklaidą ir ryškus Kremliaus taikinys prieš NVO. Taip pat neatsiejami tokie veiksniai kaip užsienio domenų blokavimai, plati interneto cenzūra, turinio filtravimas.

Tuo tarpu Kinijos kasmetiniuose raportuose pastebima VPN kontrolė, asmeninių duomenų rinkimas. Didelis dėmesys sutelkiamas į įstatymų pataisas, kurios apima administracinę ir baudžiamąją atsakomybę už tam tikrą veiklą internete. Įžvelgiama tematika apima užsienio domenų blokavimą ir žurnalistų, žmogaus teisių aktyvistų bei etninių mažumų persekiojimas

už „netinkamą“ elgesį ir veiklą internete. Taip pat pastebimas Kinijos valstybės indėlis formuojant valstybės teigiamą naratyvą internete ir sistemingo interneto vartotojų siekimo proceso kuriant mobiliąsias programėles su įdiegta sekimo įranga. Interneto cenzūravimo ir turinio filtravimas iš esmės pabrėžiamas kone kiekviename kasmetiniame raporte.

Apibendrinus *Freedom House* kasmetinius raportus apie Kinijos ir Rusijos šalis, galima išskirti šiuos skirtumus ir panašumus:

	Kinija	**Rusija**
Skirtumai	Platesnio masto persekiojimai.	Siauresnio masto persekiojimai.
	Istorinių ir politinių faktų kontrolė.	Dabartinių geopolitinių įvykių ir valstybės kritikos kontrolė.
	Griežti vartotojų identifikavimo reglamentai.	Švelnesio pobūdžio vartotojų identifikavimo sistema.
	Didesnė izoliacija nuo tarptautinio interneto tinklo dėl „Didžiosios ugniasienės”.	Šiek tiek platesnė prieiga prie pasaulinio interneto tinklo.
	Etninės mažumos cenzūra.	LGBT aktyvistų cenzūra.
	Kinija ir Rusija	
Panašumai	Aktyvi interneto cenzūra.	
	Teisiniai reglamentai skirti kontroliuoti informacijos srautą ribojant vartotojų teisę į laisvą internetą.	
	Vyriausybės institucijų stebima ir kontroliuojama interneto vartotojų veikla internete.	
	Pilietinės visuomenės, žmogaus teisių aktyvistų, žurnalistų persekiojimai.	
	Socialinių tinklų kontroliavimas.	
	VPN kontrolė.	

5 lentelė. Sudarė autorė, remiantis Freedom on The Net, Rusijos ir Kinijos raportais 2015 - 2024 m.

3.2.1. VPN ir asmeninė registracija

VPN yra plačiai naudojama IT sistema, kurios veikimas pasižymi šiais pagrindiniais principais: 1) saugaus naršymo internete užtikrinimas; 2) privatumo užtikrinimas, apeinant interneto paslaugų tiekėjo (ISP) interneto tinklą; 3) konfidencialumas, suteikiant virtualius IP adresus; 4) galimybės suteikimas kibernetinėje erdvėje virtualiai keisti geografinę lokaciją įgalinant pasiekti svetaines,

žaidimus, paslaugas, pramogas, užblokuotas dėl geografinės skaitmeninės erdvės.[115] VPN turi dviprasmišką veikimo principą: viena vertus, ši technologija apsaugo interneto vartotojo duomenis, antra vertus, VPN sistema padeda prieiti prie pasaulinio interneto tinklo, ypač valstybėse, kuriose skaitmeninė erdvė yra kontroliuojama suteikiant interneto vartotojui IP adresą pagal norimą lokaciją.

Kinija nuo 2015 m. atnaujino didžiosios ugniasienės veikimo principą užblokuodama keletą VPN tiekėjų paslaugas teikiančių įmonių[116], o 2017 m. papildomai reikalaudama, jog verslas, norintis teikti tokias paslaugas, turi gauti licencijas. Tuo tarpu 2018 m. atsirado nauji apribojimai, kuriuose buvo reglamentuojama, jog autorizuoti VPN tinklai yra skirti tik „vidiniam“ naudojimui, taip pat dėmesio susilaukė tarptautiniai viešbučiai, kurių vestibiuliuose įprastai buvo galima apeiti didžiąją ugniasienę dėl įrengto VPN, tačiau valdžios institucijos uždraudė viešbučių sistemose diegti šią sistemą.

Kinijos suverenus internetas pasižymi asmeninių duomenų rinkimu, griežtinant registraciją tinklaraščiuose, momentinių pranešimų puslapius ir diskusijų forumus, nurodant, jog privaloma naudoti asmens dokumentą norint atlikti registraciją. Šį reguliavimą sustiprino ir kibernetinio saugumo įstatymas, teigiantis, kad tinklo ir ryšio operatoriai turi saugoti dokumentus, skirtus registracijai, o neatlikus autentifikacijos, paslaugų operatoriai turi nutraukti paslaugų tiekimą. Taip pat svarbų vaidmenį atlieka kovos su terorizmu įstatymas, kuriuo visos telekomunikacijų ir interneto paslaugas teikiančios įmonės turi suteikti vyriausybei prieigą prie duomenų bei bendradarbiauti siekiant šifruoti duomenis. Tuo tarpu 2023 m. įsigaliojo prieš- žvalgybinis įstatymas, apribojantis informacijos, susijusios su nacionaliniu saugumu, perdavimą. Taip pat verta paminėti, kad valdžios institucijoms siekiant nacionalinio saugumo, leidžiama tikrinti elektroninę įrangą ir duomenis bei taikyti išvykimo ir atvykimo į valstybę draudimus, kas iš esmės pažeidžia žmogaus privatumą.

Įdomu tai, kad Kinijos valstybė imasi dviprasmiško interneto valdymo, viena vertus, įpareigojant interneto vartotojus registracijoms naudoti asmens dokumentus, kita vertus, varžant VPN(turima omenyje tai, kad jeigu prisiregistruojama asmeniniu dokumentu, tuomet galimai valstybė yra įgali matyti konkretaus asmens veiklą internete). Tuo tarpu VPN legitimacija parodo, kad nors valstybė kuria suverenų internetą turėdama tikslą sumažinti užsienio įtaką ir prieigą prie uždrausto pasaulinio tinklo, visgi VPN produkcija nėra galutinai blokuojama. Veikiau reglamentuojama, o būtent kuomet registruotas interneto vartotojas naudoja VPN, jis įgauna privatumą ir konfidencialumą dėl esamos lokacijos. Todėl šiuo atveju galima įžvelgti, jog valstybės

[115] Shahad A. Alashi ir Hanaa A. Aldahawi, „Cybersecurity Management for Virtual Private Network (VPN) Applications: A Proposed Framework for the Governance of their USe in the Kingdom of Saudi Arabia“, *Journal of Information Security* 1, No. 1 (2020): 36.

[116] BBC News, „China blocks virtual private network use“ BBC, žiūrėta 2024 m. balandžio 12 d. https://www.bbc.com/news/technology-30982198 .

veiksmai prieštarauja vienas kitam. Kaip teigia Yuen, „*Vis labiau sudėtinga informacijos kontrolės sistema ne tik dar labiau pažeidžia žmogaus teises, įtvirtintas pačioje Kinijos Konstitucijoje, bet ir mažina partijos visuomenės palaikymą bei slopina šalies kūrybiškumą ir inovacijas, būtinas sąlygas pažangesniam ekonomikos vystymuisi.*“[117] Todėl galima teigti, kad Kinija implementuoja asmeninį žmonių sekimą internete, tačiau dėl tam tikrų priežasčių visiškai nesiryžta blokuoti VPN produkcijos galimai todėl, kad tai savaime paveiktų ekonomikos vystymąsi ir įtakotų visuomeninę valdžios kritiką , ypatingai piliečių, kurie naudoja VPN socialinei veiklai, kaip, tarkim, mokslinė veikla.

Tuo tarpu Rusijoje nuo 2024 m. kovo 1 d. įsigaliojo draudimas reklamuoti VPN[118], teigiant, kad pagal Rusijos įstatymus yra draudžiama dirbti su priemonėmis, apeinančiomis prieigą prie nelegalaus ir užblokuoto turinio.[119] Įstatymas reglamentuojantis VPN veikimo principą buvo priimtas dar 2017 m., kuomet Putinas pasirašė dokumentą, leidžiantį blokuoti VPN paslaugas. Pats įstatymo principas apibrėžia, jog įgaliotos struktūros turi nustatyti internetines svetaines ir paslaugas, kurios suteikia prieigą prie užblokuotų puslapių, o jei po įspėjimo svetainė toliau tęs nelegalią veiklą, Roskomnadzor[120] turi apriboti prieigą prie tokios svetainės internetinio puslapio paslaugų.[121] Šiuo atveju reikėtų atkreipti dėmesį į tai, kad VPN reguliacija Rusijoje prasidėjo dar 2017 m., tačiau remiantis raportais pastebėta, jog Rusijoje daugiausiai cenzūruojamas Rusijos ir Ukrainos geopolitinis konfliktas, kuris tęsiasi jau nuo 2014 m., kuomet prasidėjo karas dėl Krymo ir Donbaso. Siekdama cenzūruoti tematiką minėta tema, Rusija 2017 m. ėmėsi veiksmų prieš VPN sistemą, tuo tarpu besitęsiantis karas paskatino ryškesnio rusų kontraversiško požiūrio atsiradimą, todėl 2024 m. valdžia ėmėsi toliau griežtai kontroliuoti VPN.

Nuo 2015 m. pastebima, jog Rusija pradėjo vis daugiau implementuoti galimybes prieiti prie vartotojų duomenų, įgyvendinus „Jarovajos“ antiteroristinio įstatymo pataisos paketą, kuriuo padidinamos valdžios galimybės gauti prieigą prie asmeninės informacijos. Politika paaštrėjo Rusijos invazijos Ukrainoje metu, kuomet 2022 m. vyriausybė įvedė įstatymus, įpareigojančius telekomunikacijų operatorius glaudžiau bendradarbiauti su Federaline saugumo tarnyba. Kaip teigia Orlova, Rusija pasitelkdama įstatymus visiškai pašalino anonimiškumą legitimuodama savo galimybę šalinti raišką, kuri kelia grėsmę jos dabartiniams veiksmams, nes jei anonimiškumas tampa

---

[117] Samson Yuen, „Becoming a Cyber Power: China‘s cybersecurity upgrade and its consequences“*OpenEdition* Journals (2015): 58.

[118] Meduza, „Russia may block Wikipedia due to article on VPNs that help reach blocked sites, says lawmaker“MEDUZA, žiūrėta 2024 m. balandžio 2 d. https://meduza.io/en/news/2024/03/03/russia-may-block-wikipedia-due-to-article-on-vpns-that-help-reach-blocked-sites-says-lawmaker .

[119] Anton Kuznetsov, „From March 1, Roskomnadzor will block advertising of VPN services on the network“ tass.rum žiūrėta 2024 m. balandžio 2 d. https://tass.ru/obschestvo/20124281.

[120] Rusijos Federacijos vyriausybės priežiūros institucija „Federalinė ryšių, informacinių technologijų ir masinės komunikacijos priežiūros tarnyba“

[121] Meduza, „The State Duma introduced fines for violation of the law on anonymizers“MEDUZA 2024 m. balandžio 10 d. https://meduza.io/news/2018/06/05/gosduma-vvela-shtrafy-za-narushenie-zakona-ob-anonimayzerah .

nepripažįstamas kaip būtinybė, tuomet žodžio laisvė savaime tampa privilegija, tuo tarpu nacionalinio suvereniteto formavimas kibernetinėje erdvėje gali potencialiai eskaluoti fizinius konfliktus. [122] Kita vertus, Rusijoje žodžio laisvė įvairiais įstatymais ir Kremliaus nutarimais internete plačiai cenzūruojama, todėl tai veda į galimus fizinius pilietinius konfliktus ateityje.

