

Technologinio sprendimo, ribojančio prieigą prie nelegalaus turinio internete, galimybių studija

Galutinė ataskaita

Skirta: LR kultūros ministerija

Vilnius, 2025

Turinys

| | |
|--|----|
| Trumpinių sąrašas | 3 |
| Sąvokų sąrašas..... | 4 |
| Lentelių sąrašas | 5 |
| Paveikslų sąrašas | 6 |
| Įvadas | 7 |
| 1. Nelegalaus turinio sklaidos ir vartojimo modeliai..... | 8 |
| 2. Galimų alternatyvų sudarymas..... | 24 |
| 2.1. Analizės tikslų ir metodikos apibrėžimas | 24 |
| 2.2. Technologinių sprendimų pritaikymas užsienio šalyse | 26 |
| 2.2.1. Veikiančių technologinių sprendimų pavyzdžiai | 26 |
| 2.2.2. DI integracijos galimybių analizė | 36 |
| 2.3. Ekspertinių nuomonių analizė | 39 |
| 2.4. Technologinių sprendimų lyginamoji analizė..... | 44 |
| 2.4.1. Galimos koncepcijos | 45 |
| 2.4.2. Koncepcijų išpildymo funkcinės dalys..... | 46 |
| 2.4.3. Funkcinių dalių išpildymo technologijos | 46 |
| 2.4.4. Alternatyvų formavimas | 52 |
| 2.5. Optimalaus technologinio sprendimo Lietuvos atvejui pasirinkimas..... | 56 |
| 3. Atrinktos alternatyvos konkretizavimas..... | 60 |
| 3.1. Asmens duomenų rinkimas ir apsauga | 60 |
| 3.2. Technologinio sprendimo aprašymas ir plėtros galimybės..... | 63 |
| 3.2.1. Technologinio sprendimo aprašymas | 63 |
| 3.2.2. Technologinio sprendimo plėtros ir atnaujinimo galimybės..... | 67 |
| 3.2.1. Technologinio sprendimo sukūrimo ir palaikymo proceso aprašymas | 67 |
| 3.2.2. Technologinio sprendimo sąnaudų–naudos analizė..... | 69 |
| 3.3. Technologinio sprendinio administravimo modelis..... | 73 |
| 4. Lietuvos IT sprendimų kūrėjų rinkos analizė..... | 76 |
| Priedai | 81 |
| 1 priedas. Kuriamo technologinio sprendimo techninė specifikacija..... | 81 |

Trumpinių sąrašas

| | |
|------------------------|---|
| ATPT | Audiovizualinio turinio paslaugų teikėjai |
| ATTA | Autorinių teisių turėtojus atstovaujančios organizacijos |
| BDAR | Bendrasis duomenų apsaugos reglamentas (angl. general data protection regulation) |
| DI | Dirbtinis intelektas |
| AlaaS | Dirbtinis intelektas kaip paslaugos |
| DVS | Domenų vardų sistema |
| ES | Europos Sąjunga |
| EUIPO | Europos Sąjungos intelektinės nuosavybės tarnyba |
| HTTP | Hipertekstinis perdavimo protokolas |
| IP | Interneto protokolas |
| IPT | Interneto paslaugų teikėjo |
| IRT | informacinės ir ryšių technologijos |
| JK | Jungtinės Karalystės |
| KTS | Kuriamas technologinis sprendimas |
| Kultūros ministerija | Lietuvos Respublikos kultūros ministerija |
| LDIP | Labai didelės interneto platformos |
| LDIPS | Labai didelės interneto paieškos sistemos |
| LRTK | Lietuvos radijo ir televizijos komisija |
| MVĮ | mažosios ir vidutinės įmonės |
| Piratavimas | Nelegalaus turinio vartojimas arba sklaida |
| PVP | Perdavimo valdymo protokolas |
| RRT | LR ryšių reguliavimo tarnyba |
| SPA | Skaitmeninių paslaugų aktas |
| Techninė specifikacija | Technologinio sprendimo, ribojančio prieigą prie nelegalaus turinio internete, galimybių studijos ir jos priedo - techninės specifikacijos parengimo techninė specifikacija |
| VIL | Vienodų išteklių lokatorius |

Sąvokų sąrašas

| | |
|---|---|
| „Peer-to-peer“ | Tai decentralizuota sistema, kada naudotojai dalinasi duomenis iš savo kompiuterių lygia rangių ryšių pagalba. |
| Konsultantas | Smart Continent LT, UAB |
| Kuriamas technologinis sprendimas, KTS, TS, Įrankis | Technologinis sprendimas, kuris yra kuriamas siekiant padėti naudotojams atskirti legalų ir nelegalų turinį internete ir gebėtų pasiūlyti legalų turinio šaltinį. |
| Patikimi regionai | Patikimi regionai tyrime reiškia konkrečias DI modelio įvesties erdvės sritis, kuriose modelio prognozės laikomos patikimomis ir efektyviomis. |
| Patikimi pranešėjai (angl. – trusted flaggers) | Patikimi žymėtojai yra specialūs skaitmeninių paslaugų akto – SPA subjektai. Jie yra ekspertai, gebantys aptikti tam tikros rūšies neteisėtą turinį internete, pavyzdžiui, neapykantos kalbą ar teroristinį turinį, ir apie tai pranešti interneto platformoms. Jų pateiktiems pranešimams turi būti teikiama pirmenybė, nes tikimasi, kad jie bus tikslesni nei vidutinio naudotojo pateikti pranešimai. |
| Tikslinė grupė | Kultūros ministerijos tyrimo 2024 m. respondentų agreguota grupė, kuri sunkiai atskiria nelegalų turinį nuo legalaus ir tuo pačiu naudoja nelegalų turinį. |
| Torentai | Naudotojai savo kompiuteryje talpina dokumentus su metaduomenimis, kurie yra vadinami torentais. Šie duomenys veikia kaip žemėlapis, jungiantis failus iš kelių šaltinių, turinčių tą patį failą. |
| Užsakovas | LR kultūros ministerija |
| Veidrodinės svetainės | Tai svetainės, kurios yra sukuriamos pagal neteisėtų svetainių IP adresus, kai originalios svetainės yra uždraudžiamos nelegalų turinį reguliuojančių institucijų. |

