

STIPRESNI GINKLAI ŠALIES INFORMACINEI GYNYBAI

Informacinio karo fronte per silpnai, per lėtai ir per gailestingai atsišaudome. Mums nedelsiant reikia stipresnių ginklų ne tik oro, bet ir informacinės erdvės gynybai – nes dezinformacija yra nusikaltimas ir grėsmė nacionaliniam saugumui, todėl atsakas turi būti adekvatus.

Kova su dezinformacija turi būti valstybės prioritetas – jeigu didiname lėšas gynybai, turime didinti ir lėšas kovai su kremliaus melagienomis. Klaidinantys ir bauginantys naratyvai sklinda greičiau nei migrantai ar dronai per sieną. Ir pataiko taikliau – tiesiai į mūsų žmonių širdis ir smegenis. O teisinė bazė šokiruojančiai neparuošta gynybai informaciniame kare, stinga net aiškių kovos su dezinformacija sąvokų, būtini atitinkami saugikliai.

Šis politinis dokumentas (angl. „policy paper“) apibendrina TS-LKD frakcijos narės Daivos ULBINAITĖS inicijuoto teisėkūros paketo esmę – nuo informacinės gynybos stiprinimo iki automatizuotų technologijų reguliavimo, pateikia Lietuvos institucijų vertinimus, tarptautinę praktiką bei siūlymus, kaip toliau stiprinti valstybės atsparumą informaciniams pavojams.

Išanalizavę situaciją su visomis 11 institucijų, kurios mūsų šalyje atsakingos už kovą su dezinformacija, įvertinę 9 šalių patirtis, surengę tarpinstitucinį pasitarimą, tarptautinį forumą „Informacinis karas: kuo atsišaudome“ su Lenkijos ir Suomijos ekspertais, kartu su teisės mokslininkais ir žiniasklaidos ekspertais parengėme veiksmingesnei gynybai informaciniame kare ir kovai su dezinformacija būtiną **5** įstatymų pakeitimų paketą. Tai:

Visuomenės informavimo įstatymo, Informacinės visuomenės paslaugų įstatymo, Elektroninių ryšių įstatymų bei Administracinių nusižengimų kodekso ir Baudžiamojo kodekso pataisos, kuriomis:

detaliau apibrėžiama dezinformacijos samprata, kad būtų aišku su kuo tiksliai kovojame, ką laikome nusikaltimu, kad būtų galima teisiškai kvalifikuoti pavojingą informaciją ir taikyti sankcijas, kad mūsų institucijos vienareikšmiškai atpažintų dezinformaciją ar karo propagandą;

suteikiami įgaliojimai institucijoms greičiau reaguoti į pavojingą ir nusikalstamą informaciją – turi būti užtikrinta savalaikė reakcija į grėsmes nacionaliniam saugumui keliančią dezinformaciją;

apibrėžiama automatizuotų elektroninių ryšių identifikatorių vadinamųjų „SIM spiečių“ sąvoka ir atsakomybė už jų naudojimą;

numatoma administracinė ir baudžiamoji atsakomybė platformoms bei individualiems asmenims už melagingos informacijos skleidimą;

„Pagrindinis tikslas – kriminalizuoti sisteminę dezinformaciją ir suteikti institucijoms įrankius greitai reaguoti į informacinės atakas. Įstatymų paketas sukurtas siekiant užtikrinti efektyvų nacionalinės informacinės gynybos modelį, suderintą su ES ir NATO praktika.“

Kodėl reikia stipresnių ginklų informaciniame kare?

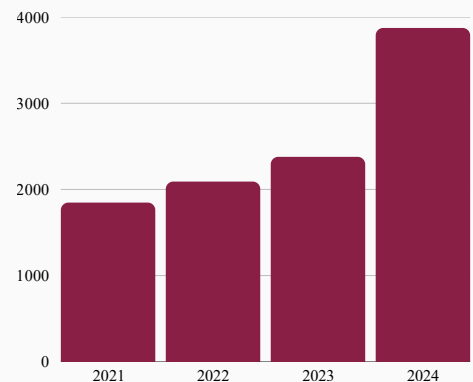
Reaguodami į geopolitinę situaciją ir nacionaliniam saugumui kylančias egzistencines grėsmes, mes sustiprinome ir net uždarėme sienas, padidinome gynybos biudžetą, ėmėmės priemonių oro gynybos stiprinimui. Tačiau iki šiol neturime deramo atsako prieš vieną sudėtingiausių šiuolaikinių grėsmių – informacinį karą, kuris ardo mus iš vidaus.

Lietuva – nuolatinis informacinio karo taikiny:

- Lietuva, būdama rytinio NATO flango priešakinėse linijose, yra nuolatinis kremliaus dezinformacijos ir propagandos taikiny.
- Dezinformacija tapo hibridinio karo ginklu, nukreiptu į visuomenės susiskaldymą, demokratijos silpninimą ir valstybės institucijų diskreditavimą.
- Klaidinantys naratyvai sklinda greičiau nei migrantai ar dronai per sieną – jie taikosi į žmonių širdis ir protus.

Informacinės atakos stiprėja:

- Nacionalinio kibernetinio saugumo centro duomenimis, 2024 m. Lietuvoje užfiksuota 3 874 kibernetiniai incidentai – 63 % daugiau nei 2023 m.
- Tuo pat metu išaugo sisteminių pažeidžiamumų skaičius – daugiau kaip 6 700 pažeidžiamų informacinių sistemų.
- Kibernetinės atakos ir dezinformacijos kampanijos veikia išvien, stiprindamos viena kitą.



Kremliaus dezinformacijos tinklas – nuo botų iki „žurnalistų“:

Kremliaus propagandos mašina veikia pilnu pajėgumu:

- naudojami botai, trolių tinklai, dirbtinis intelektas, pseudožurnalistai ir vietiniai veikėjai;
- gaminami nauji melagienų produktai, kuriais nuodijami žmonių protai;
- siekiama paveikti rinkimus, menkinti kariuomenę, NATO, energetinius projektus, klastoti istoriją, kurstyti nepasitenkinimą ir nesaugumą.

VSD duomenimis, Kremlius 2025 m. propagandai ir dezinformacijai skyrė 1,4 mlrd. eurų – įtraukiant tiek IT specialistus, tiek kultūros veikėjus.

Teisinis vakuumas:

- Kasmetiniame VSD ir AOTD Grėsmių valstybės saugumui vertinime įvardijami konkretūs kanalai ir asmenys, skleidžiantys kremliaus melus, tačiau nėra aiškių teisinių priemonių, kaip į tai reaguoti.



„Stebime agresyvesnes ir pavojingesnes nuo Šaltojo karo laikų primirštas kenkėjiško veikimo formas.“
(VSD/AOTD, 2025)

„Rusijos vykdomos istorijos politikos tikslai – socialinės ir etninės nesantaikos kurstymas, provokacijų ir informacinių akcijų organizavimas.“ (VSD, 2024)

- Tarnybos perspėja apie grėsmes iš *TikTok*, *Telegram* ir pseudožiniasklaidos kanalų, tačiau politinių sprendimų vis dar trūksta.

Technologinė bazė dezinformacijai – „SIM spiečiai“:

Lietuvoje plinta automatizuotos SIM valdymo sistemos („SIM spiečiai“), leidžiančios vienu metu valdyti tūkstančius numerių. Ši infrastruktūra naudojama ne tik sukčiavimui ar neteisėtai reklamai, bet ir masinei dezinformacijos sklaidai bei informacinėms operacijoms prieš valstybę.