Remiantis JT žmogaus teisių 12 str.: „*Niekas neturi patirti savavališko kišimosi į jo privatumą, šeimos gyvenimą, buitį ir susirašinėjimą arba kėsinimosi į jo garbę ir reputaciją. Kiekvienas turi teisę į įstatymo apsaugą nuo tokio kišimosi arba kėsinimosi*.[123] Galima teigti, kad valstybės, formuodamos prieigą prie duomenų ir mažindamos internetinį anonimiškumą, pažeidžia žmogaus teisių 12 str., o ypač Kinija, kuri dėl nacionalinio saugumo turi galimybę tikrinti piliečių elektroninius įrenginius ir reguliuoti žmonių atvykimą ir išvykimą iš valstybės.

3.2.2. Cenzūra ir persekiojimai

Kinijoje ir Rusijoje ryškėja žurnalistų ir interneto vartotojų precedento neturintys areštai, fizinis smurtas bei administracinė ir baudžiamoji atsakomybė už veiklą internete. Taip pat abiejose šalyse pastebima griežta interneto cenzūra ir turinio filtravimas.

Kinijoje 2018 m. birželio mėn. – 2019 m. gegužės mėn. laikotarpiu labiausiai cenzūruotos temos : ekonomikos naujienos atsižvelgiant į didėjantį prekybos karą su JAV ir lėtėjantį vidaus augimą, Tianmen aikštės metinės, protestai Honkonge ir masiniai etninės musulmonų mažumos sulaikymai Xinjiang provincijoje. Xinjiang provincijos tematika suverenaus valstybės interneto žmogaus teisių kontekste išties labai svarbi, kadangi pastebėta, jog interneto kontrolė būtent šioje Kinijos provincijoje yra dar griežtesnė nei kituose regionuose. Remiantis Bertolini, režimas, kovojantis su etnine uigūrų mažuma, internetą pasitelkia kaip įrankį, naudodamas jį kaip represijų ir kontrolės priemonę, kadangi, skirtingai nei kitose Kinijos provincijose, Xinjiang regione nepriklausomai ar internetas naudojamas, ar ne, jis tampa visišku žmogaus teisių pažeidimu ir yra diskriminuojantis lyginant su kitomis Kinijos teritorijomis. Todėl teigiama, kad Kinijoje vyrauja du skirtingi internetai, kurių pagrindą sudaro dvi skirtingos reguliavimo sistemos, tikslai ir pažeidimai, o pats Xinjiang interneto laukas laikomas tarsi laboratorija naujiems Kinijos represinių priemonių internete testavimams.[124] Kinijoje kovai su terorizmu didelis dėmesys skiriamas Xinjiang provincijai, reaguojant į interneto griežtesnius suvaržymus šioje teritorijoje galima teigti, kad vyrauja du skirtingi interneto veikimo principai, Kinijos ir Xinjiang provincijos, tuo tarpu pastarasis veikimo principas

[122] Alexandra V. Orlova, „"Digital Sovereignty" Anonimity and Freedom of Expression: Russia's Fight to Re-Shape Internet Governance 26, No. 2 (pavasaris 2020): 246-247.
[123] United Nations, „Universal Declarations of Human Rights" United Nations 2024 m. balandžio 10 d. https://www.un.org/en/about-us/universal-declaration-of-human-rights .
[124] Elisa Bertolini, „Internet Governance and Terrorism in the Context of the Chinese Compression of Fundamental Rights and Freedoms" *Global Jurist* (2028): 1-17.

tampa suverenus provincijos internetas, kurį testuojant formuojamas suverenus valstybės internetas. Remiantis JT žmogaus teisių chartija internete, „*Įvairovė: kultūrinė ir kalbinė įvairovė internete turi būti skatinama, o techninė ir politinė naujovės turėtų būti skatinamos, kaip raiškos įvairovė*“ ir „*Interneto lygybė: kiekvienas turi visuotinę ir atvirą prieiga prie interneto turinio, be jokių apribojimų, diskriminacinio prioritetų nustatymo, filtravimo ar komercinio duomenų srauto kontrolės politiniais ar kitais pagrindais*“ galima teigti, jog Kinija ne tik pažeidžia įvairovės skatinimą internete diskriminuodama uigūrų etninę mažumą, bet ir akivaizdžiai diskredituoja etninę mažumą nuo Han mažumos Kinijoje dėl politinių, antiteroristinių interesų, kurie neturi jokio precedento, ypač interneto kontrolės kontekste.

Kita vertus, nors Xinjiang provincija susilaukia didelio masto represijų KE, kurių viena yra interneto atjungimas, [125] visgi tai neapsaugo nuo platesnio masto persekiojimų už internetinę veiklą. Valdžios institucijos sulaiko ne tik religinių ir etninių mažumų atstovus, bet ir žinomus žurnalistus bei žmogaus teisių aktyvistus. Kaip pavyzdžiui, už “valstybės valdžios suveržimą” suimtas ir 14 metų laisvės atėmimo bausme nubaustas žinomas žmogaus teisių aktyvistas ir blogeris.

Covid-19 pandemija ne tik paskatino didesnį persekiojimą, bet ir cenzūravimą. Buvo persekiojami, baudžiami žurnalistai ir aktyvistai už pandemijos ataskaitų teikimą, šnipinėjimą, dezinformacijos ir kritiško naratyvo skleidimą bei į persekiojimo radarą pateko šeimos nariai, kalbėję viešai apie nuo viruso mirusius giminaičius. Taip pat buvo siekiama slopinti nepriklausomus informacijos šaltinius, skleidžiančius kritiką apie padarytas ankstyvas klaidas dėl netinkamos komunikacijos pandemijos pradžioje. Cenzūravo raginimus atlikti nepriklausomą tyrimą apie koronaviruso kilmę, taip pat kritiką dėl Kinijoje pagamintų covid-19 vakcinų. Tačiau, kaip teigiama ataskaitoje, covid-19 naratyvą partija panaudojo savo naudai, pasitelkdama pandemiją, kaip įrankį sekti, stebėti, kontroliuoti piliečių elgesį naudojant mobiliojo telefono programas ir kitas technologijas. Kaip teigia Jiang: „*Nors žmogaus teisės Kinijoje tradiciškai yra orientuotos į kolektyvinį socialinį ir ekonominį teisingumą, teisė į žodžio laisvę vis dažniau tampa priemone siekiant socialinio ir ekonominio teisingumo, kurį Kinijos valstybė žada užtikrinti gyventojams*.“[126] Kita vertus, nors Kinija turi tradicinį požiūrį į žmogaus teises, tai nepateisina interneto kontrolės, pažeidžiančios visuotinę žmogaus teisę, ypatingai formuojant suverenų valstybių internetą, kuriame nėra vietos jokiai opozicijai ar kritikai prieš valstybės veiksmus ir politiką. Todėl visuomenė neturi galimybių gauti informacijos tam, kad galėtų formuoti konstruktyvų požiūrį apie socialinį ir ekonominį gyvenimą Kinijoje. KKP siekis užtikrinti socialinį ir ekonominį gyvenimą pasižymi pragmatišku požiūriu siekiant opozicijos ir kritikos nelegetimumui skaitmeninėje aplinkoje, tačiau,

[125] *Ibid,* 6.

[126] Min Jiang, „Chinese Internet Business and Human Rights“ *Business and Human Rights Journal* 1 (2015): 144.

kita vertus, VPN yra vienas iš įrankių visuomenei prieiti prie konstruktyvios nuomonės. Todėl, mano manymu, interneto fragmentacija apima ne tik tarptautinį, bet ir vidinį valstybės interneto tinklą.

Taip pat pastebėtas didesnis užsienio NVO stebėjimas, kita vertus, Kinijoje dažniau užfiksuojamos represijos prieš svetainių redaktorius ir žmogaus teisių aktyvistus, užregistruoti precedento neturintys įvykiai, kuomet dėl veiklos internete asmenys patyrė teisines ir nelegalias represijas, įskaitant savavališką sulaikymą, kankinimus ir griežtas bausmes. Savo ruožtu laisvo interneto galios komponentas, pastarosios atveju, gali padėti suprasti, kodėl valstybės priešinasi priimti laisvo interneto, kaip žmogaus teisių principą, turint omenyje, kad interneto suvaržymai savaime padeda užgožti patį žmogaus teisių reglamentą.[127]

Tuo tarpu Rusijoje interneto cenzūros pagrindinis objektas – karas Ukrainoje. Visų pirma ryškus Kremliaus taikinys formuojant suverenų valstybės internetą tapo NVO. 2016 m. Levados centras, kuris yra nepriklausomas Rusijos visuomenės nuomonės tyrimų centras, įtrauktas į „užsienio agentų“ sąrašą. Nuo 2019 m. Rusija pradėjo persekioti NVO narius ir žurnalistus, baugindama juos policijos reidais ir areštais, toliau sistemingai priiminėdama įstatymus, įpareigojančius NVO gaunančius tarptautinį finansavimą užregistruoti kaip „užsienio agentus“ apribojant jų veiklą ir taipogi grasinant baudomis, reidais ir areštais. Tuo tarpu po karo pradžios įvyko „užsienio agentų“ įstatymo pataisa, įskaitant tuos, kurie laikomi „užsienio įtaka“ įtraukti į „užsienio agentų“ sąrašą. Į nepageidaujamų organizacijų sąrašą įtrauktos pilietinės visuomenės organizacijos ir naujienų agentūros, kaip pavyzdžiui, nepriklausoma naujienų agentūra „Meduza“, jas kriminalizuojant. Tuo tarpu po Rusijos invazijos į Ukrainą šalies KE, įskaitant ir televiziją, opozicinė informacija apie karą Kremliaus laikoma kaip melagingos naujienos.[128] Rusijos idėja apie suverenų valstybės internetą gimė 2015 m., paskui galima stebėti sistemingą Rusijos visiško interneto suverenumo siekį, pradedant nuo NVO ir baigiant „užsienio agentų“ sąrašu, kuris leidžia diskredituoti ir iš esmės riboti jų veiklą.

3.2.3. Blokavimas, komentarai, socialiniai tinklai

Kinijoje kasmet sistemingai blokuojami užsienio domenai, kuriuose kritiškai vertinimas Xi. Pastebima, kad 2017 m. interneto stebėjimas pasiekė naujas aukštumas dėl naujų įstatymų, kurie dar labiau kontroliuoja internetą. Atsirado didelė cenzūra „*WeChat*“ platformoje, sulaikant asmenis dėl komentarų ; teisiškai baudžiant už netinkamą turinį socialinėje medijoje ir komentarus, prasidėjo savicenzūros skatinimo strategija. Taip pat pradėta naudoti taktika, kai dėl „gandų

[127] Madeline Carr, „Internet freedom, human rights and power“ *Australian Journal of International Affairs* 67, No. 5 (2013): 623.
[128] McMahon, *Russia is Censoring News on the War in Ukraine. Foreign Media Are Trying to Get Around That* https://www.cfr.org/in-brief/russia-censoring-news-war-ukraine-foreign-media-are-trying-get-around .

platinimo“ uždaromos asmeninės „*WeChat*“ vartotojų paskyros, atimant iš jų daugiafunkcinį įrankį, kuris yra būtinas Kinijos piliečių kasdieniame gyvenime. Prieš 30-ąsias Tianmen aikštės metines turinio šalinimas, svetainių uždarymas ir socialinių tinklų paskyrų trynimo mastas išaugo įskaitant naujas platformas, kurios anksčiau necenzūravo apolitinių temų.