Lentelių sąrašas

| | |
|---|----|
| 1 lentelė. Legalaus ir nelegalaus turinio vartojimas pagal turinį visoje respondentų imtyje, tikslinėje grupėje ir specialioje imtyje..... | 20 |
| 2 lentelė. Nelegalaus turinio vartojimo pasirinkimo priežastys visoje respondentų imtyje, tikslinėje grupėje ir specialioje imtyje..... | 22 |
| 3 lentelė. Funkcijų pavadinimai, veikimo principas, bei skiriamas ženklas tekste..... | 26 |
| 4 lentelė. Rinkos konsultacijų metu pateikti pasiūlymai | 44 |
| 5 lentelė. Technologinio sprendimo alternatyvų vertinimas ir palyginimas | 58 |
| 6 lentelė. Atviro ir uždaro administravimo modelio apibendrinimas..... | 74 |
| 7 lentelė. Pridėtinė vertė gamybos sąnaudoms pagal ekonominės veiklos rūšis (konkrečiai lyginant informacijos ir ryšių veiklos rūšį ir bendrą ekonominės veiklos rūšių sumą) tūkst. Eur | 78 |
| 8 lentelė. Galimybių studijos priedas – Kuriamo Technologinio sprendimo techninė specifikacija | 81 |

Paveikslų sąrašas

| | |
|--|----|
| 1 paveikslas. Nelegalaus turinio paieškos būdai Lietuvoje, 2024 m..... | 14 |
| 2 paveikslas. Populiariausi nelegalaus turinio prieigos būdai Lietuvoje, 2024 m..... | 15 |
| 3 paveikslas. Gebėjimas atskirti legalią ir nelegalią prieigą prie internetinio turinio. Klausimas: Kiek Jums asmeniškai lengva ar sunku atskirti, ar internetinė prieiga prie Jūsų naudojamo turinio (filmų, muzikos, el. knygų ir t. t.) yra legali ar piratinė? (Visi respondentai, N žr. diagramoje), 2024 m. | 16 |
| 4 paveikslas. Respondentai pagal lytį, kurie sunkiai atskiria nelegalų turinį nuo legalaus ir tuo pačiu atsakę į klausimą, jog naudojasi nelegaliu turiniu, 2024 m..... | 18 |
| 5 paveikslas. Respondentų dalis, kurie sunkiai atskiria nelegalų / legalų turinį ir vartoja nelegalų turinį pagal amžių, 2024 m. | 18 |
| 6 paveikslas. Naudojimosi internetu įgūdžiai tikslinėje respondentų grupėje, 2024 m. | 19 |
| 7 paveikslas. Studijos I etapo metodiką vizualizuojanti schema | 25 |
| 8 paveikslas. Skaitmeninių paslaugų akto taikymo gairės, 2024 m..... | 27 |
| 9 paveikslas. Skaitmeninių paslaugų akto taikymo gairės, 2024 m..... | 27 |
| 10 paveikslas. „Lumière“ programos veikimo principas | 28 |
| 11 paveikslas. EOL įskiepis, įdiegtas Mozilla Firefox naršyklėje | 31 |
| 12 paveikslas. JustWatch paieškos rezultatas..... | 32 |
| 13 paveikslas. Naudoklegaliai.lt paieškos rezultatas..... | 33 |
| 14 paveikslas. Teramind sistemos veikimo schema..... | 35 |
| 15 paveikslas. Ekspertinių nuomonių pagrindu sudaryta problemų, priežasčių ir galimų sprendimų schema | 40 |
| 16 paveikslas. Principinė Technologinio sprendimo schema | 63 |
| 17 paveikslas. Įskiepio skirtingų scenarijų koncepcinės vizualizacijos. Pirmas paveikslas – atvejis, kai įskiepis negali pateikti vertinimo, antras paveikslas – įskiepis nustatė, kad puslapis įtrauktas į nelegalių svetainių sąrašą, trečias paveikslas – įskiepis nustatė, kad puslapis įtrauktas į legalių svetainių sąrašą | 66 |
| 18 paveikslas. Pažangiųjų ir vidutiniškai pažangiųjų technologijų gamybos sektoriaus įmonių skaičius | 76 |
| 19 paveikslas. Pažangiųjų ir vidutiniškai pažangiųjų technologijų gamybos sektoriaus pridėtinė vertė | 77 |

Įvadas

Smart Continent LT, UAB, pagal 2024 m. gruodžio 10 d. pasirašytą sutartį Nr. VP-289 su LR kultūros ministerija, rengia Technologinio sprendimo, ribojančio prieigą prie nelegalaus turinio internete, galimybių studiją ir jos priedą (toliau – Studija). Vadovaujantis sutarties priedo – techninės specifikacijos (toliau – Techninė specifikacija arba TS) – nustatytais reikalavimais parengta ši Galutinė ataskaita.

STUDIJS RENGIMO PRIELAIDOS: Europos Sąjungos intelektinės nuosavybės tarnybos (ESINT arba angl. EUIPO) 2021 metų tyrimo duomenimis, pagal nelegalaus, autorių teisių turėtojų teises pažeidžiančio turinio vartojimą Lietuva užima 3 vietą tarp visų Europos Sąjungos (ES) šalių. Vidutiniškai interneto naudotojas Lietuvoje prie nelegalaus turinio prisijungia apie 12 kartų per mėnesį, kai tuo tarpu ES vidurkis siekia tik 5,9 karto. 2019 m. tyrimo duomenimis vidutinis Lietuvos interneto naudotojas jungėsi prie piratinių svetainių beveik 26 kartus per mėnesį, kai ES vidurkis siekė 9,7 prisijungimų per mėnesį vienam vidutiniam naudotojui. Remiantis ESINT tyrimais, galima stebėti, kad jau kelerius metus iš eilės Lietuva išlieka viena labiausiai pirataujančių šalių ES. Naujausiame ESINT 2023 m. tyrime Lietuva vėlgi, kartu su Latvija, Estija ir Kipru, yra priskiriama prie aukščiausiu turinio piratavimo lygiu pasižyminčių ES narių.

Atsižvelgiant esamą situaciją, galima daryti išvadą, kad nemaža dalis audiovizualinio turinio naudotojų tiesiog nežino, kad vartoja nelegalų turinį. Lietuvos gyventojų nelegalaus turinio vartojimo lygio nustatymo tyrimas inicijuotas Kultūros ministerijos 2023 m. net 20-25 proc. turinio naudotojų nurodė negebantys atskirti legalaus turinio prieigą nuo nelegalios. Todėl Atitinkamai, šiuo metu yra iškilęs inovacinio-technologinio sprendimo poreikis, kuris suteiktų sąžiningam audiovizualinio turinio naudotojui galimybę patikrinti savo vartojamo turinio legalumą, nukreiptų jį į legalaus turinio šaltinius bei suteiktų valstybės institucijoms galimybę vykdyti nelegalaus turinio sklaidos monitoringą. Atlikus tokio technologinio sprendimo sukūrimo rinkos konsultaciją, paaiškėjo kad šiuolaikinės inovatyvios technologijos siūlo pakankamai įvairius būdus minėtiems tikslams pasiekti, todėl nuspręsta įsigyti galimybių studijos parengimo paslaugas.

