



NACIONALINĖ TEISĖS ŽINIŲ OLIMPIADA

„Internetas, dirbtinis intelektas ir teisė: galimybės ir grėsmės“ (Mokomoji medžiaga)



Mykolas Romeris
universitetas



NACIONALINĖ TEISĖS ŽINIŲ OLIMPIADA

„Internetas, dirbtinis intelektas ir teisė: galimybės ir grėsmės“



Dirbtinis Intelektas (DI) pats negali teisiškai ar moraliai atsakyti už savo veiksmus

Atsakomybė visais atvejais tenka žmogui, įmonei ar kitam teisės subjektui, kuris kuria, valdo arba naudoja šią technologiją.

Pagrindiniai argumentai, kodėl DI nėra laikomas atsakingu subjektu:

- Teisinio subjektiškumo trūkumas: Šiuo metu DI sistemos nėra pripažįstamos teisės subjektais, nes jos neturi „teisnumo“ (priklausymo teisės subjektų kategorijai) ir „veiknumo“ (galėjimo įgyvendinti teises ir susikurti civilines pareigas). Kol DI neturi asmenybės statuso, jis vertinamas kaip įrankis, o ne kaip savarankiškas veikėjas.



Mykolas Romeris
universitetas



Dirbtinis Intelektas (DI) pats negali teisiškai ar moraliai atsakyti už savo veiksmus

Atsakomybės paskirstymas tarp žmonių:

Operatoriaus atsakomybė: Dažniausiai už žalą atsako sistemos operatorius – asmuo ar verslas, kuris kontroliuoja riziką ir gauna naudos iš DI veikimo.

Gamintojo atsakomybė: Jei žala kyla dėl programinės įrangos defektų ar netinkamo informavimo apie rizikas, atsakomybė gali tekti gamintojui.

Griežtoji atsakomybė: Siūloma DI sistemas prilyginti didesnio pavojaus šaltiniui. Tai reiškia, kad valdytojas būtų atsakingas už bet kokią sukeltą žalą, net jei jis tiesiogiai nesuklydo, nes pasirinko naudoti potencialiai rizikingą technologiją.



Mykolas Romeris
universitetas



Dirbtinis Intelektas (DI) pats negali teisiškai ar moraliai atsakyti už savo veiksmus

„Juodosios dėžės“ problema: Nors DI sprendimų priėmimo procesai dažnai yra nepermatomi net jų kūrėjams (vadinamoji „juodoji dėžė“), tai neatleidžia žmonių nuo atsakomybės. Teisinės sistemos siekia užtikrinti, kad nukentėjusysis visada turėtų subjektą, iš kurio galėtų reikalauti žalos atlyginimo.

ES reglamentavimas (DI aktas): Nuo 2026 m. įsigaliosiantis ES Dirbtinio intelekto aktas įtvirtina nuostatą, kad sprendimai, darantys poveikį asmenims, visada privalo turėti atsakingą subjektą, nepriklausomai nuo to, ar sprendimą priėmė algoritmas. Dokumente pabrėžiama, kad dirbtinio intelekto sistemas privalo prižiūrėti žmonės, o ne automatizavimas.



Mykolas Romeris
universitetas



Dirbtinis Intelektas (DI) pats negali teisiškai ar moraliai atsakyti už savo veiksmus

Apibendrinant: kadangi DI neturi emocijų, savarankiškų tikslų ar moralinių vertybių, jis negali pats būti etiškas ar atsakingas – tai išlieka išskirtine žmogaus pareiga.



Mykolas Romeris
universitetas



Skaitmeniniu pėdsakas arba skaitmeninis šešėlis

Internetas turi itin ilgą atmintį, kurią specialistai vadina skaitmeniniu pėdsaku arba skaitmeniniu šešėliu. Tai unikali jūsus sekamų skaitmeninių veiksmų, indėlių ir komunikacijos visuma, kuri kaupiama internete bei skaitmeniniuose įrenginiuose.