Remiantis Roskomsvoboda duomenimis, 2022 m. Rusijoje užblokuota 247 000 domenų, įskaitant vietines ir užsienio naujienų agentūrų svetaines, žmogaus teisių organizacijas ir 2022 m. „Memorial International“ žmogaus teisių organizaciją Rusijos teritorijoje. Užkirstas kelias interneto vartotojams pasiekti informaciją dėl valdžios institucijų priimto sprendimo iš esmės pažeidžia EŽTK 10 straipsnį: [129] „*Kiekvienas turi teisę į saviraiškos laisvę. Ši teisė apima laisvę turėti savo nuomonę ir gauti bei skleisti informaciją ir idėjas nesikišant valdžios institucijoms nepriklausomai nuo valstybės sienų*.[130]

Kinijoje gresia griežta baudžiamoji atsakomybė už melagienų skleidimą socialinėje erdvėje. Pagal 2016 m. įstatymo pataisą, už tai įvesta iki 7 metų laisvės atėmimo bausmė. Tačiau 2021 m. prasidėjus kovai su verslininkais, kurie atsisakė laikytis partijos nurodymų, skirtinos bausmės tapo kur kas didesnės: kovos su korupcija aktyvistas buvo nuteistas 20 metų laisvės atėmimo bausme už „valstybės valdžios sužlugdymo kurstymą“, įrodymais pateikiant keletą Huaiqing „*WeChat*“ įrašų ir netgi privačias žinutes. 2020 m. nekilnojamojo turto magnatas ir partijos narys Zhiqiang buvo nuteistas 18 metų laisvės atėmimo bausme už korupciją po to, kai internete kritikavo Xi dėl reakcijos į pandemiją. Taip pat 2021 m. nauji įstatymai paskelbė, kad tie, kurie pažeidžia ginkluotųjų pajėgų narių reputaciją, gali būti baudžiami iki 3 metų laisvės atėmimo bausme, dar labiau apribojant laisvę į nuomonę ir saviraišką.

Rusijos invazijos Ukrainoje metu buvo atlikta įdomi įstatymo pataisa, kuri draudžia diskredituoti ar sąmoningai skleisti melagingą informaciją apie Rusijos kariuomenę, o už kritikavimą skiriamos administracinės ir baudžiamosios atsakomybės baudos. Politikas Jašinas buvo nuteistas kalėti už tai, kad „*Youtube*“ pasidalino vaizdo įrašu apie Rusijos kariuomenės įvykdytus žiaurumus Bučoje. Be to, pagal Roskomnadzor nutekintus duomenis atskleista, kokiu dideliu mastu vyriausybinės agentūros stebi asmenų veiklą socialinėje žiniasklaidoje siekiant susidoroti su pasipriešinimu, taip pat atskleista informacija apie diegiamas automatizuotas sistemas siekiant aptikti kritinį turinį.

2024 m. Rusijoje buvo reikšmingi metai dėl vykusių prezidento rinkimų. Rusijos pastarieji prezidento rinkimai, Navalno mirtis ir karas Ukrainoje paskatino Kremlių imtis griežtų interneto

---

[129] Allerson, *Internet Censorship in Russia,* 250.

[130] European Court of Human Rights, „*Euroepan Convention on Human Rights as amended by Protocols Nos. 11, 14 and 15, supplemented by Protocols Nos. 1, 4, 6, 7, 12, 13 and 16*“ France, 1970, https://www.echr.coe.int/documents/d/echr/convention_ENG (žiūrėta 2024 m. balandžio 4 d).

blokavimo procesų. Teigiama, kad per protestus buvo užfiksuoti interneto blokavimo incidentai, kuomet „*Whatsapp*“ ir kitų komunikacijos programėlių, tokių kaip „*Telegram*“, veikimas buvo nutrauktas, o sausį Baškiros provincijoje, Dagestano ir Jakutijos regionuose per protestus taip pat užfiksuoti sėkmingi interneto nutraukimo veiksmai. Navalno laidotuvės tapo dar vienu įvykiu, per kurį blokuotas internetas. Pranešama, kad per laidotuves Maskvoje interneto ryšio tinklų greitis buvo pristabdytas, todėl vartotojai susidūrė su problemomis norėdami įkelti vaizdo įrašus ar skelbdami vaizdus socialinėje erdvėje. Verta pabrėžti, kad, nepaisant visų ribojimų, Rusijos pareigūnai nustatinėja interneto srauto modelius gaunamus iš VPN sistemos, o šiems aptikus – nutraukia ryšį. Iš esmės tai parodo, kad Rusija imasi sudėtingo technologinio interneto kontrolės principo, kuriuo bando sutvarkyti spragas, kadangi tai reikalauja specializuotos technikos, pabrėžiant tai, jog Kinija tokią taktika remiasi per jautrius politinius momentus.[131]

Tuo tarpu valdant Xi, KKP smarkiai išplėtė cenzūros aparatą. Teigiama, kad Kinijoje nėra taikoma visiška interneto cenzūra, nes dažnai leidžiama diskutuoti jautriomis temomis, tokiomis kaip vietos valdžios korupcija ar netinkamas regioninis valdymas. Pabrėžiama, kad griežta cenzūra taikoma tik aukšto rango partijos lyderių, Kinijos vienpartinės sistemos ir istorinių temų, kritikai. Tačiau verta paminėti, kad Kinijos cenzūros aparatas yra netolygiai išvystytas ir turi problemų su finansavimu, o pats cenzūros organizuotumas laikomas chaotišku dėl perteklinių arba tarpusavyje persidengiančių sričių, kurios sudaro neveiksmingumo principą, savaime kuriant cenzūros spragas ir socialinius neramumus.[132]

Remiantis „Interneto ateities deklaracija“: „*[...] įskaitant teisę į saviraiškos laisvę, kartu skatinant nuomonių įvairovę, ir pliuralizmą, nebijant cenzūros, priekabiavimo ar bauginimo. Saugoti ir gerbti žmogaus teises ir pagrindines teises visoje skaitmeninėje ekosistemoje [...]. Susilaikyti nuo piktnaudžiavimo internetu ar algoritminėmis priemonėmis ar metodais neteisėtam stebėjimui, priespaudai ir represijoms, nesuderintoms su tarptautiniais žmogaus teisių principais [...].*“[133] galima daryti išvadą, jog Kinijos ir Rusijos interneto kontrolė visiškai prieštarauja žmogaus teisėms, nes apima cenzūrą, neteisėtą sekimą, bauginimus bei represijas.

Pastebima, kad lyginant Rusiją ir Kiniją, pastarojoje vyrauja kur kas konkretesnis žmonių sekimas ir yra pasitelkiama socialinių tinklų savicenzūros taktika, tuo tarpu Rusijoje tematika apima daugiausia kariuomenę. Kinijos cenzūros aparatas, nors ir apima ilgesnį laikotarpį ir atrodo geriau

---

[131] Adam Satariano et al., „Rusia Strengthens Its Internet Controls in Critical Year of Putin“, The New York Times, žiūrėta 2024 m. balandžio 15 d. https://www.nytimes.com/2024/03/15/technology/russia-internet-censors-vladimir-putin.html .

[132] Kieran Green et al. „Censhorship Practices of the People‘s Republic of China“ (Exovera‘s Center for Intelligence Research and Analysis, 2024): 2-3.

[133] Baltiejie rūmai, „*A Declaration for the Fututre of the Internet“* 2022, https://www.whitehouse.gov/wp-content/uploads/2022/04/Declaration-for-the-Future-for-the-Internet_Launch-Event-Signing-Version_FINAL.pdf (žiūrėta 2024 m. balandžio 15 d.)

išvystytas dėl ilgesnės metų praktikos, t. y. nuo 2000 m., vis dėlto nėra pakankamai subalansuotas, kad būtų visiškai efektyvus visos valstybes mastu. Dėl to Kinija neturi efektyvaus cenzūros aparato, nors ir atrodo turinti daugiau patirties šioje srityje nei Rusija. Dėl šios priežasties būtų galima daryti prielaidą, kad tokiu atveju Rusijos cenzūros veikimo principas turėtų būti dar prastesnis. Vis dėlto, esant kritinei situacijai, Rusija gali imtis kraštutinių veiksnių, tokių kaip interneto išjungimas. Rusijos įstatymo pataisa, susijusi su mobilizacija ir Rusijos karu Ukrainoje, kuriam nuolat reikia karių papildymo, susijusi su įstatymo pataisa, kurios tikslas cenzūruoti „melagingą“ informacija apie Rusijos kariuomenę ir jos išteklius. Taigi, šiais metais, kuomet vyko keletas reikšmingų įvykių Kremliui, šalis griebėsi sudėtingos techninės procedūros, t. y. interneto suvaržymo, kad galėtų pažaboti internetą kaip opozicijos įrankį, naudojamą skleisti neigiamą naratyvą prieš valdžią.

3.2.4. Įstatymai ir suverenus valstybės interneto formavimas

Nuo 2016 m. Rusija ir Kinija teisės aktų rinkinius papildė naujais įstatymais, parodydamos šalių požiūrį į kibernetinį saugumą siekiant stiprinti nacionalinę informacinę erdvę ir duomenų apsaugą.[134][135]

Rusija	Kinija
2016 m. Rusijos Federacijos informacinio saugumo doktrina	2016 m. Kinijos kibernetinio saugumo įstatymas
2016 m. „Jarovajos pataisos“ dėl priverstinio duomenų saugojimo	2021 m. Kinijos Liaudies Respublikos asmens duomenų apsaugos įstatymas*[136]
2017 m. įstatymas, draudžiantis VPN teikti prieigą prie uždraustų svetainių ir 2018 m. administracinių pažeidimų kodekso pakeitimai	2021 m. duomenų apsaugos įstatymas
2017 m. įstatymas dėl pranešimų siuntimo programų naudotojų tapatybės nustatymo	
2019 m. Interneto suverenumo įstatymas	

6 lentelė. Sudarė autorė, remiantis Data Guidance „Rusia/Cybersecurity“; „China/Cybersecurity“ ir[137][138]

[134] DataGuidance, „Russia: Cybersecurity“ *DataGuidance* (2022): 2-3.

[135] DataGuidance, „China: Cybersecurity“ *DataGuidance* (2022): 1.

[136] Ken Dai ir Jet Deng, Dentons, „China‘s Personal Information Protection Law (PIPL)“, Bloomberg Law, žiūrėta 2024 m. balandžio 4 d https://pro.bloomberglaw.com/insights/privacy/china-personal-information-protection-law-pipl-faqs/ .

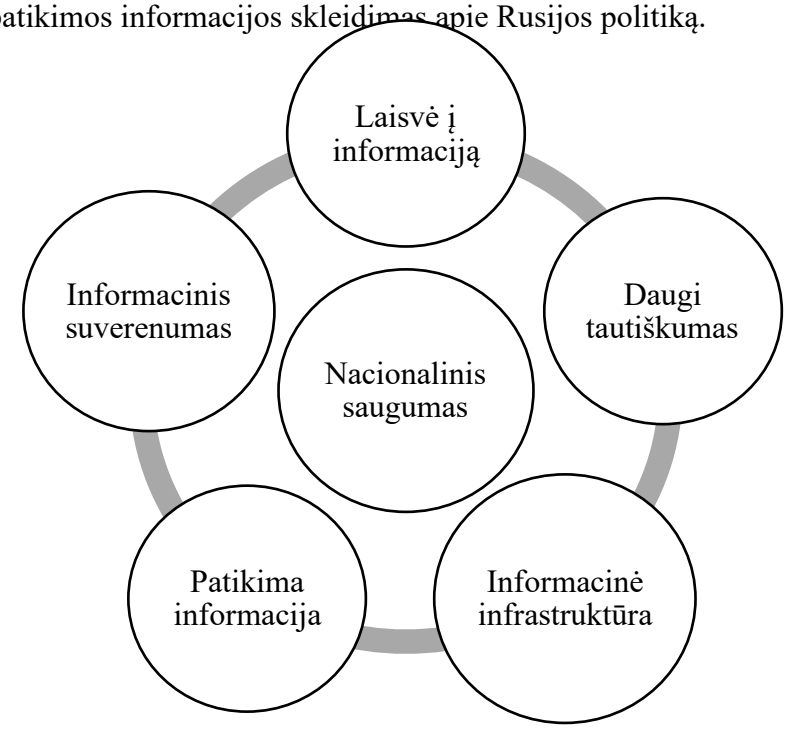
[137] Alena Epifanova, „Deciphering Russia‘s „Sovereign Internet Law““, DGAP, žiūrėta 2024 m. balandžio 5 d. https://dgap.org/en/research/publications/deciphering-russias-sovereign-internet-law .