Remiantis Kultūros ministerijos nuostatais, Kultūros ministerijos veiklos tikslai, be kita ko, yra – formuoti valstybės politiką autorių teisių, atlikėjų ir kitų gretutinių teisių, visuomenės informavimo (audiovizualinė politika yra visuomenės informavimo politikos sudėtinė dalis) srityse, organizuoti, koordinuoti ir kontroliuoti jos įgyvendinimą. Atsižvelgiant į tai, bus siekiama pozityviai formuoti legalaus turinio vartojimo įpročius padedant naudotojams ne tik identifikuoti piratinį turinį, bet ir surasti analogiško turinio legalius šaltinius.

STUDIJS TIKSLAS:

1. vadovaujantis piratavimo audiovizualinių paslaugų rinkoje ir naudotojų poreikių analize, išanalizavus užsienio valstybių gerąją praktiką bei rinkoje jau egzistuojančius technologinius sprendimus ir jų pritaikymo būdus, pagal savo pasirinktus kriterijus išskirti efektyviausią Technologinį sprendimą;
2. pateikti perkančiosios organizacijos pasirinktos Technologinio sprendimo alternatyvos struktūros aprašymą, kaštų ir naudos analizę, įgyvendinimo būdus, detalizuojant kiekvieną iš jų pagal šioje techninėje specifikacijoje nustatytus parametrus (t. y. parengti Technologinio sprendimo techninę specifikaciją).

STUDIJS STRUKTŪRA:

- Įvadas;
- Nelegalaus turinio sklaidos ir vartojimo modelių analizė;
- Galimų alternatyvų sudarymas;
- Atrinktos alternatyvos konkretizavimas;
- Lietuvos IT sprendimų kūrėjų rinkos analizė;
- Priedai.

1. Nelegalaus turinio sklaidos ir vartojimo modeliai

Šiame skyriuje yra pristatomi pagrindiniai nelegalaus turinio sklaidos ir vartojimo modeliai. Pirmiausiai yra apibendrintai aprašomi skirtingi nelegalaus turinio sklaidos ir nelegalaus turinio būdai, jie priskiriami sustambintoms kategorijoms. Toliau apžvelgiama pasaulinė situacija bei situacija Lietuvoje. Galiausiai yra suformuluojami profiliai Lietuvos gyventojų, kurie sudarytų Technologinio sprendimo, ribojančio prieigą prie nelegalaus turinio internete (toliau – Kuriamas technologinis sprendimas, KTS arba Įrankis), tikslinę auditoriją.

PASAULYJE PAPLITĘ NELEGALAUS TURINIO VARTOJIMO BŪDAI

Piratavimas internete – tai autorių teisių saugomos medžiagos ir intelektualės nuosavybės pažeidimas, turinio atsiuntimas ir jo naudojimas už jį nemokant, todėl laikomas neteisėtu veiksmu. Piratavimas yra autorių teisių įstatymų pažeidimas, už kuriuos gresia administracinė arba baudžiamoji atsakomybė. Piratavimas lemia tai, jog autorių teisių turėtojai kasmet susiduria su finansiniais nuostoliais.¹ Taip pat, piratavimas yra viena iš sudėtingiausių problemų, su kuriomis XXI a. susiduria kūrybinė industrija: piratavimas stabdo naujo turinio kūrimą, nes kelia riziką nesugrąžinti investicijų skirtų kūrybinio proceso metu.² Toliau pateikiami pagrindiniai, labiausiai paplitę piratavimo būdai įvairiam turiniui pasiekti už jį nesumokant.

Bet koku būdu nelegalaus turinio transliavimas arba platinimas yra nelegalus be autorių teisių turėtojų ir jų atstovų leidimo arba be licencijos. Tai taikoma tiek internetinėms transliacijos platformoms, tiek tradiciniams transliavimo būdams ir apima tokį turinį kaip filmai, sporto renginiai, televizijos laidos ir kitą turinį.

A. NELEGALIAI TRANSLIUOJAMAS TURINYS INTERNETINĖJE SVETAINĖJE. Nelegaliose transliacijos svetainėse, kurios neturi autorių teisių turėtojų arba jų atstovų leidimo transliuoti turinį, nėra oficialiai autorizuotos tam įgaliotų Lietuvos institucijų (t. y. nėra deklaravę savo veiklos pradžios), siūloma filmų, televizijos laidų ir tiesioginių renginių įrašų biblioteka. Tokiose svetainėse taip pat kartais yra talpinama muzika arba kiti garso įrašai. Šių svetainių turinys dažnai talpinamas serveriuose, esančiuose šalyse, kuriose autorių teises reglamentuojantys įstatymai nėra griežti arba kur valstybės institucijos negeba užkirsti kelią įstatymų pažeidimui, todėl jų vykdymą užtikrinti sudėtinga. Vartotojai šias internetines svetaines gali pasiekti per interneto naršykles, per paieškos įrankius (pavyzdžiui, *Google*). Tokiose svetainėse turinys prieinamas nemokami, tokių svetainių kūrėjai pajamas uždirba iš nelegalaus turinio tinklalapiuose talpinamos reklamos. Pažymėtina, kad ir legalų turinį talpinančiose svetainėse (pavyzdžiui, YouTube, Facebook ir t. t.) taip pat galima patalpinti nelegalų turinį, tačiau dažniausiai šios svetainės sėkmingai kovoja su tokio turinio atsiradimu jų svetainėse.³

Kultūros ministerijos 2024 m. tyrimo⁴ respondentų rezultatai renkantis šį nelegalaus turinio vartojimo ir sklaidos būdą:

- atsakymo variantas „Žiūrėjau ar klausiau turinį piratinėje svetainėje“ – 44 proc.;
- atsakymo variantas „Naudojau piratiniais grojaraščiais“ – 9 proc.

Iš viso šį būdą pasirinko 55 proc. respondentų, o nelegaliai transliuojamo turinio internetinėje svetainėje peržiūra yra populiariausias nelegalaus turinio vartojimo būdas Lietuvoje.⁵

B. NELEGALIAI PLATINAMO TURINIO PARSISIUNTIMAS Į SAVO ĮRENGINĮ IŠ INTERNETINĖS SVETAINĖS. Tiesioginis atsiuntimas – tai failų atsiuntimas iš serverio arba svetainės, kurioje talpinamas nelegalus turinys. Skirtingai nuo „*Torrent*“ programų, tiesioginiai atsiuntimai gaunami iš vieno šaltinio, todėl juos lengviau susekti ir uždrausti, nors praktikoje to užtikrinti visiškai irgi nepavyksta. Šie šaltiniai gali būti įvairūs – tinklaraščiai, forumai, susirašinėjimo platformos (pavyzdžiui, *Telegram*), kuriuose dalijamasi nuorodomis į nelegalų turinį. Tiesioginis turinio

¹ Cybersecurity and the Modern World, „The Consequences of Digital Piracy“, Patrick Putnam, 2019. Prieiga internete: <https://www.uscybersecurity.net/digital-piracy/>