VSD ir NKVC įspėja, kad „SIM spiečiai“ iš esmės tampa technologiniu įrankiu informacinio karo ir kibernetinio nusikalstamumo infrastruktūroje, informacinėse operacijose, nukreiptose prieš Lietuvos valstybę, jos institucijas ir demokratinius procesus, tačiau:

- nėra draudimo tokią įrangą laikyti ar naudoti;
- nėra atsakomybės už jos eksploatavimą;
- valstybė veikia teisinio vakuumo sąlygomis.



- Lietuvoje yra beveik 2 mln. socialinių tinklų vartotojų – ir net 30 proc. paskyrų yra netikros.
- 2024 m. Lietuvos policija fiksavo atvejį, kai vienas telefono numeris per vieną naktį bandė registruoti 41 paskyrą, iš kurių 19 paskyrų buvo sėkmingai sukurtos.
- Lietuvos kriminalistai Vilniaus mieste identifikavo vadinamuosius SIM „spiečius“ ir sulaukė kelis šią veiką organizuojančius įtariamuosius. Kratų metų buvo rasta beveik 200 SIM Box, apie 100 kompiuterių, kuriais buvo vykdoma ši nusikalstama veika, bei apie 75 000 įvairių šalių operatorių SIM kortelių. Įtariama, kad kratų metu rasti SIM BOX ir SIM kortelės buvo naudojamos sukčiavimams ir kitoms nusikalstamoms veikoms vykdyti net tik Lietuvos teritorijoje, bet ir užsienio šalyse.
- Latvijos policija įgyvendino kruopščiai suplanuotą tarptautinę operaciją „SIMcartel“ ir sutriuškino tarptautinį sukčiavimo tinklą. Pareigūnai atliko 14 kratų, konfiskavo 1 200 SIMbox įrenginių, kuriuose vienu metu veikė 40 000 įvairių šalių SIM kortelių, ir paėmė 5 serverius, visiškai perimdami įmonės IT infrastruktūrą, kurioje buvo sukurta apie 50 milijonų paskyrų, kurias buvo galima naudoti internetiniams sukčiavimams ir dezinformacijai skleisti. SIMbox platforma siūlė galimybę naudoti daugiau nei 80 šalių mobiliųjų telefonų numerius, su kuriais techniškai buvo įmanoma anonimiškai registruotis daugiau nei 160 internetinių paslaugų.

Silpna visuomenės atsparumo kultūra:

- Tik 21 % šalies gyventojų tikrina faktus, nors net 78 % pripažįsta, kad Rusija daro informacinį poveikį. Tai rodo menką medijų raštingumą ir būtinybę stiprinti visuomenės kritinį mąstymą.
- mokymai ir praktinės veiklos, ugdančios medijų raštingumą, sumažina tikėjimą melagingais teiginiais net 27 proc., o neteisingos informacijos platinimą – daugiau nei perpus.

Kaip dabar atrodo teisinė bazė?

Teisės ekspertų išvada: teisinė sistema nepasiruošusi karui informacinėje erdvėje

- Dėl **nebaudžiamumo kova su dezinformacija dažnai nerezultatyvi**. Reikia aiškos atsakomybės dezinformacijos kūrėjams, skleidėjams, gabentojams. Tarpinstituciniame pasitarime su už kovą su dezinformacija atsakingomis institucijomis pabrėžta kad:
 - jeigu pripažįstame, kad gyvename informacinio karo sąlygomis – tai ir ginklų reikia radikalesnių;
 - dezinformacinis turinys turi būti kriminalizuotas, tuomet galėsime kreiptis į soc. tinklus su prašymu blokuoti ne šiaip žalingą turinį, o nusikaltimą – reakcija ir efektas bus kitoks;
 - melų rūšių yra įvairių – reikia aiškiai apsibrėžti – kas yra nacionaliniam saugumui žalingas ir visuomenei grėsmę keliantis turinys.
- Lietuvos Respublikos Seime vykusiame tarptautiniame forume „Informacinis karas: kuo atsišaudome. Lenkijos, Suomijos ir Lietuvos patirtys“, teisės ekspertai konstatavo:



„Teisinė bazė ŠOKIRUOJANČIAI NEPARUOŠTA gynybai informaciniame kare. Nei nacionalinė, nei Europos Sąjungos teisinė bazė nėra pritaikyta laikmečio iššūkiams ir karui.“

Ši išvada atskleidžia skaudžią realybę – informacinėje erdvėje mes vis dar kovojame be aiškių ginklų. Dezinformacija nėra tik viešosios erdvės triukšmas – tai nusikaltimas ir tiesioginė grėsmė nacionaliniam saugumui, kurį kremlius naudoja kaip sisteminių hibridinio karo įrankį.

Konstitucinis pagrindas kovai su dezinformacija:

Lietuvos Respublikos Konstitucijoje dezinformacija yra įvardijama kaip nusikalstamas veiksmas:



25 straipsnis: „Laisvė reikšti įsitikinimus ir skleisti informaciją nesuderinama su nusikalstamais veiksmais – tautinės, rasinės, religinės ar socialinės neapykantos, prievartos bei diskriminacijos kurstymu, šmeižtu ir dezinformacija.“

Praktiškai poreikis kriminalizuoti dezinformaciją kyla iš šio Konstitucijos straipsnio – yra konstituciškai pagrįstas. Tai reiškia, kad Konstitucija įpareigoja valstybę sukurti tokį teisinį reguliavimą, kuris užkirstų kelią dezinformacijai, karo ar klaidinančiai propagandai.

Dabartinis Visuomenės informavimo įstatymas nurodo draudimą skleisti dezinformaciją, tačiau trūksta detalesnės apibrėžties, aiškių taikymo kriterijų ir procedūrų, leidžiančių institucijoms greitai ir teisėtai veikti.

Tai išdėstyta ir Seimo analitinėje ataskaitoje, kuri lygina ES valstybių praktiką ir konstatavo Lietuvos teisinio instrumento spragas.

Kaip dabar atrodo teisinė bazė?

- nėra detaliai apibrėžta;
- nėra aiškos atsakomybės mechanizmo;
- nėra kriminalizuota.

Nacionalinio saugumo strategijoje dezinformacija tiesiogiai priskiriama prie grėsmių valstybės saugumui. ES ir NATO dokumentuose dezinformacija įvardijama kaip hibridinės atakos elementas, kartu su kibernetinėmis atakomis ir diversijomis.

„Dezinformacija kelia grėsmę demokratijos procesams, piliečių pasitikėjimui ir valstybės saugumui“.

ES komunikatas „Tackling Disinformation: A European Approach“ (2018)

„Informacinės ir kibernetinės operacijos yra hibridinių grėsmių branduolys, todėl Aljanso narės privalo stiprinti atsparumą informacinei įtakai.“

NATO strateginė koncepcija (2022)

Tačiau šie tarptautiniai dokumentai neturi tiesioginio teisinio veikimo – jie reikalauja nacionalinio įgyvendinimo, kurio Lietuvoje kol kas trūksta.

Institucinis laukas – fragmentuotas ir per lėtas:

Šiuo metu 11 institucijų vienaip ar kitaip atsakingos už kovą su dezinformacija:

1. Ryšių reguliavimo tarnyba,
2. Žurnalistų etikos inspektoriaus tarnyba,
3. Lietuvos radijo ir televizijos komisija,
4. Valstybės saugumo departamentas,
5. Policijos departamentas,
6. Krašto apsaugos ministerija,
7. Užsienio reikalų ministerija,
8. Lietuvos kariuomenės Strateginės komunikacijos departamentas
9. Lietuvos Šaulių sąjunga
10. Vadovybės apsaugos tarnyba

Jų pastangas koordinuoja Vyriausybės kanceliarijos Nacionalinis krizių valdymo centras (NKVC). Tačiau Tarpinstitucinį kovos su dezinformacija ir manipuliacijomis planą rengia Kultūros ministerija, tačiau visos institucijos vienbalsiai sutaria:

- turimi įrankiai – nepakankami.
- reagavimas – per lėtas.
- Kova – fragmentuota.