[138] Human Rights Watch, „Russia: Growing Internet Isolation, Control, Censorship“, Human Rights Watch, žiūrėta 2024 m. balandžio 5 d. https://www.hrw.org/news/2020/06/18/russia-growing-internet-isolation-control-censorship .

Šiame darbe pasirinkta lyginti kelis įstatymus dėl to, kad šie įstatymai gali tiksliausiai atspindėti formuojamo suverenaus valstybės interneto požiūrį.

Rusijos Federacijos informacinio saugumo doktrina[139] išryškina nacionalinio saugumo užtikrinimo siekiamybę skaitmeninėje aplinkoje, taip pat aprašo Rusijos nacionalinius interesus ir grėsmes, su kuriomis ji susiduria kinetinėje erdvėje; taip pat aptariamos Rusijos kibernetinio saugumo valdymo strateginės nuostatos.[140] Doktrina – Nacionalinio saugumo koncepcijos tęsinys KE, kuri pasižymi deklaratyvumu, nes nėra pateikiama konkrečių įrankių, ką Rusija turėtų daryti, norėdama formuoti valstybės politiką, kuri užtikrintų informacinį saugumą.[141]

Nagrinėjant šią doktriną, išryškėja keli aspektai. Visų pirma, išryškinamas nacionalinis saugumas informacinėje sferoje, kurioje tarpusavyje sąveikauja informacinės sistemos, interneto svetainės, informacinių telekomunikacijų ir ryšių tinklai, IT ir subjektai, kuriantys ir apdorojantys informaciją, įskaitant jos kūrėjus, vartotojus ir reguliuojančius šio mechanizmo veiklą. Todėl išskyriau tai kaip pagrindinį šios doktrinos interesą, aplink kurį išsidėsto principai, kurie atlieka lemiamą vaidmenį įgyvendinant Rusijos Federacijos nacionalinius principus, t. y. tarptautinis bendradarbiavimas dėl informacinio suvereniteto užtikrinimo, laisvė į informacijos gavimą ir naudojimą, daugiatautiškumas ir žmonių vertybių išsaugojimas, kritinės infrastruktūros saugumo užtikrinimas ir patikimos informacijos skleidimas apie Rusijos politiką.



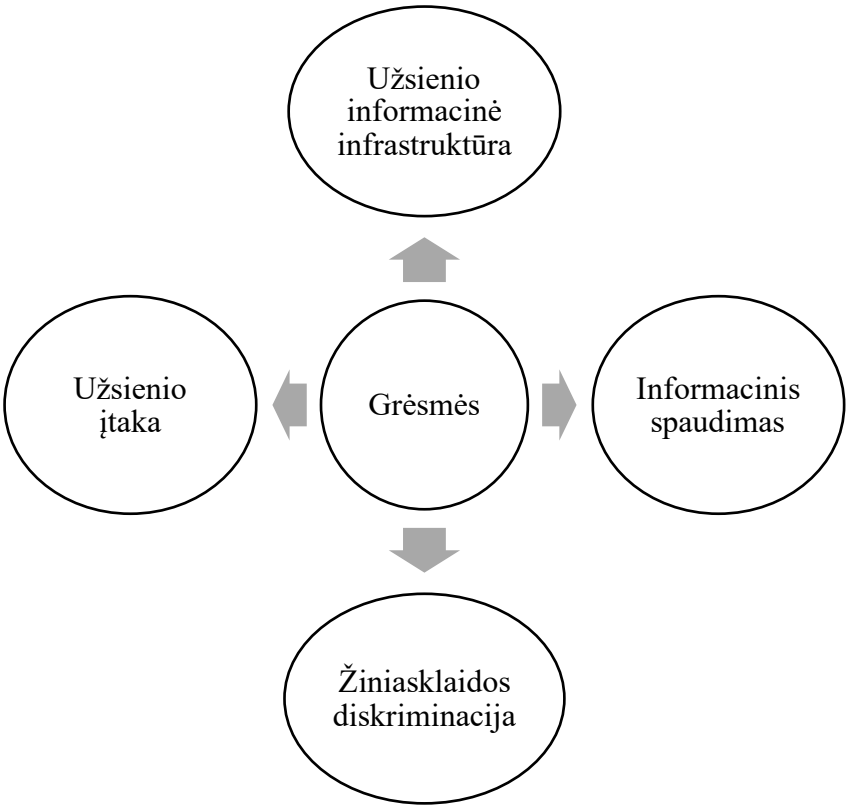
[139] Rusijos Federacija, „*Doctrine of Information Security of the Russian Federation"* Rusija, 2016, http://www.scrf.gov.ru/security/information/DIB_engl/ (žiūrėta 2024 m. balandžio 4 d.).
[140] Martti J. Kari, „Russian Strategic Culture in Cyberspace: Theory of Stratetig Culture – a tool to Explain Russia's Cyber Threat Perception and Response to Cyber Threats" (Daktaro disertacija, University of Juvaskyla, 2019), 43.
[141] Nerijus Maliukevičius, „Informacijos karas: Rusijos požiūris", Post Scriptum, žiūrėta 2024 m. balandžio 5 d. http://www.postscriptum.lt/7-karas/informacijos-karas-rusijos-poziuris .

7 lentelė. Sudarė autorė, remiantis „Doctrine of Information Security of the Russian Fedearation“ (2016)

Trečioje doktrinos dalyje aptariamos pagrindinės informacinės grėsmės, su kuriomis susiduria Rusijos valstybė kibernetinėje erdvėje. Joje pabrėžiama užsienio įtaka, įvardijama kaip viena pagrindinių grėsmių siekiant paveikti informacinę infrastruktūrą ne tik kariniams tikslams, bet ir, anot Rusijos, formuojant informacinį naratyvą skirtą žlugdyti Rusiją. „*Tam tikrų valstybių žvalgybos tarnybos vis dažniau naudoja informacines ir psichologines priemones, siekdamos destabilizuoti vidaus politinę ir socialinę situaciją įvairiuose pasaulio regionuose, menkindamos suverenitetą ir pažeisdamos kitų valstybių teritorinį vientisumą. [...]informacinės technologijos yra plačiai naudojamos siekiant šio tikslo. Užsienio žiniasklaidoje pastebima tendencija publikuoti vis daugiau medžiagos, kurioje yra netikslingai vertinama Rusijos Federacijos valstybės politika*.“ Todėl nurodoma, kad informacinis saugumo užtikrinimo tikslas – apsaugoti asmens, visuomenės ir valstybės interesus nuo vidinių ir išorinių grėsmių.[142] Vilkinas teigia, kad doktrinoje plėtojami puolamieji veiksniai formuojant galią per „veidrodinį reiškinį“, nes užsienio valstybės įvardijamos kaip agresoriai, nusitaikę prieš Rusiją, tuo tarpu pati Rusija, formuodama puolamuosius taikinius, pati taiko doktrinoje paminėtus objektus.[143] Galima teigti, kad doktrinos pagrindinis interesas yra sprendimų priėmimo dėl blokuojamų domenų pateisinimas taip siekiant apibrėžti užsienio grėsmę kaip pagrindinį subjektą KE, dėl ko skaitmeninė aplinka tampa kontroliuojama ir dėl ko galiausiai formuojamas suverenus valstybės internetas.

[142] Rusijos Federacija, „*Doctrine of Information Security of the Russian Federation“* Rusija, 2016, http://www.scrf.gov.ru/security/information/DIB_engl/ (žiūrėta 2024 m. balandžio 4 d.)

[143] Mjr. Statys Vilkinas, „Išmanioji galia – rusų kalbos naudojimas, stiprinant Rusijos Federacijos galią“ *Šiuolaikinės visuomenės ugdymo veiksniai* 2 (2017): 183-184.



8 lentelė. Sudarė autorė, remiantis „Doctrine of Information Security of the Russian Fedearation“ (2016)

Svarbiausias Rusijos įstatymas, kuris kalba apie suverenų valstybės internetą, yra 2019 m. įsigaliojęs Rusijos Federalinis įstatymas „Apie informacijos apsaugą ir IT“, žinomas kaip „suverenaus interneto“ įstatymas, kurio tikslas – užtikrinti ilgalaikį ir stabilų interneto tinklo veikimą Rusijoje ir padidinti Rusijos interneto išteklių patikimumą atsižvelgiant į JAV nacionalinės kibernetinės saugumo strategijos agresyvumą. Suverenus interneto įstatymas įvedė naujas priemones interneto kontrolei Rusijos teritorijoje, įskaitant reikalavimus ryšio operatoriams įdiegti technines priemones, kurios yra skirtos atremti grėsmes interneto stabilumui, saugumui ir vientisumui.[144] Įstatyme pabrėžiama Federalinės ryšių, IT priežiūros tarnybos ir masinės komunikacijos Roskomnadzor atsakomybė, t. y. atlikti nurodytus veiksmus, kurių esmė yra užtikrinti Rusijos interneto stabilų, saugų ir vientisą veikimą, atgrasantiš užsienio kylančią grėsmę nacionaliniam KE saugumui, o prireikus atjungti internetą nuo pasaulinio tinklo:[145] „*Kilus grėsmei Rusijos Federacijos teritorijoje esančio interneto informacinio ir telekomunikacijų tinklo ir viešųjų ryšių tinklo veikimo stabilumui, saugumui ir vientisumui, viešųjų ryšių tinklas gali būti centralizuotai valdomas federalinės vykdomosios valdžios institucijos... .*“[146] Kita vertus, įstatymo pagrindinis tikslas tampa

[144] Veni Markovski ir Alexey Trepykhalin, „Отчет о ситуации в стране: законы Российской Федерации в области интернета и участие в прениях в ООН“ ICANN, GE-006, (2021): 12-13.
[145] *Ibid*, 12-15.
[146] Rusijos Federacijos Vyriausybė, *Federal Law of May 1, 2019 N 90-FZ "On Amendments to the Federal Law "On Communications" and the Federal Law "On Information, Information Technologies and Information Protection*. Rusija, 2019, https://rg.ru/documents/2019/05/07/fz90-dok.html (žiūrėta 2024 m. balandžio 6 d.).