Mykolas Romeris
universitetas



Skaitmeniniu pėdsakas arba skaitmeninis šešėlis

Štai kaip internetas „atsimena“ jūsų veiklą:

- Pasyvus ir aktyvus pėdsakas: Internetas fiksuoja tiek tai, ką darote sąmoningai (keliate nuotraukas, rašote įrašus socialiniuose tinkluose, pildote anketas), tiek tai, ką paliekate nesąmoningai (IP adresą, naršymo istoriją, slapukus, geolokaciją bei įrenginio informaciją).
- Kur saugoma informacija: Jūsų veiksmų duomenys nugula daugybėje serverių, priklausančių interneto tiekėjams, svetainių savininkams, programėlių kūrėjams ir reklamos tinklams. Pavyzdžiui, „Google“ ekosistema renka duomenis apie lytį, amžių, pomėgius ir net buvimo vietą per visas savo naudojamąs programas.



Mykolas Romeris
universitetas



Skaitmeniniu pėdsakas arba skaitmeninis šešėlis

Ar internetas atsimena praėjusią vasarą?

O Taip, pavyzdžiui, jei jūsų paskyroje įjungta „Google Maps“ laiko juosta, galite tiksliai matyti visus maršrutus, aplankytus miestus ar vietas, kuriose buvote praėjusią vasarą ar dar seniau.

O Socialiniai tinklai veikia kaip asmeninio ir profesinio gyvenimo tęsinys, kuriame saugomi metų metai prisiminimų, pokalbių ir turinio.

O Egzistuoja tokie įrankiai kaip „Wayback Machine“, kurie archyvuoja milijardus interneto puslapių ir leidžia pamatyti, kaip jie atrodė prieš daugelį metų, net jei savininkas juos vėliau pakeitė.



Mykolas Romeris
universitetas



Skaitmeniniu pėdsakas arba skaitmeninis šešėlis

Ištrynimo sudėtingumas: Net jei ištrinate naršymo istoriją savo įrenginyje, informacija dažnai lieka susieta su jūsų internetine paskyra ir sinchronizuojama per visus prijungtus įrenginius. Be to, panaikinus socialinio tinklo paskyrą, apie jus surinkti duomenys nebūtinai bus ištrinti.

Nuspėjamumas: Analizuojant jūsų pėdsaką, algoritmai gali nuspėti net ir tokius asmeninius bruožus kaip jūsų intelekto lygį, religines ar politines pažiūras bei seksualinę orientaciją, net jei niekada to viešai neatskleidėte.



Mykolas Romeris
universitetas



Skaitmeniniu pėdsakas arba skaitmeninis šešėlis

Nors egzistuoja „teisė būti pamirštam“, leidžianti prašyti ištrinti jūsų asmens duomenis, tai nėra absoliuti teisė ir jos įgyvendinimas yra sudėtingas procesas, nes informacija internete dažnai yra tarpusavyje susieta ir išsibarsčiusi po skirtingas organizacijas.



Mykolas Romeris
universitetas



Skaitmeninė reputacija

Skaitmeninė reputacija – tai praktika, kuria stebimas ir prižiūrimas visuomenės požiūris į asmenį ar įmonę internete, formuojamas remiantis skaitmeniniu turiniu, socialinių tinklų profiliais, atsiliepimais bei paieškos sistemų rezultatais. Teigiama skaitmeninė reputacija yra kritiškai svarbi, nes ji padeda kurti pasitikėjimą, patikimumą bei pritraukti naujų galimybių, o neigiama – gali pakenkti profesiniams santykiams ar net sukelti finansinių nuostolių. Kiekvienas veiksmas internete, pavyzdžiui, impulsyvus komentaras ar nuotrauka, sukuria skaitmeninį pėdsaką, kuris gali iškilti po daugelio metų ir negrįžtamai paveikti asmens įvaizdį.