Šiuo metu, kai žalingas turinys gali išplisti per kelias minutes, institucinis reagavimas dažnai užtrunka savaites ar net mėnesius. Vietoje koordinuotos gynybos turime biurokratinį procesą, kuriame realus žalingo turinio šalinimas gali užtrukti iki 60 dienų, o siekiamybė - 15 min.

Tarptautinės platformos ir skaitmeninės erdvės kontrolė:

„Meta“ (Facebook) neveiklumas krizės metu:

- Įvykus informaciniam incidentui ar krizinei situacijai, vietiniai „Meta“ atstovai sunkiai pasiekiami, o į tarnybų prašymus pašalinti draudžiamą turinį reaguojama lėtai arba visai nereaguojama.
- Net ir faktų tikrintojų pripažintą klaidinantį turinį „Meta“ dažnai tik pažymi, bet nepašalina, taip palikdama jį veikti informacinėje erdvėje.

EBPO rekomendacijos – be realaus įgyvendinimo:

- Europos bendradarbiavimo ir plėtros organizacijos (EBPO) rekomendacijose numatyta, kad socialinių tinklų kompanijos turėtų turėti atstovus kiekvienoje šalyje, o turinio vertinimas turėtų būti atliekamas atsižvelgiant į nacionalinį kontekstą.
- Tačiau EBPO diskusijų metu „Facebook“ atstovai atvirai išsakė nenorą turėti daugiau vietinių atstovų ar taikyti nacionalinės teisės kriterijus turinio moderavimui. → Tai reiškia, kad Lietuva neturi efektyvių svertų priversti globalias platformas elgtis atsakingai pagal mūsų teisinę sistemą.

„Telegram“, „TikTok“, „X“ – už įstatymo ribų:

- „Telegram“ veikia už ES Skaitmeninių paslaugų akto (Digital Services Act) ribų ir aktyviai išnaudojama nusikaltimams organizuoti bei vykdyti.
 - Lietuvos teisėsauga fiksuoja konkrečius atvejus, kai per „Telegram“ koordinuojamos neteisėtos veikos.
 - Pareigūnai sulaiko paskyrų valdytojus, tačiau be tarptautinio reguliavimo tai – kovos su pasekmėmis, o ne priežastimis modelis.
- „TikTok“ ir „X“ (buvęs „Twitter“) formaliai patenka į DSA taikymo sritį, bet dažnai nesilaiko jo nuostatų, ypač turinio šalinimo ir vartotojų duomenų apsaugos srityse.
 - „TikTok“ algoritmų netransparentiškumas ir vartotojų duomenų perdavimas į Kinijos serverius kelia nacionalinio saugumo riziką.
 - Fiksuoti atvejai, kai per platformą platinami dirbtinio intelekto sukurti vaizdo įrašai, raginantys „bendradarbiauti su Rusija“ ar „grįžti į jos glėbį“.

Kaip institucijos vertina situaciją?

Valstybės saugumo departamentas (VSD):

VSD vertinimu, Lietuva išlieka vienu pagrindinių Rusijos informacinių atakų taikinių Baltijos regione. Priešiškos informacinės kampanijos yra nuoseklios, koordinuotos ir finansuojamos iš milžiniško – iki 1,4 mlrd. eurų – Kremliaus propagandos biudžeto.

Pagrindiniai naratyvai skirti diskredituoti Lietuvos demokratiją, jos narystę NATO, paramą Ukrainai ir istorijos politiką, vaizduojant šalį kaip rusofobišką bei Vakarų valdomą valstybę. VSD pažymi, kad 2024–2025 m. Rusija vis plačiau naudoja dirbtinio intelekto technologijas ir automatizuotus profilius (botus), kurie leidžia greitai skleisti lokalizuotą melagingą turinį. Tokios atakos siekia mažinti visuomenės pasitikėjimą valdžios institucijomis, kurstyti nepasitenkinimą ir supriešinti visuomenės grupes.

Kaip institucijos vertina situaciją?

Nacionalinis krizių valdymo centras (NKVC):

Vyriausybės kanceliarijos Nacionalinis krizių valdymo centras (NKVC) kaip centrinė institucija, koordinuoja prieš Lietuvos nacionalinio saugumo interesus nukreiptų informacinių incidentų stebėseną, analizę ir vertinimą. 2025 m. fiksuoti pagrindiniai incidentai rodo vis sudėtingesnę priešiško veiksmų pobūdį – nuo masinių melagingų pranešimų apie užminavimus švietimo įstaigose iki dezinformacinių atakų, susijusių su Lietuvos energetine nepriklausomybe, NATO pajėgų veikla ar istorine atmintimi. Šių incidentų metu plačiai naudojamos hibridinės informacinės priemonės – melagingi elektroniniai laišakai, suklastoti naujienų pranešimai, socialinių tinklų botai, dirbtinio intelekto sugeneruotas turinys ir koordinuota žinučių amplifikacija. NKVC pažymi, kad dauguma atakų siekia paveikti visuomenės emocinę būseną, mažinti pasitikėjimą valdžios institucijomis ir skatinti priešiško valstybių naratyvus.

NKVC vertinimu, informacinių atakų mastas ir technologinė įvairovė kelia nuolatinį pavojų valstybės informaciniam stabilumui, todėl būtina teisinė ir institucinė bazė, leidžianti greitai reaguoti į kintančias hibridines grėsmes bei užtikrinti atsakomybę už dezinformacijos sklaidą.

Žurnalistų etikos inspektoriaus tarnyba:

2024 m. išliko intensyvios ir koordinuotos Rusijos dezinformacijos kampanijos, nukreiptos prieš Lietuvą ir kitas Ukrainą remiančias valstybes. Pagrindiniai naratyvai – NATO ir gynybos diskreditavimas, paramos Ukrainai menkinimas, socialinio nepasitenkinimo ir energetinės krizės temų išnaudojimas.

Žurnalistų etikos inspektoriaus tarnyba atliko 85 stebėsenos aktus, pateikė 30 privalomų nurodymų pašalinti dezinformacinį turinį, 7 atvejais kreipėsi į teismą dėl blokavimo, apribojo prieigą prie 7 portalų. Užblokuota 50 propagandinių turinį platinusių socialinių tinklų paskyrų. Tarnyba nustatė, kad teisinis reguliavimas vis dar neužtikrina veiksmingo kovos su dezinformacija mechanizmo – nėra atsakomybės už propagandinių leidinių gabenimą, taip pat nėra galimybės greitai blokuoti portalo kopijų.

Situacija vertinama kaip išliekanti didelės rizikos, būtina stiprinti teisinį reguliavimą, institucijų bendradarbiavimą ir visuomenės atsparumą.

Lietuvos radijo ir televizijos komisija (LRTK)

2023–2024 m. LRTK priėmė sprendimus dėl daugiau nei 1300 IP adresų, per kuriuos buvo galima pasiekti sankcionuotas Rusijos ir Baltarusijos televizijos programas, bei nuo 2018 m. užblokavo per 720 neteisėtų svetainių, platinusių draudžiamą turinį. Be to, buvo blokuota daugiau nei 1000 IP adresų dėl autorių teisių pažeidimų, dažniausiai susijusių su rusiškais filmais, kurie naudojami kaip „minkštosios galios“ priemonės. Komisijos prašymu „YouTube“ taip pat buvo pašalintos ar apribotos paskyros, susijusios su sankcionuotais Rusijos veikėjais, o kai kuriais atvejais – net ir mobiliosios programėlės, per kurias buvo neteisėtai platinamos rusiškos ar baltarusiškos programos. LRTK aktyviai reaguoja ir į konkrečius dezinformacijos atvejus.