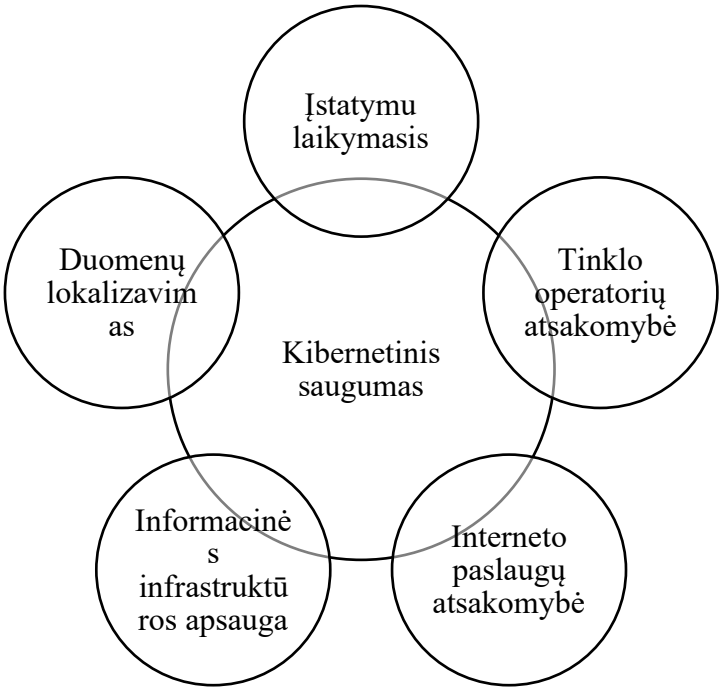
tarsi pateisinimu dėl prieš tai jau minėtos doktrinos, o grėsmė iš esmės apibrėžiama ta pati, t. y. JAV.iuo atveju, sukuriamas pateisinimas esant būtinybei visiškai atjungti internetą nuo pasaulinio tinklo.

Tuo tarpu 2016 m. Kinijos kibernetinio saugumo įstatymas siekia sustiprinti KE valdymą pateikiant keletą iniciatyvų, t. y. interneto tiekėjų saugumą, asmeninę informaciją, taip pat pabrėžiant ypatingą apsaugą kritinės informacijos infrastruktūrai, duomenų lokalizavimą ir duomenų eksporto saugumo vertinimą ir vyriausybės reguliavimą kibernetinio saugumo srityje. Pabrėžiama, jog šis įstatymas atspindi Kinijos politikos ypatybes ir yra grindžiamas Kinijos suverenaus valstybės interneto koncepcija, iškeliant duomenų saugumą kaip svarbesnį objektą nei laisvą interneto srautą ir žodžio laisvę. Šis įstatymas yra laikomas pagrindiniu dokumentu Kinijos KE valdyme, kuris ateityje galimai bus tik pildomas įgyvendinimo reglamentais.[147] Dėl šių priežasčių galima teigti, kad šis įstatymas, taip pat, kaip ir Rusijos atveju, tampa tarsi pasiteisinimas dėl laisvo interneto, turint omenyje tai, kad pagrindinis įstatymo tikslas – duomenų apsauga, o norint ją turėti, reikia kurti suverenų valstybės internetą ir atitolti nuo pasaulinio tinklo.

Teigiama, kad šis įstatymas parengtas siekiant garantuoti kibernetinį saugumą ir apsaugoti KE suverenitetą, nacionalinį saugumą ir viešąjį interesą, ginti piliečių, juridinių asmenų ir kitų organizacijų teises ir interesus,skatinti patikimą ekonominės ir socialinės informatizacijos plėtrą. Todėl tai išskyriau kaip pagrindinį šio įstatymo objektą, apie kurį išdėstyti reikalavimai ir intereso siekimo principai, apimantys įstatymą ir įstatyme įvardintus subjektus.

Pastebima, kad įstatyme pabrėžiamas ne tik valstybės vaidmuo: „*Kiekvienas internetu besinaudojantis asmuo ar organizacija privalo laikytis Konstitucijos ir įstatymų, laikytis viešosios tvarkos ir gerbti socialinę moralę, nekelti pavojaus kibernetiniam saugumui ir nesinaudoti internetu veiklai, kuri kelia pavojų nacionaliniam saugumui, garbei ir interesams ir skatina griauti valstybės valdžią ar griauna socialistinę santvarką, kursto skaldyti šalį ar suskaldyti tautinę vienybę, propaguoja terorizmą ar ekstremizmą, propaguoja etninę neapykantą ar diskriminaciją, skleidžia smurtinę ar pornografinę informaciją, sugalvoja ir skleidžia melagingą informaciją siekiant sutrikdyti ekonominę ir socialinę tvarką, arba pažeidžia bet kurio kito asmens reputaciją, privatumą, intelektinės nuosavybės teises ar kitas teises ir interesus*.“ Tad šiuo atveju svarbus ir griežtas tonas atsispindi atsakomybėje, kuri apima ne tik valstybę, tinklo operatorius, interneto paslaugų tiekėjus, bet ir pačius interneto vartotojus, kurie yra įpareigoti laikytis šio įstatymo nustatytų funkcijų, t. y. nacionalinis interneto saugumas šiuo atveju tampa valstybės, verslo ir piliečių atsakomybė.

[147] Aimin Qi, Guosong Shao, Wentong Zheng, „Assesing China‘s Cybersecurity Law, *Elsevier* 34 (2018): 1353-1354.



9 lentelė. Sudarė autorė, remiantis „Cybersecurity Law of the People's Republic of China". (2016)

Remiantis įstatymais ir Rusijos doktrina, galima išskirti skirtumus ir panašumus tarp Rusijos ir Kinijos KE valdymo ypatumų:

	Kinija	**Rusija**
Skirtumai	Įstatymas kur kas detalesnis, apimantis duomenų apsaugos, interneto tinklo saugumo ir kibernetinių incidentų temas.	Deklaratyvus strateginis dokumentas, apibrėžiantis bendras gaires ir principus.
	Įstatymas griežtesnis. Nurodomi aiškūs reikalavimai įmonėms, organizacijoms ir interneto vartotojams.	Pabrėžiamas valstybės vaidmuo, nėra nurodymų įmonėms ir organizacijoms.
	Įstatymas orientuotas į vidaus kontrolę ir reguliavimą.	Įstatymas orientuotas į iš užsienio kylančias grėsmes, susijusias su tarptautiniais kibernetinio saugumo aspektais.
	Formuojama duomenų lokalizavimo politika.	Neapibrėžiamas duomenų lokalizavimo būtinumas.
	Kinija ir Rusija	
Panašumai	Abiejų šalių pagrindinis interesas - nacionalinis saugumas ir informacijos suverenumas.	
	Pabrėžiamas valstybės vaidmuo reguliuojant ir kontroliuojant kibernetinę erdvę, ypač kritinės infrastruktūros ir informacinės sistemos kontekste.	
	Pabrėžiamas kibernetinis suverenitetas	

10 lentelė. Sudarė autorė, remiantis Kinijos ir Rusijos minėtais įstatymais.

Atsižvelgiant į Rusijos ir Kinijos pagrindinius įstatymus dėl suverenaus valstybės interneto formavimo galima teigti, kad abu įstatymai turi tą patį interesą, t. y. kibernetinį suverenitetą nacionalinių lygmeniu ir ypatingos svarbos informacinės ir kritinės infrastruktūros saugumo užtikrinimą. Taip pat pabrėžiamas abiejų šalių vaidmuo užtikrinant kritinės infrastruktūros saugumą, akcentuojant kibernetinį suverenumą. Svarbu tai, kad Kinijos įstatymas yra išsamus, kur kas detalesnis ir griežtesnis, nukreiptais tiek į verslo sektorių, tiek į piliečius, akcentuojant būtinybę laikytis įstatyme įtvirtintų principų. Tuo tarpu Rusijos doktrina turi švelnesnį toną, nors akivaizdžiai yra orientuota į išorės grėsmes, ypač atsižvelgiant į JAV įtaką. Nepaisant to, dokumente trūksta aiškaus proceso aprašymo, kaip turi būti siekiama kritinės infrastruktūros apsauga. Taip pat Kinija išryškina duomenų lokalizavimo būtinybę, tuo tarpu Rusijos doktrinoje neužsimenama apie piliečių duomenų lokalizavimo reikiamybę, nors doktrina yra nukreipta prieš užsienio įtaką.

Apibendrinant, nors Kinijos ir Rusijos metodai valdant KE turi daug bendrų bruožų – pavyzdžiui, abiejų valstybių siekis užtikrinti nacionalinį kibernetinį suverenitetą ir saugoti kritinę infrastruktūrą – tyrimas atskleidžia svarbius šių metodų skirtumus, ypač žmogaus teisų kontekste. Pastarieji atskleidžia, kaip Kinija ir Rusija taiko skirtingas strategijas interneto kontroliavimo ir suverenaus valstybės interneto formavimo srityse. Šis kontrastas rodo, kaip kiekviena šalis interpretuoja ir įgyvendina kibernetinio suverenumo principus savo teisiniuose rėmuose, o tai galiausiai formuoja skirtingas pasekmes piliečių teisėms ir laisvėms.

Išvados

Ryšys tarp Rusijos ir Kinijos KE ir suverenaus interneto formavimo žmogaus teisių kontekste iš esmės yra aiškus ir neprieštaringas. Šiame tyrime buvo siekiama išsiaiškinti, kaip Rusijos ir Kinijos formuojamas suverenus valstybės internetas užtikrina žmogaus teises internete. Pasitelkiant tarptautinių režimų teoriją, darbe išsiaiškinta, kad valstybės formuoja suverenų valstybių internetą abipusiškumo principu, kuriame laikosi panašių užmojų dėl kibernetinio suverenumo, t. y. Kinija diktuoja suverenumo skaitmeninėje aplinkoje principus, tuo tarpu Rusija imasi panašios taktikos, kurios tikslas – tarptautinėje arenoje įtvirtinti interneto kontrolės normas ir priešintis demokratija ir liberalizmu paremtu interneto valdymu JAV.

Visų pirma, darbe buvo siekiama apibrėžti teorinį pagrindą, kuris padėjo išgryninti esminius bei struktūrinius darbui taikytinus principus tiriant gilesnes KE problemas, šiuo atveju žmogaus teises skaitmeninėje aplinkoje. Išsiaiškinta, kad tokios klasikinės teorijos kaip realizmas ir konstruktyvizmas neapima gilesnių KE dilemų, šiuo atveju žmogaus teisių dėl to, kad jos veikiau nagrinėja valstybės galios poziciją arba, konstruktyvizmo atveju, valstybės identitetą. Tačiau remiantis Nye nustatyta, kad KE yra inertiška tarptautinių santykių struktūros dalis, todėl pastebima, kad valstybės priimti sprendimai KE valdyme yra per lėti ir dažnu atveju neatitinka skaitmeninės aplinkos kitoniškumo, tad tampa nebeaktualūs. Tuo tarpu tarptautinių režimų teorija nagrinėja platų spektrą valstybės valdymo ypatumų, t. y. nuo principų, taisyklių, normų, iki elito priimamų veiksmų. Taip pat pastaroji teorija pasikliaunama nagrinėjant fundamentalias kinetinės erdvės problemas todėl, kad KE valdymo struktūra sudaryta iš konstruktyvaus valdymo turint omenyje tai, kad skaitmeninės aplinkos valdymo procesuose dalyvauja tokie subjektai kaip valstybė, privatus verslas ir interneto vartotojai. Dėl šios priežasties galima daryti prielaidą, jog tarptautinių režimų teorija yra geriausias įrankis, padedantis aiškintis suverenų valstybių internetą žmogaus teisių kontekste.

Siekiant apsibrėžti suverenaus valstybės interneto sampratą, išanalizuotas interneto susiskaldymo fenomenas, kuris apima platų tarptautinių santykių lauką ir kelia geopolitinį iššūkį. Pastebėta, kad interneto susiskaldymas nebūtinai turi apimti tik geopolitinį JAV ir Kinijos interneto valdymo skirtumo problematiką. Tačiau, remiantis analizės rezultatais, prieinama išvada, kad interneto susiskaldymas gali apimti kiekvieną valstybę darant prielaidą, kad valstybės dėl interneto ir KE laikosi skirtingų požiūrių, kas lemia priimamus įvairialypius, tarptautiniu mastu nesuderintus teisės aktus ar sprendimus. Šiuo atveju išryškėja skirtingas valstybių požiūris į duomenų saugumą, turinio cenzūravimą, socialinių tinklų politiką ir veikimo principą bei interneto teisių suvaržymus, tokius kaip interneto atjungimas. Todėl galima daryti išvadą, kad interneto skilimas vyksta ne tik dėl skirtingo valstybės identiteto KE atžvilgiu, bet taip pat todėl, kad KE tampa tarsi nacionalinis objektas, kurį valstybės formuoja pagal savo politines vertybes ir socialinį identitetą. Interneto skilimo koncepcijos apibrėžimas savaime padėjo išsiaiškinti suverenaus valstybės interneto sampratą.