Mykolas Romeris
universitetas



Skaitmeninė reputacija

Atsakant į klausimą dėl informacijos šalinimo, visiškai ištrinti visą informaciją apie save iš interneto yra praktiškai neįmanoma. Nors egzistuoja teisiniai mechanizmai ir įrankiai, padedantys valdyti savo tapatybę, štai pagrindinės priežastys, kodėl visiškai „išsitrynimas“ yra sudėtingas:

1) Teisė būti pamirštam nėra absoliuti: įgyvendinant šią teisę, informacija paprastai pašalinama tik iš paieškos variklių (pvz., „Google“) rezultatų, tačiau ji išlieka pirminiuose šaltiniuose – svetainėse, kuriose buvo paskelbta.



Mykolas Romeris
universitetas



Skaitmeninė reputacija

2) Organizacijų teisė saugoti duomenis: Prašymas ištrinti duomenis gali būti atmestas, jei informacija yra svarbi viešajam interesui, saviraiškos laisvei, moksliniams tyrimams arba jei egzistuoja teisinė prievolė tuos duomenis saugoti.

3) Duomenų kopijavimas ir sklaida: Skaitmeninėje erdvėje turinys gali būti akimirksniu nukopijuotas ir perpublikuotas kitur, todėl asmuo praranda jo kontrolę.



Mykolas Romeris
universitetas



Skaitmeninė reputacija

4) Paskyrų trynimo ribotumas: Net ir panaikinus socialinio tinklo paskyrą, apie jus surinkti duomenys nebūtinai ištrinami iš platformos serverių. Be to, dalis informacijos gali būti patekusi į duomenų brokerių rankas, iš kurių ją pašalinti yra itin sudėtinga.

5) Archyvavimo sistemos: Tokie įrankiai kaip „Wayback Machine“ nuolat fiksuoja ir saugo interneto puslapių kopijas, kurios leidžia pamatyti, kaip svetainės atrodė praeityje, net jei jų savininkai turinį vėliau pakeitė ar ištrynė.



Mykolas Romeris
universitetas



Teisė būti pamirštam

Teisė būti pamirštam (dar žinoma kaip teisė reikalauti ištrinti duomenis) yra asmens teisė tam tikromis aplinkybėmis reikalauti, kad duomenų valdytojai (pavyzdžiui, interneto paieškos sistemos ar kitos platformos) pašalintų su juo susijusius asmeninius duomenis. Ši teisė leidžia asmeniui kontroliuoti savo skaitmeninę tapatybę ir siekti, kad informacija, kuri nebėra aktuali ar yra žalinga, nebebūtų prieinama trečiosioms šalims.



Mykolas Romeris
universitetas



Teisė būti pamirštam

Kada ši teisė taikoma?

Remiantis Bendruoju duomenų apsaugos reglamentu (BDAR) ir teismų praktika, asmuo gali prašyti ištrinti duomenis šiais atvejais:

1. Nebėra poreikio: Asmens duomenys nebėra reikalingi tiems tikslams, kuriais jie buvo renkami.
2. Atšaukiamas sutikimas: Asmuo atšaukia savo sutikimą tvarkyti duomenis ir nėra kito teisinio pagrindo tai daryti.
3. Neteisėtas tvarkymas: Duomenys buvo tvarkomi nesilaikant įstatymų.
4. Prieštaravimas: Asmuo nesutinka su duomenų tvarkymu (pvz., tiesioginės rinkodaros tikslais).
5. Teisinė prievolė: Duomenys privalo būti ištrinti laikantis ES ar nacionalinės teisės aktų.
6. Informacija yra „neadekvati“: Duomenys tapo neadekvatūs, nebereikšmingi arba pertekliniai, atsižvelgiant į laiką ir pirminį jų paskelbimo tikslą.



Mykolas Romeris
universitetas



Teisė būti pamirštam

Svarbu pabrėžti, kad ši teisė nėra absoliuti. Prašymas gali būti atmestas, jei duomenys yra būtini saviraiškos ir informacijos laisvei, viešajam interesui (pvz., sveikatos apsaugai), moksliniams tyrimams ar teisiniams reikalavimams vykdyti.

Be to, įgyvendinus šią teisę paieškos sistemose, informacija dažniausiai pašalinama tik iš rezultatų sąrašo, tačiau ji gali išlikti pirminiuose šaltiniuose.