² CreativeContent, „What’s so bad about Piracy?“. Prieiga internete: <https://creativecontentaustralia.org.au/whats-so-bad-about-piracy/>

³ Ten pat

⁴ Ten pat

⁵ Ten pat

parsisiuntimas iš svetainės yra paprastas – jis trunka sąlyginai greitai, reikalauja mažai techninių žinių. Šis būdas – tiesioginis turinio parsisiuntimas iš internetinės svetainės yra susijęs su rizika, pavyzdžiui, kenkėjiška programine įranga ir teisinėmis pasekmėmis dėl autorių teisėmis saugomos medžiagos parsisiuntimo.⁶

Kultūros ministerijos 2024 m. tyrimo⁷ respondentų rezultatai renkant šį nelegalaus turinio vartojimo ir sklaidos būdą:

- atsakymo variantas „Parsisiunčiau piratinį turinį tiesiai iš interneto svetainės“ – 23 proc.;
- atsakymo variantas „Gavau piratinį turinį per *Telegram*, *Messenger* ar kitas momentinių pranešimų programas“ – 9 proc.;
- atsakymo variantas „Parsisiunčiau piratinį turinį iš *Facebook* grupių, kuriose dalijamasi tokiu“ – 7 proc.

Iš viso šį būdą pasirinko 39 proc. Kultūros ministerijos 2024 m. tyrimo⁸ respondentų, o nelegalios medžiagos tiesioginis parsisiuntimas į savo įrenginius yra 3-ioje vietoje pagal populiarumą Lietuvoje.⁹

C. TECHNOLOGINĖS MANIPULIACIJOS / SAUGOS SISTEMŲ APĖJIMAS (VPN, DNS, PROXY). Skirtingų technologijų naudojimas nesankcionuoti prieigai gali būti siejamas ir su neteisėtais internetinio turinio vartojimo veiksmais. VPN dažniausiai naudojami konfidencialumui internete užtikrinti, tačiau jų naudojimas geografiniams apribojimams apeiti ir prieigai prie autorių teisių saugomos medžiagos be tinkamos licencijos gauti gali būti siejamas su neteisėtomis praktikomis. Šis būdas yra technologiškai pažangesnis ir reikalauja daugiau kompiuterinių žinių, nei anksčiau minėti. Tas pat pasakytina ir apie bandymą neteisėtai gauti prieigą ir parsisiųsti įvairias mokamas programas darbui su kompiuteriui (antivirusinės, maketavimo / programavimo programos). Priklausomai nuo taikomų autorių teisių įstatymų programinė įranga gali būti neteisėta ir už ją gali būti taikomos griežtos administracinės ar baudžiamosios sankcijos.¹⁰

Rezultatai, pagal prieš tai minėtą Kultūros ministerijos atliktą tyrimą 2024 m.:

- atsakymo variantas „Pakeičiau DNS nustatymus arba naudoju DNS teikėjus arba kitas atblokovimo priemones“ – 11 proc.;
- atsakymo variantas „Prieidamas (-a) prie nelegalaus turinio naudojami VPN paslauga“ – 11 proc.;
- atsakymo variantas „Gavau piratinę / „nulaužtą“ kompiuterinę programą(-as) iš pasamdytų ar pažįstamų kompiuterių specialistų“ – 10 proc.

D. LYGIARANGIŲ RYŠIŲ PAGALBA (ANGL. PEER-TO-PEER). Praktikoje šis piratavimo būdas yra įgyvendinamas torentų technologijos pagalba. Naudotojai savo kompiuteryje talpina dokumentus su metaduomenimis (vadinamus torentais), kurie veikia kaip žemėlapis, jungiantis šaltinius, turinčius tą patį failą. Šį **decentralizuotą** metodą sunku susekti ir uždrausti, nes nėra vieno konkretaus failų šaltinio. Kiekvienas naudotojas, atsisiunčiantis arba įkeliantis rinkmenos dalis, prisideda prie tinklo plėtros, todėl rinkmenos perduodamos be poreikio turėti centralizuotą serverį. Lygiarangių ryšys dažniausiai naudojamas dalijantis sąlyginai didelės apimties failais, pavyzdžiui, filmais, žaidimais ir programine įranga. Praktikoje naudojama tokia programinė įranga kaip „BitTorrent“¹¹ prisijungimui prie lygiarangių ryšio, o torentų dokumentus su metaduomenimis galima rasti specializuotuose agregatoriuose, kurie yra prieinami per paieškos internete įrankius (pavyzdžiui, *Google*). Šis būdas naudotojui yra rizikingas, nes į platinamą turinį neretai integruojamos kenkėjiškos programos.¹²

⁶ Ten pat

⁷ Ten pat

⁸ Lietuvos Respublikos kultūros ministerija, Lietuvos gyventojų nelegalaus turinio vartojimo lygio nustatymo tyrimas, 2024m. Prieiga internetu: https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.kulturostyrimai.lt%2Fwp-content%2Fuploads%2F2024%2F10%2FLietuvos-gyventoju-nelegalaus-turinio-vartojimo-lygio-nustatymo-tyrimas_Santrauka_2024.pdf&psig=AOvVaw3MghNTtLV2OUBBamkt3No2&ust=1740728977480000&source=images&cd=vfe&opi=89978449&ved=0CAQQn5wMahcKEwiYsbP0ruOLaxUAAAAAHQAAAAQBA

⁹ Ten pat

¹⁰ Norton, Software piracy: Types, risks, and how to stay safe, 2023. Prieiga internete: <https://us.norton.com/blog/emerging-threats/software-piracy>

¹¹ BitTorrent. Prieiga internetu: <https://www.bittorrent.com/>

¹² Bytescare blogs, „How does piracy work?“, 2024. Prieiga internetu: <https://bytescare.com/blog/how-does-piracy-work>

Šiam būdui yra aktualūs Kultūros ministerijos 2024 m. tyrimo, kuris buvo atliktas siekiant nustatyti Lietuvos gyventojų nelegalaus turinio vartojimo lygį, rezultatai¹³. **Atsakymai, referuojantys į lygiarangių ryšio pagalbą renkantiems vartoti arba platinti nelegalų turinį, yra pateikti toliau:**

- atsakymo variantas „Parsisiunčiau piratinį turinį per torentus“ – 24 proc.;
- atsakymo variantas „Parsisiunčiau piratinį turinį per P2P tinklus“ – 3 proc.