Šiuo atveju prieita išvada, kad suverenus valstybės internetas yra dinamiškas ir, priklausomai nuo valstybės lūkesčių ir politikos strategijos, gali būti skirtingas. Dėl šios priežasties, norint geriau suprasti, į kokias konstruktyvias detales šalys atsižvelgia kontroliuojant internetą ir formuojant suverenumą KE, svarbu apibrėžti konkrečios ar keleto valstybių atvejus. Todėl galima teigti, kad interneto skilimas savaime irgi yra įtakojamas skaitmeninio suverenumo, bet pats suverenitetas kiekvienos valstybės atveju gali būti traktuojamas skirtingai. Remiantis šiuo faktu daroma prielaida, kad geopolitiškai kibernetinis suverenumas yra dinamiška sąvoka, kuri negali būti taikytina visoms suverenų internetą formuojančioms valstybėms bendrai. Dėl to sąvoka turi būti apibrėžta kiekvienai valstybei atskirai.

Suverenus valstybių interneto ryšys su antidemokratiškomis, autoritarinę ideologiją palaikančiomis valstybėmis yra tiesioginis, todėl galime daryti prielaidą, kad jis savaime asocijuojasi su žmogaus teisių pažeidimais. Žmogaus teisių užtikrinimas skaitmeninėje aplinkoje – taip pat, kaip ir interneto susiskaldymas – kelia ne tik iššūkius valstybės vidaus valdyme ir užtikrinat piliečių teises, bet ir lemia geopolitinius sunkumus, kadangi KE neturi konkrečios, tarptautiniu mastu priimtos reglamentacijos dėl žmogaus teisių užtikrinimo. Vis dėlto reikia pabrėžti, kad tam tikros normos yra pateiktos ir aprašytos, tačiau jos nėra tiesiogiai priimtos tarptautiniu mastu, kaip, pavyzdžiui, visuotinė žmogaus teisių chartija. Kita vertus, ITPK bukletą ir „Interneto ateities deklaraciją“ galima interpretuoti kaip žmogaus teisių internete visuotinę paradigmą, kuri suteikia galimybę suprasti, kokios žmogaus teisės internete jau egzistuoja. Galima daryti prielaidą, kad šie principai taps pamatiniais Jungtinėms Tautoms kuriant visuotinį, tarptautiniu mastu priimtiną žmogaus teisių kodeksą KE. Kol kas, išsiaiškinus žmogaus teisių probleminį konceptą skaitmeninėje erdvėje, galima daryti išvadą, kad KE žmogaus teisių atžvilgiu šiandien yra reikšminga ir problematiška sritis, kuri tarptautiniuose santykiuose kelia nemažai iššūkių ir yra plačiai kvestionuojama.

Atsižvelgiant į darbe atliktą Kinijos ir Rusijos suverenaus interneto empirinę analizę, galima daryti išvadą, kad abi strategijos iš esmės turi panašumų. Tie panašumai kyla iš to, kad abi valstybės palaiko panašią politinę ideologiją, kuria tarpvalstybinį bendradarbiavimą ir turi vienodą požiūrį į KE saugumą. Valstybėse pastebėta tolygi KE strategijos taktika šiais klausimais: VPN reglamentacija ir asmeninė registracija naudojantis internetu, cenzūra, turinio filtravimas, užsienio ir vietinių domenų ir komentarų blokavimas ir pan. Nors abi šalys yra linkusios į interneto išjungimą, Rusijoje tai vyksta nuo 2024 m. ir per jautrius politinius įvykius, tokius kaip prezidento rinkimai, Rusijos opozicijos lyderio Navalno laidotuvės. Tarpu Kinijoje matoma akivaizdi Xinjiang regiono ir joje gyvenančių uigūrų diskreditacija, kurioje užfiksuoti interneto atjungimai apima kur kas ilgesnį laikotarpį. Dar daugiau, Rusijos įstatymų tematika iš esmės yra nukreipta į iš užsienio kylančią grėsmę, t. y. JAV, neapibrėžiant jokių konkrečių veiksmų, kurių bus imtasi tam, kad būtų užtikrintas KE suverenumas. Tuo tarpu Kinijos įstatymai turi griežtą toną, nukreiptą į visus, kurie turi bet kokias sąsajas su

internetu, įskaitant pačius vartotojus. Tai parodo, kad Kinijos KE įstatymai ir skaitmeninis savarankiškumas veikiau nukreiptas į vidinį šalies procesą, primetantį svarbias atsakomybes dėl nurodytų teisės aktų laikymosi. Galima daryti prielaidą, kad Kinija šiuo atveju turi daugiau patirties formuojant skaitmeninę nepriklausomybę dėl to, kad tai yra pirmoji šalis, kuri apskritai į tarptautinių santykių diskursą įvedė KE suverenumo sampratą, o Rusija tėra Kinijos pasekėja ir kol kas dar neturi konkrečių veiksmų, kuriais pasiektų interneto nepriklausomybę be Kremliaus staigių sprendimų atjungti internetą, ką leidžia vykdyti Rusijos KE suverenumo įstatymas.

Vertinant Kinijos ir Rusijos suverenaus valstybės interneto strategijų įtaką žmogaus teisėms galima teigti, kad skaitmeninė nepriklausomybė šių šalių kontekste apima reikšmingą sąsają ir poveikį žmogaus teisėms KE. Šalyse yra pažeidžiamos žmogaus teisės į žodžio laisvę, informacijos gavimą, kūrimo ir dalijimosi galimybes, o precedento neturintys fiziniai veiksniai prieš asmenis už jų veiklą internete aiškiai parodo, kad šiose valstybėse skaitmeninis suverenitetas neatitinka daugelio žmogaus teisių principo. Be to, galima daryti išvadą, kad Kinija ir Rusija ne tik siekia atskirties nuo Vakarų laisvo interneto kibernetinės erdvės ideologijos, bet ir formuojama politika gali būti traktuojama, kaip režimo doktrina, kuria siekiama įteisinti autoritarinio režimo interesą kibernetinės erdvės veikimo principuose. Taip pat, galima daryti prielaidą, kad Kinijos režimo doktrinos interesas yra vidiniai, tuo tarpu Rusija siekia geopolitinio susiskaldymo kibernetinės erdvės atžvilgiu, viešai tai deklaruodama.

Literatūros sąrašas

1. A Liaropoulos, „Exercising State Sovereignty in Cyberspace: An International Cyber-Order under Construction?“ *Journal of Information Warfare* 12, No. 2 (2013): 23.

2. Adam Segal, „China‘s Alternative Cyber Governance Regime, *Council on Foreign Relations* (2020): 3.

3. Aimin Qi, Guosong Shao, Wentong Zheng, „Assesing China‘s Cybersecurity Law, *Elsevier* 34 (2018): 1353-1354.

4. Alexandra V. Orlova, „“Digital Sovereignty“ Anonimity and Freedom of Expression: Russia‘s Fight to Re-Shape Internet Governance 26, No. 2 (pavasaris 2020): 246-247.

5. Anna Litvinenko, „Re-Defining Borders Online: Russia‘s Strategic Narrative on Internet Sovereignty“, *Media and Communications* 9, No. 4 (2021): 5-15.

6. Anqi Wang, „Cyber Sovereignty as Its Boldest: A Chinese Perspective“ *Ohio State Technology Law Journal* 16, No. 2 (2020).

7. Antonio Guterres, „The Highest Aspiration: A Call to Action for Human Rights“, United, Nations, (2020): 8.

8. Begum Burak, „Human Rights Violations in Cyberspace: Internet Censorship and Online Surveillance in Turkey“ *Cyberpolitik Journal* 6, No. 12 (2022): 205.

9. Benjamin J. Cohen, *International Political Economy: An Intelectual History* (New Jersay: Princeton University Press, 2008), 68.

10. Charles Grant, *Russiam China and Global Governence* (London, Centre of European Reform, 2012), i.

11. Clement Perarnaud et al., „‘Splinternets‘: Addressing the renewed debate on internet fragmentation“ *European Parliamentary Research Service* PE 729.530, (2022): 1-3.

12. Cornelia Bogen, „Overcoming Modernity? How China‘s Splinternet Reinforces the Impact of Geography in Global Internet Governance“ Navigationen - Zeitschrift für Medien- und Kulturwissenschaften 23, No.2 (2023): 130.

13. Danielle Flonk, Markus Jachtenfuchs ir Anke S. Obendiek, „Authority conflicts in internet governance: Liberals vs. Sovereigntists“ *Cambridge University Press* 9, No.2, (2020): 365.

14. David P. Fidler, „Cyberspace and human rights“, Elgar Online, (2018): 111.

15. Dmitri Alperovitch, „The Case for Cyber-Realism: Geopolitical Problems Don‘t Have Technical Solutions“ *Foreign Affairs* 101, No.1, (2022): 48.

16. Elisa Bertolini, „Internet Governance and Terrorism in the Context of the Chinese Compression of Fundamental Rights and Freedoms“ *Global Jurist* (2028): 1-17.

17. Erik Allerson, „International Censorhsip in Russia: The Sovereign Internet Laws and Russia‘s Obligations under the European Convention on Human Rights“, *Minnesota Journal of International Laws* 31, No.1 (Pavasaris 2022): 233-258.

18. Hao Yeli, „A Three-Perspective Theory of Cyber Sovereignty“ *Institute for National Strategic Security, National Defence University* 7, No.2 (2017): 112-114.

19. Hidetaka Yoshimatsu, „International Regimes, International Society, and Theoretical Relations“ *The International Centre for the Study of East Asian Development, Kitakyushu* 98, No.10 (1998): 12.

20. Ian Hosein ir Johan Eriksson, „International policy dynamics and the regulation of dataflows: bypassing domestic restrictions“ kn. *International Relations and Security in the Digital Age* sud. Johan Eriksson ir Giampriero Giacomello (New York: Routledge, 2007), 157.

21. Ilona Stadnik, „Russia: An Independent and sovereign internet?“, kn. *Power and Authority in Internet Governance: Return of the State?* ed., Blayne Haggart, Natasha Tusikov ir Jan Aart Scholte (New York: Routledge), 186-205.

22. Internet Society, „Navigating Digital Sovereignty and Its Impact on the Internet:, Internet Society, (2022): 5.

23. Jessica Chen Weiss ir Jeremy L. Wallace, „Domestic Politics, China’s Rise, and the Future of Liberal International Order”*International Organization* 75, (2021): 635-664.

24. Jia Lianrui, „Building China‘s tech superpower: State, domestic champions and foreign capital“, kn. *Power and Authority in Internet Governance: Return of the State?* ed., Blayne Haggart, Natasha Tusikov ir Jan Aart Scholte (New York: Routledge), pilnas tekstas 126-147.

25. Jinghan Zeng, Tim Stevens ir Yaru Chen, „China‘s Solution to Global Vyber Governance: Unpacking the Domestic Discourse of „Internet Sovereignty““, *Politics & Policy,* 45, No.3 (2017): 434.

26. John P. Barlow, *A Declaration of the Independence of Cyberspace,* Editions-hache, 1996.

27. Joseph S. Nye, „The Regime Complex for Managing Global Cyber Activities“ *Centre for International Governance Innovation and the Royal Institute for International Affairs* No.1 (2014): 11-12.