Mykolas Romeris
universitetas



Kaip ankstesnė veikla internete veikia ateitį?

Praeities veiksmai internete sukuria skaitmeninį pėdsaką (arba šėšėlį), kuris išlieka ilgą laiką ir gali turėti lemtingos įtakos. Štai pagrindiniai būdai, kaip tai veikia jūsų ateitį:

1. Profesinės galimybės ir karjera: Vis daugiau darbdavių tikrina kandidatų skaitmeninį pėdsaką socialiniuose tinkluose prieš priimdami į darbą. Netinkama kalba, neprofesionalūs vaizdai ar įrašai apie narkotikų bei alkoholio vartojimą gali lemti neigiamą vertinimą.



Mykolas Romeris
universitetas



Kaip ankstesnė veikla internete veikia ateitį?

2. Mokslas ir studijos: Aukštosios mokyklos taip pat analizuoja būsimų studentų veiklą internete. Pavyzdžiui, Harvardo universitetas yra atšaukęs priėmimo pasiūlymus studentams dėl jų įžeidžiančių žinučių socialiniuose tinkluose.

3. Reputacija ir visuomenės suvokimas: Internetas „atsimena“ jūsų praeities klaidas, neapgalvotus žodžius ar skandalus. Spontaniškas įrašas ar nuotrauka gali iškilti po daugelio metų ir tapti nuolatine jūsų įvaizdžio dalimi.



Mykolas Romeris
universitetas



Kaip ankstesnė veikla internete veikia ateitį?

4. Finansinis poveikis: Skaitmeninis pėdsakas gali būti naudojamas vertinant asmens kreditingumą ar net nustatant draudimo įmokas.

5. Saugumo rizikos: Pernelyg gausus asmeninės informacijos dalijimasis praeityje didina tapatybės vagystės riziką ateityje.



Mykolas Romeris
universitetas



Kaip ankstesnė veikla internete veikia ateitį?

Kadangi bet kas internete gali būti nukopijuota ir persiųsta akimirksniu, asmuo praranda pirminę informacijos kontrolę, o jo praeitis tampa prieinama milžiniškai, nematomi auditorijai.



Mykolas Romeris
universitetas



Kaip veikia apgavystės ir manipuliacija?

Internetas gali būti galingas įrankis ne tik informacijos sklaidai, bet ir manipuliacijai, spaudimui ar apgaulei, pasitelkiant vis tobulesnes technologijas.



Mykolas Romeris
universitetas



Kaip veikia apgavystės ir manipuliacija?

- Deepfake (Sintetinis vaizdo ir garso klastojimas): Tai dirbtinio intelekto technologija, kuri leidžia sukurti itin tikrovišką vaizdo ar garso turinį, sukeičiant asmenų veidus ar balsus. Tokiu būdu sudaromas vaizdas, kad žmogus sako ar daro tai, ko niekada nėra sakęs ar daręs. Ši technologija gali būti naudojama reputacijai griauti, šantažui (pvz., kuriant pornografinio turinio klastotes) ar dezinformacijai skleisti.
- Melaginga informacija ir dezinformacija: Sąmoningai klaidinanti informacija naudojama siekiant kontroliuoti žmonių elgesį, įsitikinimus, sukelti visuomenės nepasitikėjimą ar pasipelnyti krizinėse situacijose. Botai (netikri profiliai) leidžia melagingoms naujienoms plisti žaibiškai, pasiekiant tūkstančius žmonių per kelias sekundes.



Mykolas Romeris
universitetas



Kaip veikia apgavystės ir manipuliacija?

- Duomenų išviliojimas (Phishing) ir tapatybės vagystės: Sukčiai naudoja el. laiškus ar svetaines, kurios atrodo kaip tikros, kad išviliotų prisijungimo duomenis, banko informaciją ar pavogtų asmens tapatybę. Suasmenintas išviliojimas (Spearphishing) yra dar pavojingesnis, nes sukčius naudoja apie jus jau žinomą informaciją, kad apgautų įtikinamiau.
- Apsimetinėjimas (Catfishing): Socialiniuose tinkluose kuriami netikri profiliai siekiant užmegzti ryšį ir išvilioti asmeninę informaciją.