Iš viso 27 proc. apklausos respondentų, kurie reprezentuoja reikšmingą Lietuvos gyventojų dalį, dalyvavusių prieš tai minėtoje Kultūros ministerijos 2024 m. tyrimo apklausoje, pasirinko lygiarangių ryšio pagalbą vartojant bei skleidžiant nelegalų turinį. Tai yra antras pagal populiarumą nelegalaus turinio vartojimo būdas Lietuvoje.¹⁴

E. PRIEIGOS GAVIMAS IŠ DRAUGO / ARTIMO ŽMOGAUS, KURIS TURI LEGALIĄ PRIEIGOS TEISĘ. Keli naudotojai, besinaudojantys ta pačia internetinio turinio platformos paskyra arba prieiga, irgi sudaro prielaidą nelegaliam turinio naudojimui kaip kad muzika, vaizdo įrašai, programinė įranga, internetiniai įrankiai. Pavyzdžiui, „Spotify Premium“ naudotojai gali klausytis muzikos ir ją atsisiųsti, savo paskyra prisijungę prie ne daugiau kaip trijų įrenginių – taip siekiama išvengti atvejų, kai naudotojai dalinasi savo prisijungimo duomenimis su kitais asmenimis. Remiantis „Hub“ 2019 m. apklausos „Video Redefined 2019“ duomenimis, 47 proc. respondentų arba dalijosi savo paskyros informacija arba naudojos kieno nors kito slaptažodžiu apsaugoto turinio žiūrėjimui. 18–25 metų amžiaus žmonių kategorijoje šis skaičius išauga iki 81 proc. Šis turinio prieigos platinimo mažose grupėse būdas kiekvienais metais atneša nuostolius turinio kūrėjams. Bendrovė „Parks Associates“ prognozuoja, kad paskyros dalijimasis 2024 m. vaizdo transliacijų ir mokamos televizijos bendrovėms kainuos 12,5 mlrd. dolerių, palyginti su 2019 m. prarastais 9,1 mlrd.¹⁵

Rezultatai, pagal prieš tai minėtą Kultūros ministerijos atliktą tyrimą 2024 m.:

- atsakymo variantas „Naudojasi iš kitų gautais mokamų prieigų slaptažodžiais ar programinės įrangos licencijomis“ – 15 proc.

Iš bendro skaičiaus šiame tyrime dalyvavusių respondentų 15 proc. dalis pasirinko šį nelegalaus piratavimo būdą Lietuvoje.

F. MOKESTIS UŽ NELEGALŲ TURINĮ. Anketoje, kaip papildomas atsakymas, buvo teigiama, jog respondentas susimokėjo už prieigą prie nelegalaus turinio.

- Atsakymo variantas „Mokėjau už prieigą prie piratinių šaltinių“ – 6 proc.

Priskirti šį būdą prie įprastų piratavimo būdų yra sudėtinga, nes, vertinant pagal atsakymą galima spėti, jog žmogus neturėjo intencijos naudotis nelegaliu turiniu ir negebėjo atskirti legalaus turinio nuo nelegalaus, todėl susimokėjo už prieigą prie nelegalaus. Tai gali būti tokios nelegalaus, tačiau mokamo turinio svetainės, kaip *Filmait.in*, kurią respondentai prieš tai minėtame tyrime paminėjo prie nelegalaus turinio internetinių tinklapių kaip labiausiai žinomą ir populiariausią Lietuvoje. Galima kelti hipotezę, jog šį atsakymą pasirinkusioji respondentų dalis tikriausiai nežinojo, jog naudojasi nelegaliu turiniu dėl prastų internetu naudojimosi įgūdžiai.

Kita galima priežastis mokėti už nelegalų turinį – šių svetainių siūloma kaina už nelegalų turinį buvo mažesnė nei kitose legaliose svetainėse esanti kainų pasiūla. Taip pat šį variantą galėjo pasirinkti žmonės, kurie sutiko mokėti už piratinį turinį, todėl, nes nerado legalaus šaltinio (legalios pasiūlos trūkumas).

G. NELEGALUS LEGALIAUS TURINIO KOPIJŲ ATLIKIMAS. Šis būdas yra panašus į būdą D tuo, jog siekiama dalintis informacija su kitais asmenimis arba išsisaugoti informaciją savo reikmėms vėlesniam laikotarpiui (kai turinio platformos prenumerata bus atšaukta ir / ar prieiga prie turinio apribota). Šis būdas gali apimti atvejus, kai asmuo,

¹³Lietuvos Respublikos kultūros ministerija, Lietuvos gyventojų nelegalaus turinio vartojimo lygio nustatymo tyrimas, 2024m. Prieiga internetu: https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.kulturostyrimai.lt%2Fwp-content%2Fuploads%2F2024%2F10%2FLietuvos-gyventoju-nelegalaus-turinio-vartojimo-lygio-nustatymo-tyrimas_Santrauka_2024.pdf&psig=AOvVaw3MghNTtLV2OUBBamkt3No2&ust=1740728977480000&source=images&cd=vfe&opi=89978449&ved=0CAQQn5wMahcKEwiYsbP0ruOLaxUAAAAAHQAAAAQBA

¹⁴Ten pat

¹⁵Red points, When account sharing becomes a piracy issue, 2024. Prieiga internetu: <https://www.redpoints.com/blog/account-sharing/>

turintis legalią prieigą prie turinio, planuoja atšaukti šią prieigą ir atlieka turinio kopijų vėlesniam naudojimui ir vėliau naudojasi nelegaliai atliktomis turinio kopijomis. Šiam būdai taip pat priklauso tiesioginis turinio transliavimas iš legalios prieigos ir dalinimasis su neturinčiais legalios prieigos asmenimis. Transliavimas be autorių teisių turėtojų arba jų atstovų leidimo ir transliavimas tiesiogiai be reikiamų licencijų ar leidimų prieštarauja įstatymams.¹⁶

Rezultatai, pagal prieš tai minėtą Kultūros ministerijos atliktą tyrimą 2024 m.:

- atsakymo variantas „Dariau muzikos ar filmų srautinės transliacijos įrašą“ – 3 proc.

Iš bendro skaičiaus šiame tyrime dalyvavusių respondentų 3 proc. dalis pasirinko šį nelegalaus piratavimo būdą Lietuvoje. Pažymėtina, kad nors šis būdas yra santykinai retais naudojamas – tai yra būdas, kurio pagalba nelegaliai turinį transliuojančių svetainių administratoriai gauna prieigą prie turinio.

Toliau skyriuje yra vertinamos pasaulinės tendencijos.