28. Julien Nocetti, „Contest and conquest: Russia and global internet governance“ *International Affairs* 91, No. 1 (2015): 111-130.

29. Justin Sherman, „Chinese and Russian Efforts to Undermine the Global Internet“ *Fletcher Security Review,* (2023): 22.

30. Kieran Green et al. „Censhorship Practices of the People‘s Republic of China“ (Exovera‘s Center for Intelligence Research and Analysis, 2024): 2-3.

31. Laura Denardis, *The Global War for Internet Governance* (New Haven and London: Yale University Press, 2014), 226.

32. Lorenzo Valeri, „Public-private cooperation and information accurance: a liberal institutionalist approach“kn. *International Relations and Security in the Digital Age* sud. Johan Eriksson ir Giampriero Giacomello (New York: Routledge, 2007), 137–142.

33. Madeline Carr, „Internet freedom, human rights and power“ *Australian Journal of International Affairs* 67, No. 5 (2013): 623.

34. Mark A. Lemley, „The Splinternet“ *Stanfort Law and Economics Olin Working Paper* 555 (2021).

35. Martti J. Kari, „Russian Strategic Culture in Cyberspace: Theory of Stratetig Culture – a tool to Explain Russia‘s Cyber Threat Perception and Response to Cyber Threats“ (Daktaro disertacija, University of Juvaskyla, 2019), 43.

36. Milton L. Mueller, „China and Global Internet Governance“, kn. *Access Contested: Security, Identity, and Resistance in Asian Cyberspace“* ed., Ronald John et al. (Cambridge: The Mit Press, 2012), 181.

37. Min Jiang, „Chinese Internet Business and Human Rights, *Business and Human Rights Journal* 1 (2015): 139-144.

38. Mjr. Statys Vilkinas, „Išmanioji galia – rusų kalbos naudojimas, stiprinant Rusijos Federacijos galią“ *Šiuolaikinės visuomenės ugdymo veiksniai* 2 (2017): 183-184.

39. Nazli Choucri, *Cyberpolitics in International Relations* (Lodong: The MIT Press, 2012),13.

40. Oran R. Young, *International Cooperation: Building Regimes for Natural Resources and the Environment* (New York: Cornell University Press (1989): 12-15.

41. Ovgu Kalkan Kucuksolak, „Cyberspace: The Fifth Domain of Escalating Security Challenges, „*International Relations & Law* 24, No.15, (2018): 25.

42. P. W. Singer ir Allan Friedman, *Cybersecurity and Cyberwar what Everyone needs to know* (New York: Oxford University Press, 2014),176.

43. Rika Isnarti, „A Comparison of Neorealism, Liberalism, and Constructivism in Analysing Cyber War“ *Andalas Journal of International Studies* 5, No. 2, (2016): 159-161.

44. Ronald J. Deibert ir Louis W. Pauly „Mutual Entanglement and Complex Sovereignty in Cyperspace“ kn. *Data Politics: Worlds, Subjects, Rights*, ed. Didier Bigo et al. (New York: Routledge, 2019), 95-86.

45. Samson Yuen, „Becoming a Cyber Power: China‘s cybersecurity upgrade and its consequences“*OpenEdition* Journals (2015): 58.

46. Samuele Dominioni, „Internet Fragmentation and Cybersecurity“, The United Nations Institute for Disarmament Research, (2023): 12.

47. Scott Malcomson, *Splinternet: How Geopolitics and Commerce are Fragmenting the World Wide Web* (Indija: AarkMany Media, 2016), 112.

48. Shahad A. Alashi ir Hanaa A. Aldahawi, „Cybersecurity Management for Virtual Private Network (VPN) Applications: A Proposed Framework for the Governance of their USe in the Kingdom of Saudi Arabia“, *Journal of Information Security* 1, No. 1 (2020): 36.

49. Simon K. Zhen, „Combating Censorship in China: Forcing China‘s Hand through the WTO and Collective Action:, *Cornell International Law Journal* 53, No. 4 (žiema 202): 731-798.

50. *Special Rapporteur‘s Report* (n 17); *Freedom House* (n 20); *Freedom House* (n 22) cituota iš David P. Fidler, „Cyberspace and human rights“ *Elgar Online* (2018): 102.

51. Stacie Hoffmann et. al., „Standardising the splinternet: how China‘s technical standarts could fragment the internet“ *Journal of Cyber Policy,* 5, No.2 (2020): 239.

52. Stephen D. Krasner, „Structural causes and regime consequences: regimes as intervening variables: kn. *International regimes*, ed. Stephen D. Krasner (New York: Cornell University Press, 1983): 2-3.

53. Timothy S. Wu, „Cyberspace Sovereignty? – The Internet and the International System“ Harvard Journal of Law & Technology 10, No. 3 (1997): 648-666.

54. Veni Markovski ir Alexey Trepykhalin, „Отчет о ситуации в стране: законы Российской Федерации в области интернета и участие в прениях в ООН“ ICANN, GE-006, (2021): 12-13.

55. William J. Drake, Vinton G. Cerf ir Wolfgang Kleinwachter, „Future of the Internet Initiative White Paper: Internet Fragmentation: An Overview“, *World Economic Forum*, (2016): 7-8.

56. Xui Li ir Xin Yang, Co-governed Sovereignty Network: Legal Basis and Its Prototype & Applications with MIN Architecture (Singapore: The Springer, 2021), XI.

Žiniasklaidos šaltiniai

1. Adam Satariano et al., „Rusia Strengthens Its Internet Controls in Critical Year of Putin“, The New York Times, žiūrėta 2024 m. balandžio 15 d. https://www.nytimes.com/2024/03/15/technology/russia-internet-censors-vladimir-putin.html .

2. Alena Epifanova, „Deciphering Russia‘s „Sovereign Internet Law““, DGAP, žiūrėta 2024 m. balandžio 5 d. https://dgap.org/en/research/publications/deciphering-russias-sovereign-internet-law .

3. Anton Kuznetsov, „From March 1, Roskomnadzor will block advertising of VPN services on the network“ tass.ru žiūrėta 2024 m. balandžio 2 d. https://tass.ru/obschestvo/20124281.

4. Article19, „Sovereign Internet Networks and Net Neutrality“, Article19, žiūrėta 2024 m. kovo 24 d. https://www.article19.org/reader/global-expression-report-2018-19/global-analysis/global-analysis-2/digital/sovereign-internet-networks-and-net-neutrality/ .

5. BBC News, „China blocks virtual private network use“ BBC, žiūrėta 2024 m. balandžio 12 d. https://www.bbc.com/news/technology-30982198 .

6. Clyde Wayne Crews, „One Internet Is Not Enough“, Cato Institute, žiūrėta 2024 m. kovo 1 d. https://www.cato.org/techknowledge/one-internet-not-enough .

7. Dakota Cary, „Community watch: China‘s vision for the future of the internet“, Atlantic Council, žiūrėta 2024 m. kovo 4 d., https://www.atlanticcouncil.org/in-depth-research-reports/report/community-watch-chinas-vision-for-the-future-of-the-internet/ .

8. Deborah Brown, „It‘s Time to Treat Cybersecurity as a Human Rights Issue“, Human Rights Watch, žiūrėta 2024 m. kovo 31 d. https://www.hrw.org/news/2020/05/26/its-time-treat-cybersecurity-human-rights-issue .

9. Deborah Lynn Blumberg, „3 ways the ‚splinternet‘is damaging society“, Management Sloan School, žiūrėta 2024 vasario 25 d., https://mitsloan.mit.edu/ideas-made-to-matter/3-ways-splinternet-damaging-society .

10. Elaine Korzak, „Have Russia and China Signed a Cyber Nonaggression Pact“, The Diplomat, žiūrėta 2024 m. kovo 4 d., https://thediplomat.com/2015/08/have-russia-and-china-signed-a-cyber-nonaggression-pact/ .

11. Elizabeth C. Economy, „The great firewall of China: Xi Jinping‘s internet shutdown“, The Guardian, žiūrėta 2024 m. vasario 25 d.,https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown .

12. European Centre for Democracy and Human Rights, „In the shadow of the Burj Khalifa: the case of Ahmed Mansoor and the whitewashing of the United Arab Emirates, European Centre for Democracy and Human Rights, žiūrėta 2024 m. kovo 31 d. https://www.ecdhr.org/?p=1650 .

13. Evgeny Morozov, „Freedom.gov: Why Washington‘s support for online democracy is the worst thing ever to happen to the Internet“, Foreign Policy, žiūrėta 2024 m. kovo 23 d.https://web.archive.org/web/20110913073036/http://www.foreignpolicy.com/articles/2011/01/02/freedomgov?page=0,1 .

14. George Qi, „China Finalizes Data Security Law“, Greenberg Traurig, žiūrėta 2024 m. kovo 20 d. https://www.gtlaw.com/en/insights/2021/7/china-finalizes-data-security-law .

15. Human Rights Watch, „Russia: Growing Internet Isolation, Control, Censorship“, Human Rights Watch, žiūrėta 2024 m. balandžio 5 d. https://www.hrw.org/news/2020/06/18/russia-growing-internet-isolation-control-censorship .

16. Issie Lapowsky, „California Unanimously Passes Historic Privacy Bill“, WIRED, žiūrėta 2024 m. vasario 27 d. https://www.wired.com/story/california-unanimously-passes-historic-privacy-bill/ .

17. James Griffiths, „Blocking social media would be ‚the end of the open internet of Hong Kong‘. It also wouldn‘t work“, CNN, žiūrėta 2024 m. kovo 28 d. https://edition.cnn.com/2019/08/29/tech/hong-kong-internet-block-emergency-powers-intl-hnk/index.html .

18. Justin Sherman, „Russia is weaponizing its data laws against foreign organizations“, The Brooking Institution, 2024 m. kovo 21 d. https://www.brookings.edu/articles/russia-is-weaponizing-its-data-laws-against-foreign-organizations/ .

19. Katitza Rodriguez ir Hilal Temel, „Turkey Doubles Down on Violations of Digital Privacy and Free Expression, „Electronic Frontier Foundation, žiūrėta 2024 m. kovo 28 d. https://www.eff.org/deeplinks/2020/11/turkey-doubles-down-violations-digital-privacy-and-free-expression .

20. Ken Dai ir Jet Deng, Dentons, „China‘s Personal Information Protection Law (PIPL)“, Bloomberg Law, žiūrėta 2024 m. balandžio 4 d https://pro.bloomberglaw.com/insights/privacy/china-personal-information-protection-law-pipl-faqs/ .

21. Li Yuan, „A Generation Grows up in China Without Google, Facebook or Twitter“, The New York Times, žiūrėta 2024 m. kovo 26 d. https://ir.westcliff.edu/wp-content/uploads/2018/08/A-Generation-Grows-Up-in-China-Without-Google-Facebook-or-Twitter.pdf .

22. Lietuvos nacionalinis radijas ir televizija, „JAV siekia uždrausti „TikTok“: kaip tai atsilieps Europai?“„ LRT, žiūrėta 2024 m. kovo 23 d. https://www.lrt.lt/naujienos/mokslas-ir-it/11/2225454/jav-siekiama-uzdrausti-tiktok-kaip-tai-atsilieps-europai .

23. Lietuvos nacionalinis radijas ir televizija, „Kinijos valdžia blokuoja užsienio žiniasklaidos portalus, kurių žurnalistai dirba šalyje“, LRT, žiūrėta 2024 m. vasario 25 d.,https://www.lrt.lt/naujienos/pasaulyje/6/1109130/kinijos-valdzia-blokuoja-uzsienio-ziniasklaidos-portalus-kuriu-zurnalistai-dirba-salyje .