Mykolas Romeris
universitetas



Kaip atpažinti, kada technologijos naudojamos prieš tave?

Atidumas detalėms yra pagrindinis būdas atpažinti klastą:

1. Deepfake požymiai: Stebėkite vaizdo įrašų keistumus: iškraipytus tekstus, dingstančius objektus, fizikos dėsniams prieštaraujančius judesius ar nenatūralią veido mimiką. Taip pat verta ieškoti DI žymėjimų arba tikrinti metaduomenis (informaciją apie vaizdo kilmę).

2. Svetainių ir nuorodų tikrinimas: Įtartini URL adresai (pvz., papildomos raidės ar kiti domenų galai), „https://“ protokolo nebuvimas ar per daug geri pasiūlymai dažnai signalizuoja apie sukčiavimą.



Mykolas Romeris
universitetas



Kaip atpažinti, kada technologijos naudojamos prieš tave?

3. Netikrų profilių požymiai: Naujos paskyros su mažai įrašų, neryškios profilio nuotraukos (arba jų vogtos kopijos), mažas draugų skaičius ir nerišliai pateikta informacija „Apie mane“ turėtų kelti abejonių.

4. Kritinis vertinimas: Jei matoma naujiena skamba šokiruojančiai, naudokitės „3 žingsnių metodu“: vadovaukitės sveiku protu, kelkite klausimus apie šaltinio kompetenciją ir motyvus bei patikrinkite, ar tą pačią informaciją skelbia kiti patikimi šaltiniai.



Mykolas Romeris
universitetas



Kaip technologijos padeda apsiginti?

Nors technologijos sukuria rizikų, jos taip pat suteikia priemonių gintis:

- Saugumo įrankiai: Naudokite stiprius slaptažodžius, slaptažodžių tvarkykles, ugniasienes ir dviejų pakopų patvirtinimą (2FA), kuris sukuria papildomą barjerą sukčiams.
- Privatumo nustatymai: Galimybė patiems kontroliuoti, kas mato jūsų informaciją, draugų sąrašą ar buvimo vietą, padeda sumažinti jūsų „skaitmeninį pėdsaką“, kurį galėtų panaudoti piktavaliai.
- Įrodymų rinkimas: Jei susiduriate su priekabiavimu ar apgaule, technologijos leidžia pasidaryti ekrano nuotraukas (screenshots), kurios tampa svarbiais įrodymais kreipiantis pagalbos į suaugusiuosius ar teisėsaugą.



Mykolas Romeris
universitetas



Kaip technologijos padeda apsiginti?

- Teisė būti pamirštam: ES piliečiai gali naudotis teisiniais ir techniniais mechanizmais prašydami „Google“ ar kitų platformų pašalinti neadekvačią, pasenusią ar asmens privatumą pažeidžiančią informaciją iš paieškos rezultatų.
- Specializuoti paslaugų įrankiai: Egzistuoja paslaugos, kurios padeda surasti nenaudojamas paskyras arba automatiškai išsiunčia prašymus duomenų brokeriams ištrinti jūsų asmeninius duomenis.



Mykolas Romeris
universitetas



Ką reiškia sutikti su platformų taisyklėmis?

Sutikimas su platformų taisyklėmis ir privatumo politika reiškia, kad vartotojas leidžia paslaugų teikėjui tvarkyti jo asmens duomenis ir informaciją nurodytais tikslais. Tai dažnai apima:

- Slapukų naudojimą: sutinkama, kad svetainė į įrenginį įrašytų nedidelius failus, kurie padeda suasmeninti turinį, reklamas ir analizuoti srautą.
- Elgesio taisyklių laikymąsi: vartotojas įsipareigoja neplatinti neteisėto turinio, o platforma įgyja teisę moderuoti arba šalinti taisykles pažeidžiančius įrašus.
- Atsakomybės pasidalijimą: pavyzdžiui, „Facebook“ atveju, už duomenų rinkimą ir tvarkymą bendrai atsakingi ir platformos valdytojas, ir puslapio, kuriame lankotės, administratorius.