Komisija pabrėžia, kad ilgalaikėje perspektyvoje vienas svarbiausių kovos su dezinformacija elementų yra visuomenės švietimas ir informacinio raštingumo ugdymas. Tuo pat metu LRTK akcentuoja poreikį stiprinti tarptautinį koordinavimą – ES šalys narės vis dar skirtingai interpretuoja sankcijų taikymo ir įgyvendinimo tvarką, todėl būtina užtikrinti nuoseklų požiūrį visos Sąjungos mastu.

Kaip institucijos vertina situaciją?

Ryšių reguliavimo tarnyba (RRT):

RRT identifikuoja augančią technologinę grėsmę – vadinamuosius „SIM spiečius“ (automatizuotas SIM kortelių sistemas), kurios leidžia vykdyti masinę SMS, registracijų ir patvirtinimų srautą, naudojamą finansiniam sukčiavimui bei dezinformacijos kampanijoms. Šių sistemų veikla šiuo metu nėra teisiškai reglamentuota, todėl vyksta teisinio vakuomo sąlygomis.

RRT vertinimu, būtina įstatymu uždrausti neteisėtą automatizuotą SIM kortelių naudojimą ir suteikti tarnybai įgaliojimus stabdyti tokią veiklą bei taikyti administracinę atsakomybę. Tarnyba taip pat siūlo įtvirtinti prievolę operatoriams teikti duomenis apie įtartinas SIM veiklas ir stiprinti technologinę stebėseną, siekiant apsaugoti informacinę erdvę.

RRT nuo 2024 m. birželio mėn. paskirta Skaitmeninių paslaugų koordinatoriumi (SPK) pagal Europos Parlamento ir Tarybos reglamentą (ES) 2022/2065 dėl bendrosios skaitmeninių paslaugų rinkos, kuriuo iš dalies keičiama Direktyva 2000/31/EB (Skaitmeninių paslaugų aktas, DSA) siekiant didesnio veiksmingumo, svarbu užtikrinti institucinį pajėgumą reaguoti į sistemines grėsmes. Todėl galėtų būti sukurtas centralizuotas nacionalinis mechanizmas (pvz. per NKSC), kuris leistų kompetentingoms institucijoms realiuoju laiku sekti pranešimų dėl žalingo turinio skaičių, platformų atsakymus ir jų veiksmingumą.

Toks mechanizmas turėtų būti papildytas aiškia ir greita atvejų eskalavimo procedūra tarp pagrindinių institucijų – RRT, ŽEIT, LRTK, LB, VVTAT, LPT, NTAKD, NKSC ir PD – kad būtų užtikrinta savalaikė reakcija į pasikartojančius ar sisteminius turinio atvejus, keliančius grėsmę nepilnamečiams ar visuomenės saugumui. Šis sprendimas padėtų ne tik efektyviau taikyti DSA numatytas priemones, bet ir sustiprintų koordinuotą valstybės poziciją bendradarbiaujant su platformomis ir Europos Komisija.

Krašto apsaugos ministerijos Strateginės komunikacijos departamentas (STRATCOM):

STRATCOM pabrėžia, kad informacinės grėsmės tampa vis labiau hibridinės – jose derinamos kibernetinės, psichologinės ir socialinės manipuliacijos priemonės. Priešiški veikėjai išnaudoja emocinį turinį, humorą ir memus, kad melaginga informacija atrodytų autentiška ir patraukli jaunajai auditorijai. Fiksuojamos atakos, nukreiptos prieš Lietuvos kariuomenę, NATO sąjungininkų buvimą bei valstybės pasirengimą gynybai. STRATCOM teigimu, atsparumas informacinėms atakoms yra ne tik technologinis, bet ir visuomeninis iššūkis, todėl būtina nuosekliai stiprinti visuomenės švietimą, medijų raštingumą ir institucijų komunikacijos koordinavimą.

Policijos departamentas

Policijos departamentas nuomone, kontrabandinių oro balionų ataka taip pat parodė, kad SIM korteles tampa ginklu ir nusikaltimų įrankiu.

mobiliųjų operatorių SIM kortelės tampa neatsiejama kontrabandininkų priemone vykdyti savo veiklą. Vienas asmuo perka 10 tūkst. SIM kortelių ir operatoriai tai leidžia, nes niekas neriboja. Atsirado naujas fenomenas kaip SIM kortelių mulai, t. y. žmonės, kurie versliškai perpardavinėja korteles. Už tai nenumatyta jokia atsakomybė. Kontrabanda ir balionai, tai yra ir botai, dezinformacija ir visi kiti hibridinio karo elementai, kurie gali būti panaudoti prieš valstybę.

Seimo tyrimų skyrius atliko tyrimą apžvelgiami Lietuvos, Austrijos, Čekijos, Estijos, Latvijos, Lenkijos, Prancūzijos, Slovakijos, Suomijos ir Vokietijos nacionaliniai sprendimai kovoje su dezinformacija ir karo propaganda, sąvokų apibrėžtimi ar apibūdinimais.

Dezinformacija įvairiuose nacionaliniuose dokumentuose yra apibrėžiama panašiai, tačiau beveik kiekviename aprašyme galima išskirti kokį nors papildomą sąvokos kompleksiskumą žymintį aspektą. Subendrinus skirtingas apibrėžtis, dezinformaciją galima apibrėžti kaip melagingą ir klaidinančią informaciją, kuri skleidžiama sąmoningai ir tikslingai, siekiant pakenkti asmeniui, organizacijai, visuomenei, šaliai ar demokratijai. Be to, tai vertinama kaip tyčinis, slaptas veiksmas, kartais suprantamas ir kaip hibridinio karo ginklas, skirtas paveikti sprendimų priėmimą arba sprendimus priimančių asmenų nuomonę, taip siekiant politinės, socialinės, finansinės, karinės ir kitokios naudos.

Siekdamos neutralizuoti dezinformaciją, kai kurios žiniasklaidos priemonės savo interneto svetainėse suteikia galimybę skaitytojams pateikti įtariamas melagingas naujienas patikrai. Reikšmingą vaidmenį atlieka švietėjiška veikla, ugdant kritišką mąstymą ir stiprinant visuomenės atsparumą.

Kovodamos su dezinformacijos sklaida, nacionalinės žiniasklaidos priežiūros institucijos nurodo šalinti neteisėtą turinį, gali savo kompetencijos ribose taikyti administracinio poveikio priemones. Pažymėtina, kad Austrijos baudžiamajame kodekse (toliau – BK) nustatyta laisvės atėmimo iki 6 mėnesių bausmė arba bauda už melagingos informacijos viešą sklaidimą prieš rinkimus ar referendumus. Latvijos Baudžiamasis įstatymas numato atsakomybę už poveikį rinkimų procesui, pasinaudojant išmaniojo vaizdo klastojimo („deep fake“) technologija.

Karo propagandą draudžia tarptautinė teisė, ji kriminalizuota ir dalies Europos valstybių nacionaliniais baudžiamaisiais įstatymais. Šiuose įstatymuose gali būti numatyta atsakomybė už agresyvaus karo kurstymą, viešą raginimą padaryti agresijos nusikaltimą, kvietimą sukelti agresyvų karą ar ginkluotą konfliktą, karo ar ginklų panaudojimo, pažeidžiant bendrai pripažįstamus tarptautinės teisės principus, kurstymą, karo pateisinimą ir kt. Kai kuriose valstybėse (pavyzdžiui, Čekijoje, Suomijoje) baudžiamoji atsakomybė už karą skatinančius ir propaguojančius veiksmus taikoma tik tais atvejais, kai dėl jų gresia būtent tų valstybių įtraukimas į karą.