PASAULINĖS TENDENCIJOS

Autorius Benjamin Gorman straipsnyje „*Software piracy: Types, risks, and how to stay safe*“¹⁷ teigia, jog 2024 m. piratavimas tebėra pasaulinė problema, ypač augant skaitmeninio turinio vartojimui. Taip pat, *Coollest Gadgets* straipsnyje „*Piracy Statistics By Demographics, Frequency, Reasons, Types, Software and Regions*“ pateikiama bendra pasaulinio lygio nelegalaus turinio vartojimo tendencijų statistika¹⁸, kuri rodo, jog 2023 m. programinės įrangos piratavimo lygis siekia – 35 proc., o filmų ir televizijos laidų piratavimo lygis siekia – 31 proc. Reikšmingą įtaką piratavimas daro muzikos pramonei, nes daugiau kaip 30 proc. pasaulio muzikos srautinių transliacijų vyksta iš nelicencijuotų platformų.¹⁹ Dirbtinio intelekto (toliau – DI) pritaikymas piratavimo praktikų užkardymui, labiau ribojančios turinio platformų prieigos platinimo galimybės bei valstybių griežtinami įstatymai prisideda prie piratavimo mažinimo, tačiau jis vis dar plačiai paplitęs šalyse, kuriose atsakingų valstybės institucijų pajėgumai yra riboti. Jose, pavyzdžiui, neteisėtas tiesioginis turinio transliavimas vis dar gajus.²⁰

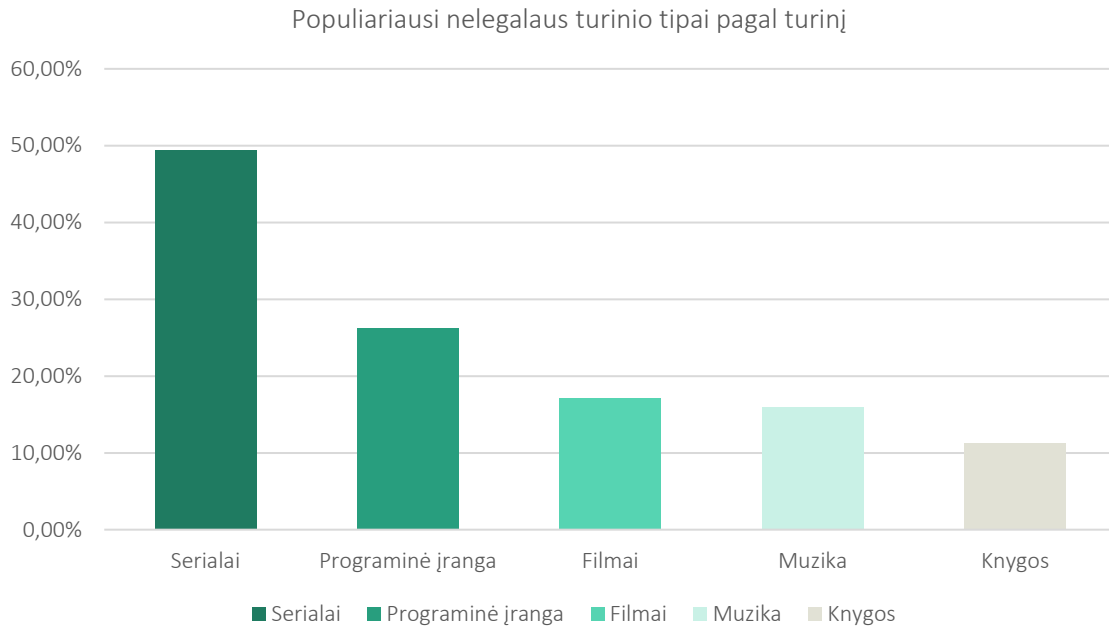
¹⁶ Copyrighted, It is illegal to watch copyrighted material?, 2024. Prieiga internetu: <https://www.copyrighted.com/blog/is-it-illegal-to-watch-copyrighted-material#is-it-illegal-to-watch-copyrighted-material>

¹⁷ Norton, Benjamin Gorman, „Software piracy: Types, risks, and how to stay safe“, 2023 m. Prieiga internete: <https://us.norton.com/blog/emerging-threats/software-piracy>

¹⁸ Saisuman Revankar, Coolest gadgets, „Piracy Statistics By Demographics, Frequency, Reasons, Types, Software and Regions“, 2024. Prieiga internete: <https://www.coolest-gadgets.com/piracy-statistics/?utm>

¹⁹ Ten pat

²⁰ Ten pat



3 paveikslas. Populiariausi NTV produktai internete pasauliniu mastu

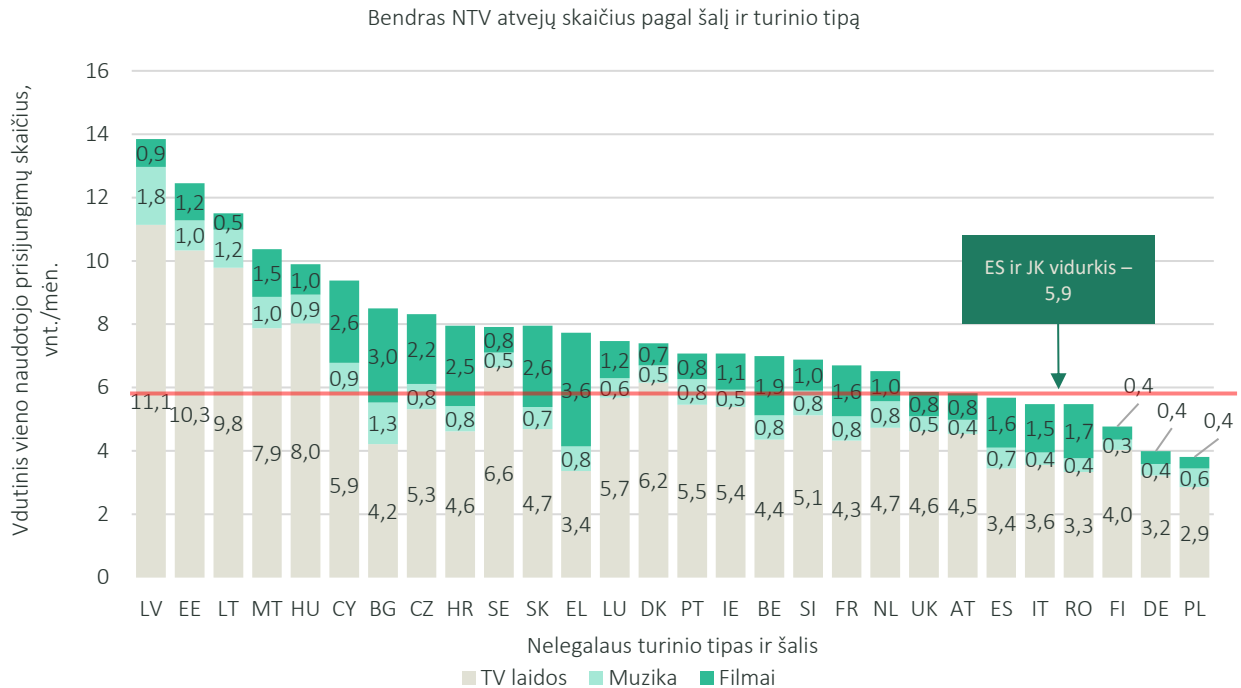
Šaltinis: Coolest gadgets „Piracy Statistics By Demographics, Frequency, Reasons, Types, Software and Regions“. Prieiga internete: <https://www.coolest-gadgets.com/piracy-statistics/?utm>