Mykolas Romeris
universitetas



Kokią informaciją apie tave renka socialiniai tinklai?

Socialiniai tinklai renka itin platų spektrą duomenų, kurie tampa jų pagrindiniu pajamų šaltiniu. Ši informacija skirstoma į kelias grupes:

- Tapatybės ir kontaktiniai duomenys: vardas, pavardė, asmens kodas, gimimo data, adresas, telefono numeris, el. pašto adresas.
- Elgesio duomenys: prisijungimo laikas ir vieta, tinkle praleidžiama trukmė, paieškos užklauskos, lankomi kitų vartotojų ar įmonių puslapiai, domėjimasis tam tikra reklama.
- Sąveikos ir aktyvumas: paspaudimai „patinka“, prenumeratos, komentarai, reakcijos į įrašus, vaizdo įrašų peržiūros, naudojami prietaisai, kalba ir interesai.
- Trečiųjų šalių duomenys: jei naudojate socialiniame tinkle siūlomais žaidimais ar programėlėmis, jų kūrėjai taip pat gali matyti jūsų viešą bei dalį privačios informacijos.



Mykolas Romeris
universitetas



Ar platformos gali ištrinti tavo turinį ar paskyrą?

Taip, platformos gali šalinti turinį arba sustabdyti paskyros veikimą. Pagal Skaitmeninių paslaugų aktą (SPA), platformos privalo kovoti su neteisėtu turiniu, neapykantą kurstančia kalba ir dezinformacija. Svarbu žinoti:

- Skaidrumas: jei jūsų turinys pašalinamas, platforma privalo paaiškinti, kodėl tai buvo padaryta.
- Apskundimas: vartotojai turi teisę užginčyti turinio moderavimo sprendimus per pačią platformą arba kreiptis į neteisminio ginčų sprendimo įstaigas.



Mykolas Romeris
universitetas



Kokia atsakomybė kyla už reklamos, konkursų ar kitų veiklų vykdymą?

Vykdant komercinę veiklą socialiniuose tinkluose, galioja griežti reikalavimai, ypač dėl reklamos žymėjimo:

- Žymėjimo prievolė: bet kokia reklamos forma turi būti aiškiai atpažįstama (naudojamos grotažymės #reklama arba Reklama), o paslėpta reklama yra draudžiama.
- Pasidalinta atsakomybė: už teisingą žymėjimą yra atsakingas ir reklamos užsakovas (prekės ženklas), ir nuomonės formuotojas (influenceris).
- Baudos: Lietuvoje už paslėptą reklamą, taiko tūkstantines baudas.



Mykolas Romeris
universitetas



Kaip apsaugoti save ir artimuosius nuo finansinių ir tapatybės vagysčių?

Ekspertai pataria derinti technines priemones ir budrumą:

- Naudokite dviejų dalių autentifikavimą (2FA): tai vienas efektyviausių būdų, nes prisijungimui reikia ne tik slaptažodžio, bet ir antros patvirtinimo formos (kodo į telefoną, biometrinių duomenų).
- Sukurkite stiprius slaptažodžius: naudokite daugiau nei 10–12 simbolių su skaičiais ir specialiais ženklais, nenaudokite to paties slaptažodžio keliose paskyrose.



Mykolas Romeris
universitetas



Kaip apsaugoti save ir artimuosius nuo finansinių ir tapatybės vagysčių?

- Būkite budrūs dėl sukčiavimo (phishing): nepasitikėkite laiškais, kuriuose prašoma asmeninių duomenų, banko prisijungimų, net jei jie atrodo kaip siųsti žinomų institucijų. Tikrinkite siuntėjo adresą ir nuorodas (svetainė turi naudoti saugų https protokolą).
- Ribokite viešinamą informaciją: neviešinkite namų adreso, asmens kodo, telefono numerio ar informacijos apie tai, kad esate išvykę atostogauti.
- Apsaugokite vaikus: kalbėkitės apie grėsmes, naudokite tėvų kontrolės programas ir administratoriaus teisių ribojimą naršymo metu.
- Naudokite saugumo įrankius: VPN ryšio užšifravimui (ypač viešajame Wi-Fi) bei antivirusines programas kenkėjiškos įrangos prevencijai.