Pažymėtina, kad už veikų, susijusių su karo propaganda, padarymą daugelyje Europos valstybių numatytos gana griežtos sankcijos, dažniausiai be alternatyvų taikomas laisvės atėmimas (Lenkijoje, Vokietijoje maksimali bausmė – 5 metai, Latvijoje – 8 metai, Čekijoje, Suomijoje – 10 metų laisvės atėmimo). Slovakijoje už kvalifikuotą „grasinimą taikai“ (pavyzdžiui, bendradarbiaujant su užsienio jėgomis ar veikiant grupėje) gali būti baudžiama laisvės atėmimu nuo 10 iki 25 metų arba laisvės atėmimu iki gyvos galvos. Tuo tarpu Estijoje už karo propagandą baudžiama bauda arba laisvės atėmimu iki 3 metų.

Europos šalių baudžiamuosiuose įstatymuose įtvirtintų sankcijų už veikas, susijusias su karo propaganda, griežtumas gali būti aiškinamas tuo, kad dažniausiai tokios veikos laikomos nusikaltimais, kuriais kėsinamasi į itin svarbius baudžiamosios teisės ginamus teisinius gėrius (taiką, žmoniškumą, tarptautinį bei valstybės saugumą ir kt.), bei priskiriamos atitinkamiems baudžiamųjų įstatymų skyriams. Šiuo požiūriu kiek išsiskiria Austrija, kur tam tikromis aplinkybėmis padarytas agresijos akto pateisinimas yra priskirtas BK skyriui „Nusikalstamos veikos viešajai rimčiai“, o už jį bendru atveju baudžiama laisvės atėmimu iki 2 metų.



Lietuva: dezinformacijos ir propagandos sąvokų apibrėžimai ir alternatyvios sąvokos

Dezinformacijos sąvoka. Lietuvos Respublikos Konstitucijos 25 straipsnyje įtvirtinta, kad laisvė reikšti įsitikinimus ir skleisti informaciją nesuderinama su nusikalstamais veiksmais, kuriems priskiriama dezinformacija. Visuomenės informavimo įstatymo 2 straipsnio 15 dalyje yra apibrėžiama, kad dezinformacija yra „tyčia viešai paskleista melaginga informacija“.

Kituose įstatymuose dezinformacijos sąvoka papildomai nėra apibrėžiama. Dezinformacijos sąvoka minima Tautinių mažumų įstatyme[3]. 13 straipsnio 4 dalyje nustatyta, kad „įgyvendinant tautinėms mažumoms priklausančių asmenų teises, draudžiama kurstyti tautinę, rasinę, religinę ar socialinę neapykantą, prievartą, skleisti šmeižtą ar dezinformaciją“.

Dezinformacija taip pat minima ir strateginio lygmens dokumentuose. Pavyzdžiui, Valstybės pažangos strategijoje „Lietuvos ateities vizija „Lietuva 2050“[4] pažymima, kad strateginę ambiciją įgyvendinusioje Lietuvoje „nuosekliai visuose švietimo lygmenyse ugdant kritinį mąstymą, visuomenė tampa vis atsparesnė dezinformacijai ir kitoms informacinėms manipuliacijoms“.

Nacionalinio saugumo strategijoje[nurodoma būtinybė plėtoti valstybės institucijų ir įstaigų gebėjimus vykdyti kryptingą kovą su dezinformacija, siekiant užtikrinti koordinuotą informacinės aplinkos stebėjimą, analizę, vertinimą ir operatyvų perspėjimą bei savalaikį reagavimą į informacinius incidentus. Būtina stiprinti visuomenės atsparumą dezinformacijai ir kitoms informacinėms grėsmėms.



Vokietijoje kova su dezinformacija sutelkta ne į atskirą „dezinformacijos“ straipsnį, o į hibridinių grėsmių valdymą, platformų atsakomybę ir žurnalistinių standartų priežiūrą. Koordinuoja Vidaus reikalų ir bendruomenės ministerija (BMI); nuo 2024 m. jai pavaldus ZEAM anksti identifikuoja užsienio informacijos manipuliacijas.

Skaitmeninių paslaugų akto įgyvendinamasis įstatymas (DDG) pakeitė NetzDG: Bundesnetzagentur koordinuoja priežiūrą, numatyti įpareigojimai platformoms (pranešimų/skundų sistemos, skaidrumas, veiksmai prieš neteisėtą turinį) ir administracinės sankcijos.

Baudžiamojo kodekso lygmeniu taikomi bendrieji straipsniai (šmeižtas, melagingi pranešimai ir pan.), o už agresijos nusikaltimo kurstymą (BK §80a) – nuo 3 mėn. iki 5 m. laisvės atėmimo. Modelis pabrėžia tarpžinybinį atsaką, ankstyvą užsienio įtakos nustatymą ir stiprią platformų priežiūrą, kartu išlaikant žodžio laisvės apsaugai svarbią savireguliaciją.



Suomijoje vietoj siauro „dezinformacijos“ apibrėžimo taikomas platesnis informacinio poveikio ir informacinės gynybos modelis, akcentuojant prevenciją ir atsparumą. Krizių ir intensyvių atakų metu atsaką bei strateginę komunikaciją koordinuoja Ministro Pirmininko kanceliarija; gynybinį komponentą vykdo Gynybos ministerija ir ginkluotosios pajėgos su partneriais. Traficom prižiūri Skaitmeninių paslaugų akto įgyvendinimą: neteisėto turinio šalinimo procedūros, platformų skaidrumas ir sankcijos už nesilaikymą. Medijų raštingumą sistemingai stiprina Nacionalinis audiovizualinis institutas. BK numato atsakomybę už specifines melagingos informacijos veikas (pvz., šmeižtas, melagingi pranešimai), o už karo kurstymą – 1–10 m. laisvės atėmimo, kai viešai raginama agresijai ar sistemingai skleidžiama klaidinanti informacija apie gynybą (BK 12 sk.).



Austrijoje kova su dezinformacija grindžiama aiškiu reguliavimu ir institucijų bendradarbiavimu. Pagrindinę priežiūrą vykdo Ryšių tarnyba (Kommunikationsbehörde Austria), užtikrinanti, kad žiniasklaidos turinys būtų tikslus ir nepažeistų įstatymų – už klaidinančią ar propagandinę informaciją gali būti taikomos baudos ar licencijų panaikinimas. Vidaus reikalų ministerijos Valstybės apsaugos ir žvalgybos direkcija stebi informacinį lauką ir tiria užsienio dezinformacijos kampanijas, ypač susijusias su Rusijos įtaka.

Medijų raštingumui stiprinti veikia švietimo iniciatyvos – Politiškumo ugdymo centras (Zentrum polis) ir Saugesnio interneto centras, organizuojantys mokymus ir kuriantys metodinę medžiagą. Dezinformaciją tikrina ir viešai paneigia tokios platformos kaip „APA-Faktencheck“, „Mimikama.at“ ir „#UseTheNews“.

Teisiniu lygmeniu atsakomybė už melagingos informacijos skleidimą numatyta Baudžiamojo kodekso 264 ir 283 straipsniuose, o Komunikacijos platformų įstatymas įpareigoja socialinius tinklus šalinti neteisėtą turinį, už pažeidimus numatydamas iki 10 mln. eurų baudas. Kovos su propagandiniu ir ekstremistiniu turiniu koordinavimą vykdo Nacionalinis ekstremizmo prevencijos ir deradikalizacijos tinklas (BNED).

Austrijos sistema išsiskiria tuo, kad derina turinio priežiūrą, teisinę atsakomybę ir švietimą – siekiama mažinti dezinformacijos poveikį ne tik sankcijomis, bet ir visuomenės atsparumo stiprinimu.