24. Lietuvos rytas, ,,Leidžiasi skaitmeninė Geležinė uždanga: Rusijos internetas netrukus gali tapti panašus į Kinijos internetą“, Lrytas, žiūrėta 2024 m. vasario 24 d.,https://www.lrytas.lt/it/ismanyk/2022/03/08/news/leidziasi-skaitmenine-gelezine-uzdanga-rusijos-internetas-netrukus-gali-tapti-panasus-i-kinijos-interneta-22650678#google_vignette .

25. Meduza, ,,Russia may block Wikipedia due to article on VPNs that help reach blocked sites, says lawmaker“ MEDUZA, žiūrėta 2024 m. balandžio 2 d. https://meduza.io/en/news/2024/03/03/russia-may-block-wikipedia-due-to-article-on-vpns-that-help-reach-blocked-sites-says-lawmaker .

26. Meduza, ,,The State Duma introduced fines for violation of the law on anonymizers“ MEDUZA 2024 m. balandžio 10 d. https://meduza.io/news/2018/06/05/gosduma-vvela-shtrafy-za-narushenie-zakona-ob-anonimayzerah .

27. Nathan Hodge ir Mary Ilyushina, ,,Putin signs law to create an independent Russian internet“, CNN, žiūrėta 2024 m. vasario 24 d., https://edition.cnn.com/2019/05/01/europe/vladimir-putin-russian-independent-internet-intl/index.html .

28. Nerijus Maliukevičius, ,,Informacijos karas: Rusijos požiūris“, Post Scriptum, žiūrėta 2024 m. balandžio 5 d. http://www.postscriptum.lt/7-karas/informacijos-karas-rusijos-poziuris .

29. Paul Bischoff, ,,Internet Censorship 2024: A Global Map of Internet Restrictions“, Comparitech, žiūrėta 2024 m. kovo 22 d. https://www.comparitech.com/blog/vpn-privacy/internet-censorship-map/ .

30. Rob Binns, ,,Websites banned in China: Access, alternatives and unblocked sites“, Independent Advisor, žiūrėta 2024 m. kovo 26 d. https://www.independent.co.uk/advisor/vpn/websites-banned-in-china .

31. Robbie Fordyce, ,,What is the ‚splinternet‘? Here‘s why the internet is less whole than you might think“, The Conversation, žiūrėta 2024 vasario 25 d., https://theconversation.com/what-is-the-splinternet-heres-why-the-internet-is-less-whole-than-you-might-think-207033 .

32. Robert McMahon, ,,Russia is Censoring News on the War in Ukraine. Foreign Media Are Trying to Get Around That.“ Council on Foreign Relations, žiūrėta 2024 m. balandžio 4 d. https://www.cfr.org/in-brief/russia-censoring-news-war-ukraine-foreign-media-are-trying-get-around .

33. Roskomvsoboda, „How Internet censorship changed in Russia during the 1st year of military conflict in Ukraine“, Open Observatory of Network Interference, žiūrėta 2024 m. kovo 27 d. https://ooni.org/post/2023-russia-a-year-after-the-conflict/ .

34. Sean Costigan, „Trouble in Cyberspace: increasing crime and exporting authoritarianism, Iris Report, žiūrėta 2024 m. balandžio 8 d. https://www.iris.report/p/trouble-in-cyberspace .

35. United Nations, „Activists: Internet shutdowns violate human rights“, United Nations, žiūrėta 2024 m. kovo 26 d. https://www.ohchr.org/en/stories/2022/08/activists-internet-shutdowns-violate-human-rights .

36. Xiao Qiang, „How China‘s Internet Police Control Speech on the Internet‘‘, Radio Free Asia, žiūrėta 2024 m. vasario 25 d., https://www.rfa.org/english/commentaries/china_internet-11242008134108.html .

37. Yaqiu Wang, „In China, the „Great Firewall“ Is Changing a Generation“, POLITICO, žiūrėta 2024 m. vasario 25 d., https://www.politico.com/news/magazine/2020/09/01/china-great-firewall-generation-405385 .

Oficialūs dokumentai

1. Australian Human Rights Commission, „Background paper: Human rights in cyberspace“, Australian Human Rights Commission, (2013): 3.

2. Baltiejie rūmai, „*A Declaration for the Fututre of the Internet“* 2022, https://www.whitehouse.gov/wp-content/uploads/2022/04/Declaration-for-the-Future-for-the-Internet_Launch-Event-Signing-Version_FINAL.pdf (žiūrėta 2024 m. balandžio 15 d.)

3. China Briefing, „The PRC Personal Information Protection Law (Final): A Full Translation, China Briefing, žiūrėta 2024 m. kovo 20 d. https://www.china-briefing.com/news/the-prc-personal-information-protection-law-final-a-full-translation/ .

4. European Court of Human Rights, „*Euroepan Convention on Human Rights as amended by Protocols Nos. 11, 14 and 15, supplemented by Protocols Nos. 1, 4, 6, 7, 12, 13 and 16*“ France, 1970, https://www.echr.coe.int/documents/d/echr/convention_ENG (žiūrėta 2024 m. balandžio 4 d).

5. Freedom Online Coalition, „Openess, Accessibility and Inclusion – Human Rights Online in the 2020“ (pranešimas konferencijoje Freedom Online: 2021: 10th Anniversary of the Freedom Online Coalition, Lapkričio 30 d. – Gruodžio 3 d., 2021) 10.

6. Freedom House, „Freedom on the Net 2023: The Repressive Power of Artificial Intelligence“, Freedom House (2023): 24-27.

7. Internet Rights and Principles Dynamic Coalition UN Internet Governance, *the charter of human rights and principles for the internet* 4 (2014).

8. Note by Secretary-General, „Group of Government Experts on Developing in the Field of Information and Telecommunications in the Context of Internatonal Security“, United Nations General Assembly, 2015, *United General Assembly*, liepos 22d., 2015, 8.

9. People‘s Republic of China, *Data Security Law of the People‘s Republic of China*, China, žiūrėta 2024 m. kovo 31 d. http://www.bi168.cn/thread-37794-1-1.html .

10. Rusijos Federacija, „*Doctrine of Information Security of the Russian Federation“* Rusija, 2016, http://www.scrf.gov.ru/security/information/DIB_engl/ (žiūrėta 2024 m. balandžio 4 d.).

11. Rusijos Federacijos Vyriausybė, *Federal Law of May 1, 2019 N 90-FZ "On Amendments to the Federal Law "On Communications" and the Federal Law "On Information, Information Technologies and Information Protection*. Rusija, 2019, https://rg.ru/documents/2019/05/07/fz90-dok.html (žiūrėta 2024 m. balandžio 6 d.).

12. United Nations, „Universal Declarations of Human Rights“ United Nations 2024 m. balandžio 10 d. https://www.un.org/en/about-us/universal-declaration-of-human-rights .

13. United Nations, *Report of the Secretary-General: Roadmap for Digital Cooperation* (United Nations, 2020),14.

14. United Nations, *United Nations International Covenant on Civil and Political Rights, General comment No.34: Article 19: Freedoms of opinion and expression*, Geneva, 11-29 July, 2011, https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf (žiūrėta 2024 m. kovo 31 d.).

15. Xi Jinping, *Remarks by H.E. Xi Jinping President of the People's Republic of China At the Opening Ceremony of the Secong World Internet Conference*(Wuzhen, 2015 m. gruodžio 16 d.) 2.

Raportai Kinija

1. Freedom House, „Freedom on the Net: China 2015“
2. Freedom House, „Freedom in the World 2016 Country Report: China“
3. Freedom House, „Freedom in the World 2017 Country Report: China“
4. Freedom House, „Freedom in the World 2018 Country Report: China“
5. Freedom House, „Freedom in the World 2019 Country Report: China“
6. Freedom House, „Freedom in the World 2020 Country Report: China“
7. Freedom House, „Freedom in the World 2021 Country Report: China“
8. Freedom House, „Freedom in the World 2022 Country Report: China“
9. Freedom House, „Freedom in the World 2023 Country Report: China“
10. Freedom House, „Freedom in the World 2024 Country Report: China“

Raportai Rusija

1. Freedom House, „Freedom on the Net: Russia 2015“
2. Freedom House, Freedom on the Net: Russia 2016“

3. Freedom House, „Freedom in the World 2017 Country Report: Russia“
4. Freedom House, „Freedom in the World 2018 Country Report: Russia“
5. Freedom House, „Freedom in the World 2019 Country Report: Russia“
6. Freedom House, „Freedom in the World 2020 Country Report: Russia“
7. Freedom House, „Freedom in the World 2021 Country Report: Russia“
8. Freedom House, „Freedom in the World 2022 Country Report: Russia“
9. Freedom House, „Freedom in the World 2023 Country Report: Russia“
10. Freedom House, „Freedom in the World 2024 Country Report: Russiaa“

Kita

1. Cloudfare, „What is data sovereignty“, Cloudfare, žiūrėta 2024 m. kovo 29 d. https://www.cloudflare.com/en-gb/learning/privacy/what-is-data-sovereignty/ .

2. DataGuidance, „China: Cybersecurity“ *DataGuidance* (2022): 1.

3. DataGuidance, „Russia: Cybersecurity“ *DataGuidance* (2022): 2-3.

4. Duomenų apsaugos tarnyba, „GDPR įstatymas Lietuvoje – kaip prisitaikyti organizacijoms?“, Duomenų apsaugos tarnyba, žiūrėta 2024 vasario 16 d. https://dat.lt .

5. Harvard University, „Survey of Government Internet Filtering Practices Indicates Increasing Internet Censorship“, Berkman Klein Center For Internet & Society at Harvard University, žiūrėta 2024 m. kovo 22 d. https://cyber.harvard.edu/newsroom/first_global_filtering_survey_released .

6. Rima Varnienė, „Visuotinė žmogaus teisių deklaracija“, Visuotinė Lietuvių Enciklopedija, žiūrėta 2024 m. kovo 31 d. https://www.vle.lt/straipsnis/visuotine-zmogaus-teisiu-deklaracija/ .

Summary

„Digital Sovereignty and Human Rights: A Comparative Analysis of Cyberspace Regulation in China and Russia“

Nowadays, cyberspace become one of the most important battlefields in international relations and diplomacy. Cyberspace governance is fragmented into many segments, forming a multi-polar network involving the state, private IT businesses, organizations, and internet users, all contributing to internet governance. Western countries such as the USA are implementing the free and liberal ideologies of the internet, while the authoritarian states China and Russia are creating digital sovereignty of cyberspace and influencing geopolitical fragmentation of the network. This campaign is the assessment of this thesis because it poses a twofold threat to the democratic paradigm: the human rights of the individual and the human right to free access to information dissemination on the internet. While talking about cyberspace, one of the most controversial topics is the human rights of every internet user. This paper aims to answer how China and Russia formulate the doctrine of cyber-sovereignty and put it into practice regarding the Western principles of human rights on the internet.

To implement the research, this paper first analyses all leading international relations theories, from which it is found that international regime theory is the most suitable to analyze deep cyberspace topics, such as human rights. The main empirical objective is the Freedom House “Freedom on the Net" annual reports from 2015 year. Exactly at that year, China was the first country to bring "Digital Sovereignty" to the international relations discourse, and Russia, in those years, started to think about digital sovereignty in Russia's cyberspace.

In conclusion, this paper finds that both China and Russia are actively pursuing cyber sovereignty, with their strategies often overlapping. The analysis reveals that the fragmentation of the internet, driven by differing state perspectives on data security and content censorship, poses significant challenges to the protection of human rights online. Both countries have implemented similar measures in internet governance, such as VPN regulation and content filtering. However, their approaches differ in key aspects. China focuses on internal state processes, while Russia's strategy includes occasional internet shutdowns during politically sensitive events. These actions, which compromise human rights, indicate that their digital sovereignty does not align with international human rights standards. Therefore, their shaping policies can be viewed as a regime doctrine, legitimizing authoritarian interests in cyberspace operations.