Mykolas Romeris
universitetas



Kaip apsaugoti save ir artimuosius nuo finansinių ir tapatybės vagysčių?

- Būkite budrūs dėl sukčiavimo (phishing): nepasitikėkite laiškais, kuriuose prašoma asmeninių duomenų, banko prisijungimų, net jei jie atrodo kaip siųsti žinomų institucijų. Tikrinkite siuntėjo adresą ir nuorodas (svetainė turi naudoti saugų https protokolą).
- Ribokite viešinamą informaciją: neviešinkite namų adreso, asmens kodo, telefono numerio ar informacijos apie tai, kad esate išvykę atostogauti.
- Apsaugokite vaikus: kalbėkitės apie grėsmes, naudokite tėvų kontrolės programas ir administratoriaus teisių ribojimą naršymo metu.
- Naudokite saugumo įrankius: VPN ryšio užšifravimui (ypač viešajame Wi-Fi) bei antivirusines programas kenkėjiškos įrangos prevencijai.



Mykolas Romeris
universitetas



Svarbu atsiminti

Gyvename laikais, kai internetas, socialiniai tinklai ir dirbtinis intelektas tapo neatsiejama kasdienio gyvenimo dalimi. Skaitmeninės technologijos suteikia didžiules galimybes mokytis, bendrauti, kurti ir dalintis informacija. Tačiau kartu jos sukuria ir naujų rizikų, susijusių su privatumu, reputacija, manipuliacija informacija bei kibernetiniais nusikaltimais.



Mykolas Romeris
universitetas



Svarbu atsiminti

Todėl kiekvienas interneto vartotojas turi suprasti, kad skaitmeninis pasaulis nėra visiškai anonimiškas ar be taisyklių. Internetinėje erdvėje galioja tie patys teisiniai ir etiniai principai kaip ir realiame gyvenime. Už savo veiksmus, komentarus ar paskelbtą turinį žmogus gali būti atsakingas teisiškai.



Mykolas Romeris
universitetas



Svarbu atsiminti

Svarbu suvokti, kad kiekvienas įrašas, nuotrauka ar komentaras gali sukurti ilgalaikį skaitmeninį pėdsaką, kuris ateityje gali turėti įtakos žmogaus reputacijai, studijoms ar karjerai. Todėl prieš dalijantis informacija verta pagalvoti, kokias pasekmes tai gali turėti ateityje.



Mykolas Romeris
universitetas



Svarbu atsiminti

Kartu svarbu žinoti ir savo teises. Europos Sąjungos teisė suteikia galimybių ginti savo privatumą, reikalauti pašalinti neteisėtai tvarkomus duomenis, apskusti platformų sprendimus ar kreiptis į institucijas, jei pažeidžiamos jūsų teisės.



Mykolas Romeris
universitetas



Svarbu atsiminti

Skaitmeniniame pasaulyje svarbiausia yra ne tik technologijos, bet ir kritinis mąstymas, atsakomybė bei pagarba kitų žmonių teisėms.



Mykolas Romeris
universitetas



Aukštinės taisyklės gyvenant skaitmeniniame pasaulyje

1. Pagalvok prieš paskelbdamas. Kiekvienas įrašas, nuotrauka ar komentaras gali išlikti internete ilgus metus ir turėti įtakos tavo reputacijai ateityje.
2. Saugok savo asmens duomenis. Neviešink jautrios informacijos – adreso, dokumentų duomenų, telefono numerio ar finansinės informacijos.
3. Naudok stiprius slaptažodžius ir dviejų veiksmų autentifikaciją. Tai vienas efektyviausių būdų apsaugoti paskyras nuo įsilaužimų.
4. Kitiškai vertink informaciją. Ne viskas, kas parašyta internete, yra tiesa. Tikrink šaltinius ir neplatink nepatikrintos informacijos.
5. Būk atsargus su nuorodomis ir laiškais. Jei žinutė ar pasiūlymas atrodo per geras, kad būtų tiesa, dažnai tai gali būti sukčiavimas.