Čekijoje kova su dezinformacija grindžiama valstybės saugumo ir hibridinių grėsmių valdymo principais. Pagrindinė institucija – Centras kovai su terorizmu ir hibridinėmis grėsmėmis, veikiantis Vidaus reikalų ministerijoje nuo 2017 m. Jis analizuoja informacinio saugumo rizikas, teikia pasiūlymus Vyriausybei, konsultuoja dėl teisėkūros ir vykdo švietėjišką veiklą, tačiau neturi įgaliojimų šalinti turinio iš interneto. Kovos su dezinformacija koordinavimas taip pat priskirtas Nacionalinio saugumo patarėjui, kuris užtikrina institucijų bendradarbiavimą reaguojant į hibridines grėsmes. Saugumo informacijos tarnyba stebi užsienio poveikio veiklą ir užkerta kelią manipuliacijoms informacine erdve. Parlamentiniu lygmeniu šias temas prižiūri nuolatinė komisija hibridinių grėsmių klausimais.

Teisiniu požiūriu, Čekijos baudžiamasis kodeksas numato atsakomybę už veikas, susijusias su melagingų ar nerimą keliančių žinių skleidimu, šmeižtu ir karo propagavimu. 2023 m. policija tyrė kelias dešimtis bylų, susijusių su dezinformacija. Karo propagandos skleidimas pagal BK 407 straipsnį gali būti baudžiamas iki 10 metų laisvės atėmimu.

Įdomus precedentas susiformavo 2025 m., kai Konstitucinis Teismas išteisino aktyvistą, nuteistą už „nerimą keliančių žinių“ skleidimą. Teismas pabrėžė, kad politinė kalba turi būti ypač saugoma, o baudžiamoji atsakomybė už dezinformaciją taikytina tik kaip kraštutinė priemonė – valstybė turėtų pirmiausia remtis viešu faktų tikrinimu ir švietimu.

Čekijos požiūris išsiskiria tuo, kad didžiausias dėmesys skiriamas saugumo institucijų koordinavimui ir visuomenės informuotumui, o ne griežtam turinio ribojimui. Tokiu būdu siekiama išlaikyti pusiausvyrą tarp kovos su manipuliacijomis ir žodžio laisvės apsaugos.



Estija kovoje su dezinformacija remiasi ne siauru teisiniu apibrėžimu, o „visuomenės atsparumo“ ir psichologinės gynybos modeliu. Vyriausybės kanceliarija koordinuoja strateginę komunikaciją ir informacinės erdvės stebėseną; rinkimų vientisumą stiprina Valstybinė rinkimų tarnyba su „i-balsavimo mitų ir realybės“ portalu. Užsienio ir vidaus žvalgyba (Välisluureamet, KAPO) identifikuoja poveikio operacijas, o savanoriška Kaitseliit iniciatyva „Propastop“ vykdo viešą stebėseną. 2024 m. Estija su JAV pasirašė memorandumą dėl kovos su užsienio informacine manipuliacija; valstybė remia kokybišką, įskaitant rusišką, žiniasklaidą, medijų raštingumas yra privalomosiose programose.

Reguliavimo ašis – Vartotojų apsaugos ir techninės reguliavimo tarnyba (TTJA), kuri pagal Žiniasklaidos paslaugų įstatymą gali nurodyti nutraukti retransliavimą, jei kyla grėsmė saugumui; 2022–2023 m. ji masiškai blokavo Rusijos kanalus ir svetaines. Baudžiamasis kodeksas numato atsakomybę už karo propagandą (BK 92 str.: bauda arba iki 3 m. laisvės atėmimo; juridiniams – didelės baudos). Modelis derina technines blokavimo priemones, žvalgybinę analizę ir ilgalaikį atsparumo ugdymą.



Latvijoje kova su dezinformacija organizuota per aiškiai apibrėžtą strateginį valstybinį mechanizmą. 2023 m. Vyriausybės patvirtintoje Nacionalinėje strateginės komunikacijos ir informacinės erdvės saugumo koncepcijoje dezinformacija apibrėžiama kaip melagingas ar klaidinantis turinys, skleidžiamas siekiant apgauti ar gauti politinės ar ekonominės naudos ir galintis pakenkti valstybei ar visuomenei. Vyriausybės kanceliarijos Strateginės komunikacijos koordinavimo skyrius stebi informacinę erdvę, koordinuoja institucijų veiksmus, rengia mokymus ir administruoja platformą „Juodu ant balto“, kurioje gyventojai gali pranešti apie melagingą ar manipuliacinį turinį.

Žiniasklaidos priežiūrą vykdo Nacionalinė elektroninės žiniasklaidos taryba, turinti įgaliojimus sustabdyti ar uždrausti iš trečiųjų šalių retransliuojamą turinį, jei jis kelia grėsmę nacionaliniam saugumui – 2022 m. ji uždraudė apie 80 Rusijos kanalų. Kovos su propaganda funkcijas vykdo Konstitucijos apsaugos biuras ir Valstybės saugumo tarnyba, kurios vertina informacinių atakų mastą, turinį ir grėsmės lygį.

Teisiniame reguliavime 2024 m. įvestas Baudžiamojo įstatymo 901 straipsnis, numatantis atsakomybę už melagingos informacijos apie politinius kandidatus ar partijas kūrimą ir platinimą naudojant „deep fake“ technologijas – iki 5 metų laisvės atėmimo. Be to, 77 straipsnis nustato iki 8 metų laisvės atėmimo bausmę už viešą raginimą imtis agresyvaus karo ar jį skatinti.

Latvijos modelis išsiskiria stipria strateginės komunikacijos koordinacija valstybės lygmeniu, žiniasklaidos priežiūros griežtumu ir naujomis baudžiamosiomis nuostatomis, pritaikytomis kovai su technologiniu manipuliavimu bei užsienio informacinės įtakos formomis.



Lenkijoje nėra atskiro „dezinformacijos“ įstatymo – sąvoka aiškinama vyriausybės ir praktikos dokumentuose, o reguliavimas išskaidytas per nacionalinio saugumo, kibernetinio saugumo ir rinkimų teisę. Strateginiame lygmenyje 2020 m. nacionalinio saugumo strategija numato sisteminę kovą su informacinėmis manipuliacijomis ir visuomenės atsparumo stiprinimą; nacionalinės kibernetinio saugumo sistemos įstatymas ir institucinis tinklas (Skaitmeninio ministerija bei NASK projektas „Przeciwdziałamy dezinformacji“, URM strateginės komunikacijos ir dezinformacijos prevencijos departamentas, #FakeHunter, „Demagog“, kiti NVO) užtikrina stebėseną, faktų tikrinimą ir pranešimų kanalus. Praktinę apsaugą nuo priešiškos propagandos vykdo saugumo ir gynybos institucijos bei žiniasklaidos reguliuotojas KRRiT.

Teisinės priemonės: Baudžiamojo kodekso 130 str. (9 d.) kriminalizuoja užsienio žvalgybų vardu vykdomą dezinformaciją (nuo 8 m. laisvės atėmimo), 117 str. (3 d.) – viešą agresyvaus karo kurstymą ar jam pritarimą (iki 5 m.), Rinkimų kodekso 111 str. leidžia teismui skubiai drausti ir taisyti melagingą kampanijų informaciją, o Telekomunikacijų įstatymo 180 str. įpareigoja operatorius blokuoti ryšius grėsmės nacionaliniam saugumui atvejais. Modelis išsiskiria plačiu instituciniu bendradarbiavimu, greito reagavimo procedūromis rinkimuose ir griežta atsakomybe už valstybei priešišką, užsienio remiamą dezinformaciją.