Pagal NTV lygį pasaulyje pirmauja televizijos laidos – 49,4 proc. Programinės įrangos NTV siekia 26,2 proc. Filmai ir muzika sudaro atitinkamai 17,1 proc. ir 16 proc. Leidybos industrijoje, ypač kai tai liečia knygas, NTV lygis siekia 11,2 proc. Per pastaruosius kelerius metus atsirado nauja NTV rinka – knygos. Dažniausiai knygas NTV 30–44 metų amžiaus grupės asmenys. NTV pramogų srityje statistika rodo, kad muzikos ir filmų NTV išliko populiariausias tarp jaunesnių žmonių. Nors abi lytys reguliariai NTV muzikos ir televizijos laidų įrašus, atrodo, kad vyrai labiau linkę tokį elgesį vertinti teigiamai.²¹

EUROPINIAI RODIKLIAI

Taip pat remiantis **EUIPO atlikto tyrimo 2020 m. duomenimis** (žr. paveikslėlį toliau), NTV lygis kiekvienoje ES valstybėje narėje ir Jungtinėje Karalystėje, suskirstytas pagal turinio tipą. Latvijoje, Estijoje ir Lietuvoje vienam naudotojui per mėnesį teko daugiausia NTV turinio peržiūrų – atitinkamai 13,9, 12,5 ir 11,5 procentų. Lenkijoje, Vokietijoje ir Suomijoje šis rodiklis mažiausias – atitinkamai 3,8, 4,0 ir 4,8 procentų prieigos vienam naudotojui per mėnesį. Ispanijoje, Italijoje, Austrijoje ir Rumunijoje šis rodiklis taip pat yra mažesnis už ES vidurkį (5,9).

²¹Coolest gadgets, „Piracy Statistics By Demographics, Frequency, Reasons, Types, Software and Regions“, 2024. Prieiga internete: <https://www.coolest-gadgets.com/piracy-statistics/?utm>



4 paveikslas. Bendras NTV atvejų skaičius pagal šalį ir turinio tipą, vidutinė vertė 2020 m.

Šaltinis: Online copyright infringement in the European Union music, films and tv (2017–2020), trends and drivers. Prieiga internete: https://euiipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/quantification-of-ipr-infringement/online-copyright-infringement-in-eu/online_copyright_infringement_in_eu_en.pdf

Taip pat, buvo išnagrinėti keli veiksniai, galintys turėti įtakos NTV turinio vartojimui konkrečioje šalyje. Šie veiksniai apėmė socialinius ir ekonominius kintamuosius (pajamų lygis, išsilavinimas, nelygybė, nedarbas); demografinį kintamąjį, pavyzdžiui, jaunimo dalis populiacijoje; kintamąjį, susiję su atitinkamos rinkos ypatybėmis, įskaitant rinkos dydį, jos mastą, naudotojų internete infrastruktūrą ir teisėtų pasiūlymų, susijusių su įvairių rūšių turiniu, skaičių; ir požiūrį į intelektualinės nuosavybės pažeidimus, kaip nurodyta intelektualinės nuosavybės suvokimo tyrime, kurį paskelbė EUIPO.²² O NTV būdas ir turinio rūšis taip pat, kaip ir pasaulio mastu, Europoje yra labai panašus: populiariausia NTV rūšis yra TV laidos.

LIETUVOS SITUACIJA

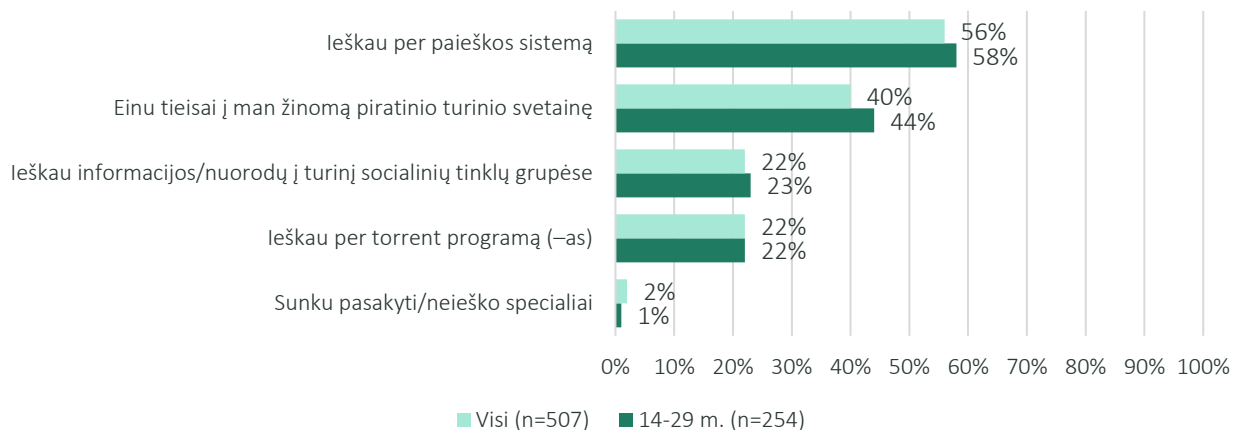
Remiantis Kultūros ministerijos 2024 m. atliktu tyrimu, 4 iš 10 Lietuvos gyventojų bent kartais vartoja nelegalų turinį (įvertinus paklaidą, tikrasis skaičius būtų 37–43 proc. Lietuvos gyventojų), o reguliariai tai daro ketvirtadalis gyventojų. Nelegalus dažniausiai vartojamas audiovizualinis turinys (filmai, serialai, televizijos laidos, vaizdo įrašai) (33 proc.) bei klausoma muzika (26 proc.). Lietuvos respondentai pasižymėjo sąlyginai nuolankiu požiūriu į nelegalaus turinio naudojimą bei platinimą. Būtina turėti omenyje, kad realus nelegalių šaltinių vartojimo lygis gali būti didesnis, nes Kultūros ministerijos atliktas tyrimas yra tik respondentų subjektyvus įsivertinimas (atsižvelgiant į jiems užduotus klausimus). Lietuvoje dar nėra iki galo aiškiai suprantama, jog bet kokia nelegalaus turinio vartojimo forma yra laikoma piratavimu ir daro žalą turinio kūrėjams. Aptarti rezultatai parodo aiškų gyventojų švietimo poreikį šia tema. Taip Lietuvoje gyvenantys piliečiai (į tyrimą įtraukta 14–64 m. amžiaus gyventojų imtis), pabrėžia pagrindines priežastis nelegalaus turinio naudojimui:

- kaina;
- prieigos prie legalaus turinio nepakankamumas;
- informacijos spragos dėl piratavimo sukiamų nuostolių;

²² EUIPO, „ONLINE COPYRIGHT INFRINGEMENT IN THE EUROPEAN UNION MUSIC, FILMS AND TV (2017–2020), TRENDS AND DRIVERS“, 2021, 70 p. Prieiga internetu: https://euiipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/quantification-of-ipr-infringement/online-copyright-infringement-in-eu/online_copyright_infringement_in_eu_en.pdf

- aukštas piratavimo tolerancijos lygis.