Aukštinės taisyklės gyvenant skaitmeniniame pasaulyje

6. Gerbk kitų žmonių teises. Internetu galioja tie patys įstatymai kaip ir realiame gyvenime – už šmeižtą, patyčias ar autorių teisių pažeidimus gali kilti teisinė atsakomybė.
7. Žinok savo teises. Tu turi teisę į privatumo apsaugą, teisę kontroliuoti savo asmens duomenis ir tam tikrais atvejais reikalauti pašalinti informaciją apie save.
8. Jei susidūrei su problema – nelik vienas. Apgaulės, priekabiavimo ar kitų pažeidimų atveju kreipkis į suaugusiuosius, institucijas ar platformų pagalbos centrus.
9. Kurk teigiamą skaitmeninę reputaciją. Internetas gali būti vieta mokytis, kurti ir dalintis vertinga informacija. Naudok jį atsakingai.
10. Atmink – technologijos yra įrankis. Svarbiausia yra žmogaus atsakomybė, kritinis mąstymas ir pagarba kitų teisėms.



Ruošiantis olimpiadai yra aktualūs šie šaltiniai:

1. Europos Parlamentas ir Taryba. Bendrasis duomenų apsaugos reglamentas (BDAR / GDPR), Reglamentas (ES) 2016/679. Prieiga per EUR-Lex: <https://eur-lex.europa.eu>
2. Europos Parlamentas ir Taryba. Skaitmeninių paslaugų aktas (Digital Services Act), Reglamentas (ES) 2022/2065. Prieiga per EUR-Lex: <https://eur-lex.europa.eu>
3. Europos Parlamentas ir Taryba. Dirbtinio intelekto aktas (Artificial Intelligence Act). Informacija: <https://digital-strategy.ec.europa.eu>
4. Europos Komisija. Digital Strategy – politika dėl skaitmeninių technologijų, dirbtinio intelekto ir interneto platformų. <https://digital-strategy.ec.europa.eu>
5. ENISA – European Union Agency for Cybersecurity. Kibernetinio saugumo tyrimai ir rekomendacijos. <https://www.enisa.europa.eu>



Mykolas Romeris
universitetas



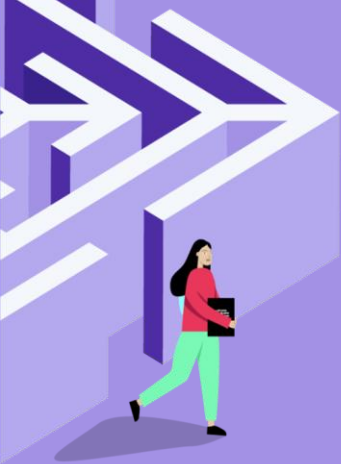
Ruošiantis olimpiadai yra aktualūs šie šaltiniai:

6. Europol. Internet Organised Crime Threat Assessment (IOCTA) – ataskaitos apie kibernetinius nusikaltimus ir internetines grėsmes. <https://www.europol.europa.eu>
7. Valstybinė duomenų apsaugos inspekcija (VDAI). Informacija apie asmens duomenų apsaugą Lietuvoje. <https://vdai.lrv.lt>
8. Nacionalinis kibernetinio saugumo centras (NKSC). Patarimai apie saugų naudojimąsi internetu ir kibernetinę saugą. <https://www.nksc.lt>
9. Ryšių reguliavimo tarnyba (RRT). Informacija apie elektroninių ryšių paslaugas ir vartotojų teises. <https://www.rrt.lt>
10. Draugiškas internetas (Safer Internet Centre Lithuania). Edukacinė informacija apie saugų internetą vaikams ir jaunimui. <https://www.draugiskasinternetas.lt>



Mykolas Romeris
universitetas





NACIONALINĖ TEISĖS ŽINIŲ OLIMPIADA