Prancūzijoje kova su dezinformacija remiasi aiškiu reguliavimu ir tarpžinybiniu veikimu. Centrinė ašis – 2018 m. Įstatymas prieš manipuliavimą informacija: jis suteikia ARCOM įgaliojimus rinkimų laikotarpiu riboti užsienio kontroliuojamų transliuotojų veiklą, įpareigoja didžiąsias platformas dėl skaidrumo (reklamos registrai, pažymėjimo ir pranešimo mechanizmai) ir leidžia taikyti greitąjį teismo „référé“ – per 48 val. stabdyti akivaizdžiai klaidinančio turinio sklaidą likus 3 mėn. iki balsavimo. Valstybinę apsaugą nuo užsienio informacinės įtakos vykdo VIGINUM (stebi, analizuoja ir nustato užsienio skaitmenines intervencijas), o COLMI prie URM koordinuoja operacinį atsaką. Vyriausybė taip pat stiprina švietimą (kritinio mąstymo ir medijų raštingumo nuostatos švietimo kodekse) ir diegia naujus saugiklius – parengtas įstatymo projektas dėl DI sukurtų vaizdų privalomo ženklinimo.

Sankcijų bazė daugiausia kyla iš Spaudos laisvės įstatymo: už melagingų naujienų skleidimą, galintį sutrikdyti viešąją tvarką, – iki 45 tūkst. € (kariniams pajėgumams kenkiančiu atveju – iki 135 tūkst. €); už kurstymą daryti nusikaltimus ar viešą karo nusikaltimų šlovinimą – iki 5 m. laisvės atėmimo. BK taikomas siauriau (pvz., dokumentų klastojimas, žalinga melaginga informacija institucijoms). Terminijoje vartojami „désinformation“, „mésinformation“, „malinformation“, o politikoje ir teisėje – platesnė „manipuliavimo informacija“ sąvoka.



Slovakijoje dezinformacija priskiriama hibridinėms grėsmėms. Praktinį koordinavimą nustatė 2022–2024 m. veiksmų planas: tarpžinybinis bendradarbiavimas, nuolatinė stebėseną ir reagavimas. Žiniasklaidos paslaugų taryba gali įpareigoti platformas šalinti neteisėtą turinį ir taikyti baudas/licencijų ribojimus. Hibridinių grėsmių centras (VRM sistemoje) renka ir analizuoja duomenis, stiprina atsparumą; Nacionalinė saugumo tarnyba gali blokuoti žalingas svetaines kibernetinio saugumo tikslais. Baudžiamosios teisės lygmenyje už „nerimą keliančių pranešimų“ skleidimą – iki 2 m. laisvės atėmimo (BK 361), o už karo propagandą – 1–10 m., sunkinti gali užsienio sąveika, veikimas grupėje ar krizinė situacija (BK 417).

Siūlymai veiksmingesei gynybai informaciniame kare

Įstatymų keitimo paketo tikslas – sukurti vientisą sistemą, kuri gintų demokratiją, visuomenės pasitikėjimą ir valstybės informacinį saugumą šiuolaikinėje skaitmeninėje erdvėje.

Visuomenės informavimo įstatymo pakeitimas

Keičiamo įstatymo esmė:

Įstatymo projektu atnaujinama dezinformacijos sąvoka ir stiprinamas teisinis atsakas į informacines grėsmes. Įstatyme pirmą kartą aiškiai apibrėžiama, kas laikoma dezinformacija – „*Dezinformacija – tai tyčia kuriama, pateikiama, skleidžiama ar platinama melaginga arba klaidinanti informacija, kuria siekiama apgauti visuomenę, paveikti Seimo, Prezidento, Savivaldybių tarybų, Europos parlamento rinkimus, referendumus, pakenkti Lietuvos Respublikos nacionaliniam saugumui, konstitucinei santvarkai, viešajai tvarkai ar kitiems svarbiems visuomenės interesams.*“

Pagrindiniai pakeitimai:

- Įtraukiamos naujos draudžiamos informacijos kategorijos, tarp jų karo propaganda, priešiška ar klaidinanti informacija, kelianti grėsmę valstybės saugumui.
- Išplečiami Žurnalistų etikos inspektoriatų įgaliojimai — jie galės teikti privalomus nurodymus dėl melagingo turinio pašalinimo.
- Įtvirtinamas aiškus reagavimo mechanizmas – institucijos galės greitai ir proporcingai riboti pavojingos informacijos sklaidą.

Šis įstatymo pakeitimas užtikrins teisinį pagrindą greitai reaguoti į dezinformaciją ir sustiprinti valstybės informacinį saugumą.

Informacinės visuomenės paslaugų įstatymo papildymas

Keičiamo įstatymo esmė:

Projektu siekiama nustatyti socialinių tinklų, vaizdo platformų ir naujienų agregatorių atsakomybę už melagingos informacijos sklaidą ir įpareigoti juos bendradarbiauti su valstybės institucijomis.

Pagrindiniai pakeitimai:

- Įtvirtinama pareiga taikyti technines ir organizacines priemones (žymėti, riboti ar šalinti melagingą turinį).
- Numatyta administracinė atsakomybė už institucijų sprendimų nevykdymą.

Šis įstatymas sustiprins visuomenės atsparumą dezinformacijai, užtikrins platformų atsakomybę ir veiksmingą institucijų bendradarbiavimą kovojant su melagingu turiniu.

Elektroninių ryšių įstatymo papildymas

Keičiamo įstatymo esmė:

Projektu siekiama užkirsti kelią piktnaudžiavimui automatizuota įranga, naudojama neteisėtai veiklai elektroninių ryšių tinkle – masinėms žinutėms, skambučiams ar sukčiavimo atvejams vykdyti.

Pagrindiniai pakeitimai:

- Apibrėžiama automatizuota abonento identifikavimo modulių naudojimo įranga – priemonė, leidžianti vienu metu ar pakaitomis valdyti penkis ir daugiau SIM kortelių ir automatizuotai vykdyti ryšio veiksmus.
- Įtvirtinamas draudimas įsigyti, naudoti, laikyti ar gabenti tokią įrangą, išskyrus elektroninių ryšių veiklą vykdančius asmenis.

Šis įstatymas sumažins automatizuoto sukčiavimo ir šlamšto mastą, sustiprins vartotojų apsaugą bei ryšių tinklų saugumą.

Administracinių nusižengimų kodekso papildymas

Keičiamo įstatymo esmė:

Projektu siekiama nustatyti atsakomybę už neteisėtą automatizuotos SIM kortelių (abonento identifikavimo modulių) įrangos naudojimą ir už dezinformacijos skleidimą, kai tokia veikla kelia grėsmę valstybės saugumui ar demokratiniais procesams.

Pagrindiniai pakeitimai:

- Nustatoma administracinė atsakomybė už neteisėtą automatizuotos SIM įrangos įsigijimą, naudojimą, laikymą ar gabenimą; pakartotinai padarius nusižengimą – didesnės baudos ir privalomas įrangos konfiskavimas. Baudos asmenims – nuo 1 000 iki 3 000 eurų, pakartotinio nusižengimo atveju – iki 6 000 eurų.
- Į kodeksą įtraukiamas naujas 507² straipsnis, numatantis baudą už tyčinį dezinformacijos kūrimą, pateikimą ar skleidimą, kai siekiama apgauti visuomenę ar pakenkti valstybės interesams. Baudžiamas nuo dviejų šimtų iki trijų tūkstančių eurų bauda.
- Patikslinamos 589 straipsnio nuostatos dėl institucijų kompetencijos nagrinėti šiuos nusižengimus.

Šie pakeitimai sustiprins teisinį atsaką į informacinės grėsmes, sudarys sąlygas veiksmingiau riboti automatizuoto sukčiavimo ir dezinformacijos plitimą bei užtikrins institucijų koordinuotą veikimą.

Baudžiamojo kodekso papildymas

Keičiamo įstatymo esmė:

Įstatymo projektu siekiama nustatyti baudžiamąją atsakomybę už priešišku valstybių vykdomą informacinę veiklą prieš Lietuvos Respubliką bei už agresyvaus karo propagavimą.

Pagrindiniai pakeitimai:

- Į Baudžiamąjį kodeksą įtraukiamas 118¹ straipsnis, nustatantis atsakomybę už veikimą kitos valstybės pavedimu, kai rengiamas ar platinamas melagingas turinys, siekiant pakenkti Lietuvos nacionaliniam saugumui ar konstitucinei santvarkai. Baudžiamas bauda, areštu arba laisvės atėmimu iki penkerių metų.
- Papildomas 118² straipsnis, numatantis atsakomybę už viešą agresyvaus karo kurstymą ar pateisinimą, kai tokia veikla pažeidžia tarptautinės teisės principus. Už šias veikas numatyta bauda, areštas arba laisvės atėmimas iki penkerių metų.

Šie pakeitimai sustiprins valstybės atsparumą priešiskai informacinei veiklai, užkirs kelią karo propagandai ir pabrėš baudžiamąją atsakomybę už veiksmus, keliančius grėsmę Lietuvos nacionaliniam saugumui ar konstitucinei santvarkai.

O kas toliau?

Šiuo įstatymų paketu žengiame tik pirmą, tačiau itin svarbų žingsnį siekiant pažaboti kremliaus dezinformaciją, klaidinančią propagandą ir technologinius įrankius, kurie kelia tiesioginę grėsmę mūsų valstybės saugumui. Efektyvi kovos su dezinformacija strategija turi būti daugiasluoksni ir nuosekli, apimanti ne tik teisėkūros sprendimus, bet ir technologines, komunikacines bei švietimo priemones. Tik taip galime užtikrinti ilgalaikį visuomenės atsparumą.

Kova su dezinformacija yra investicija į valstybės saugumą — tai ne vien įstatymų leidybos uždavinys, bet ir investicija į visuomenės sąmoningumą, nepriklausomą žiniasklaidą, technologinį budrumą ir tarptautinį bendradarbiavimą.

1. Reguliavimo stiprinimas nacionaliniame ir ES lygmenyje

- | | |
|--|---|
| <ul style="list-style-type: none">• Sukurti aiškesnius interneto platformų veiklos reikalavimus, įskaitant skaidrumo ataskaitas, pareigą turėti vietinius atstovus ir greito reagavimo kanalus.• Įtvirtinti atsakomybę už nenukreiptą ar neveiksmingą bendradarbiavimą su nacionalinėmis institucijomis.• Į teisės aktus įtraukti ir dirbtinio intelekto (AI) bei “deepfake” turinio atpažinimo bei žymėjimo nuostatas – tam, kad melagingai sukurtas audiovizualinis turinys negalėtų būti naudojamas manipuliacijai, rinkimams ar valstybės saugumui kenkiančioms kampanijoms. | <ul style="list-style-type: none">• Privalumai: aiškesnė atsakomybė, didesnis skaidrumas, efektyvesnė priežiūra.• Rizikos: laisvės ribojimo interpretacijos, galimi teisiniai ginčai su tarptautinėmis platformomis. |
|--|---|

2. Nacionalinis greito reagavimo modelis

- | | |
|--|---|
| <ul style="list-style-type: none">• Sukurti nacionalinį „rapid response“ mechanizmą, jungiantį RRT, NKVC, VSD, ŽEIT, LRTK, kariuomenės Strateginės komunikacijos departamentą ir pilietinės visuomenės partnerius.• Modelis turėtų gebėti realiuoju laiku identifikuoti koordinuotas dezinformacijos ir deepfake kampanijas bei greitai reaguoti – per kelias valandas, o ne savaites.• Įtraukti automatizuotus signalų aptikimo algoritmus, bendradarbiauti su žiniasklaidos priemonėmis ir faktų tikrintojais. | <ul style="list-style-type: none">• Privalumai: greita kontrapropagandinė reakcija, stipresnis visuomenės pasitikėjimas.• Rizikos: dideli resursų poreikiai, būtinas institucinis koordinavimas. |
|--|---|

3. Informacinis raštingumas ir švietimas

- | | |
|---|---|
| <ul style="list-style-type: none">• Įgyvendinti masinę informacinio atsparumo kampaniją: nuo programų mokyklose iki viešųjų kursų visuomenei.• Sukurti specialias edukacines priemones pažeidžiamoms grupėms – vyresnio amžiaus žmonėms, regioninėms bendruomenėms, jaunimui.• Įtraukti deepfake ir AI turinio atpažinimo mokymus tiek švietimo, tiek žurnalistikos ir viešojo sektoriaus darbuotojams. | <ul style="list-style-type: none">• Privalumai: ilgalaikis atsparumo augimas, mažėjantis manipuliacijų poveikis.• Rizikos: reikalauja nuoseklumo, poveikis matomas tik ilginiui. |
|---|---|

4. Parama nepriklausomai žiniasklaidai ir faktų tikrintojams

- Užtikrinti finansinę ir institucinę paramą nepriklausomiems žurnalistams, redakcijoms ir faktų tikrintojams, ypač regionuose.
- Stiprinti jų saugumo, teisinės gynybos ir technologinius pajėgumus, kad jie galėtų veikti nepriklausomai nuo politinių ar ekonominių spaudimų.
- Sukurti ilgalaikį žiniasklaidos atsparumo fondą, kuris remtų tiriamosios žurnalistikos, medijų raštingumo ir dezinformacijos tyrimų projektus.
- **Privalumai:** išlaikomas pluralizmas, mažinamas informacinis vakuumas, didėja visuomenės pasitikėjimas.
- **Rizikos:** būtinas pastovus finansavimas ir skaidrus paskirstymo mechanizmas.

5. Technologinė gynyba ir inovacijos

- Investuoti į dirbtinio intelekto įrankius, kurie automatiškai aptinka koordinuotas dezinformacijos kampanijas, netikras paskyras ir deepfake turinį.
- Skatinti viešojo ir privataus sektoriaus partnerystės inovacijoms informacinės gynybos srityje.

6. Socialinių tinklų atsakomybė ir apmokestinimas

- Įvesti socialinių tinklų atsakomybės mokestį („Digital Responsibility Levy“), pagal kurį dalis Lietuvoje sugeneruotų didžiųjų platformų („Meta“, „TikTok“, „X“, „YouTube“) pajamų būtų nukreipiama į Viešosios informacijos atsparumo fondą.
- Fondo lėšos būtų skirtos faktų tikrinimo iniciatyvoms, nepriklausomos žiniasklaidos stiprinimui, medijų raštingumo ir inovatyvių dezinformacijos atpažinimo technologijų kūrimui.
- Nustatyti aiškius platformų atsakomybės standartus – reagavimo į institucijų prašymus terminus, privalomą vietinių atstovų buvimą Lietuvoje ir turinio moderavimo atskaitomybę.
- Skatinti ES lygmens iniciatyvą, kad technologijų gigantai prisidėtų prie informacinės erdvės apsaugos ir demokratijos stiprinimo, o nacionaliniu lygmeniu – užtikrinti jų veiklos skaidrumą bei atsakomybę.
- **Privalumai:** užtikrinamas platformų atsakomybės principas, sukuriamas tvarus finansavimo šaltinis kovai su dezinformacija, stiprinama nepriklausoma žiniasklaida.
- **Rizikos:** gali kilti teisiniai ginčai dėl ES konkurencijos ir mokesčių teisės, būtina užtikrinti aiškią skaidrumo sistemą ir politinį neutralumą.