Didžiausiu piratavimo mastu pasižymi 14–29 m. amžiaus respondentų grupė. 14–64 m. amžiaus respondentų grupėje 25 proc. apklaustųjų nurodo, jog negeba atskirti legalaus turinio nuo nelegalaus. Tikslinėje jaunimo grupėje 14–29 m. šis rodiklis siekia 20 proc. Bendras piratavimo indeksas (apskaičiuotas Kultūros Ministerijos 2024 m. tyrime surinktais duomenimis) 14–64 m. gyventojų grupėje yra reikšmingai mažesnis (38 proc.), nei tikslinėje 14–29 m. amžiaus jaunimo grupėje (53 proc.).²³ Populiariausias nelegalaus turinio paieškos būdas yra per paieškos sistemą, o antras pagal populiarumą metodas – pasirenkant konkrečią jau iš anksto žinomą nelegalaus turinio svetainę. Prie nelegalaus turinio sklaidos ženkliai prisideda socialinių tinklų grupėse esanti informacija apie nelegalaus turinio svetaines bei gerai pažįstamas nelegalaus turinio paieškos metodus torentų sklaidos tinklais.



1 paveikslas. Nelegalaus turinio paieškos būdai Lietuvoje, 2024 m.

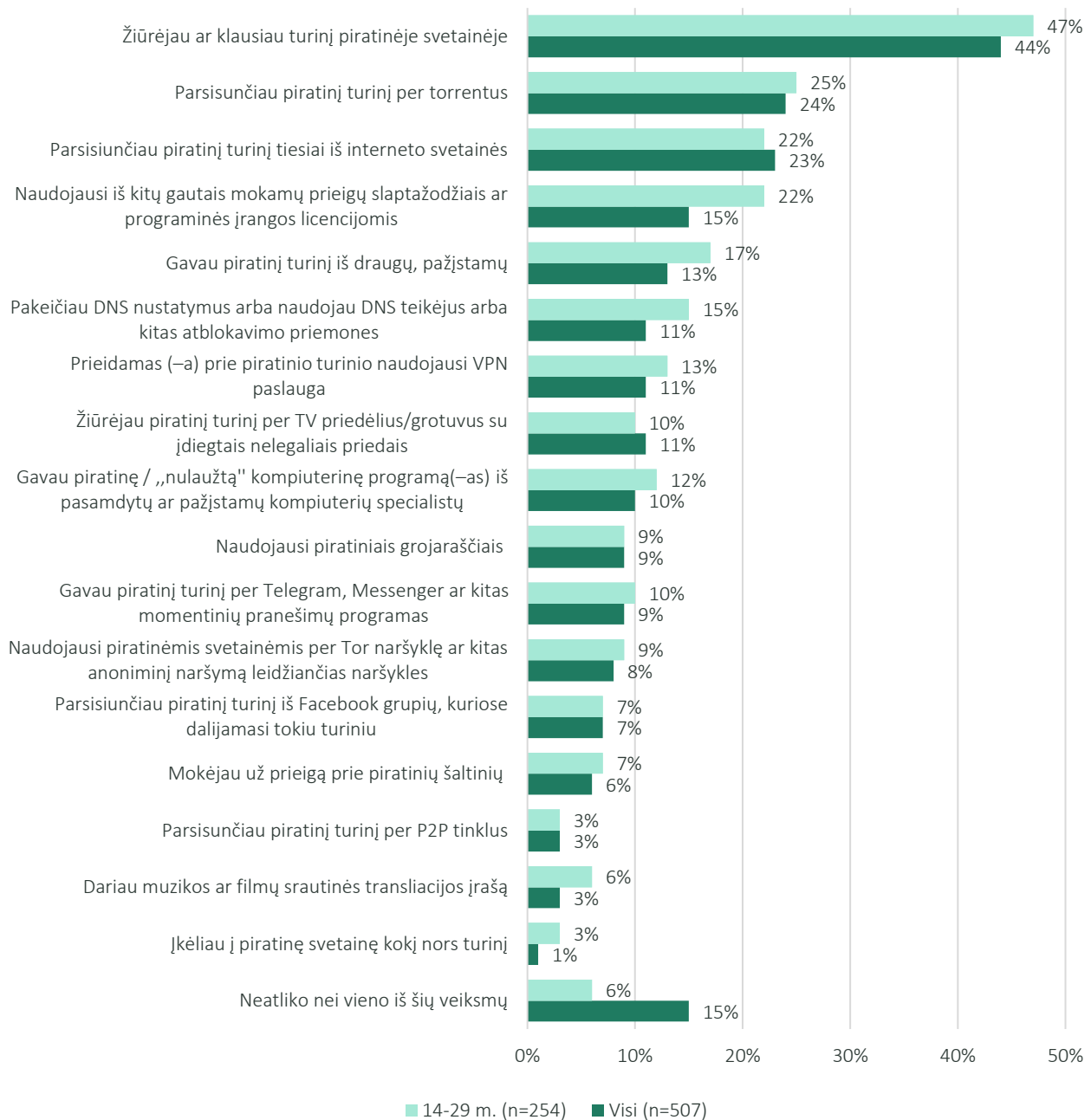
Šaltinis: parengta Konsultanto, remiantis Kultūros ministerijos duomenimis²⁴

Populiariausi nelegalaus turinio prieigos būdai išlieka šie trys:

- prieiga prie žinomų NTS svetainių;
- nelegalaus turinio parsisiuntimas per torentų sklaidos puslapius;
- nelegalaus turinio siuntimasis tiesiai iš internetinių svetainių.

²³ Lietuvos Respublikos kultūros ministerija, Lietuvos gyventojų nelegalaus turinio vartojimo lygio nustatymo tyrimas, 2024m. Prieiga internetu: https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.kulturostyrimai.lt%2Fwp-content%2Fuploads%2F2024%2F10%2FLietuvos-gyventoju-nelegalaus-turinio-vartojimo-lygio-nustatymo-tyrimas_Santrauka_2024.pdf&psig=AOvVaw3MghNTtLV2OUBBamkt3No2&ust=1740728977480000&source=images&cd=vfe&opi=89978449&ved=0CAQQn5wMahcKEwiYsbP0ruOLAxUAAAAAHQAAAAAQBA

²⁴ Ten pat

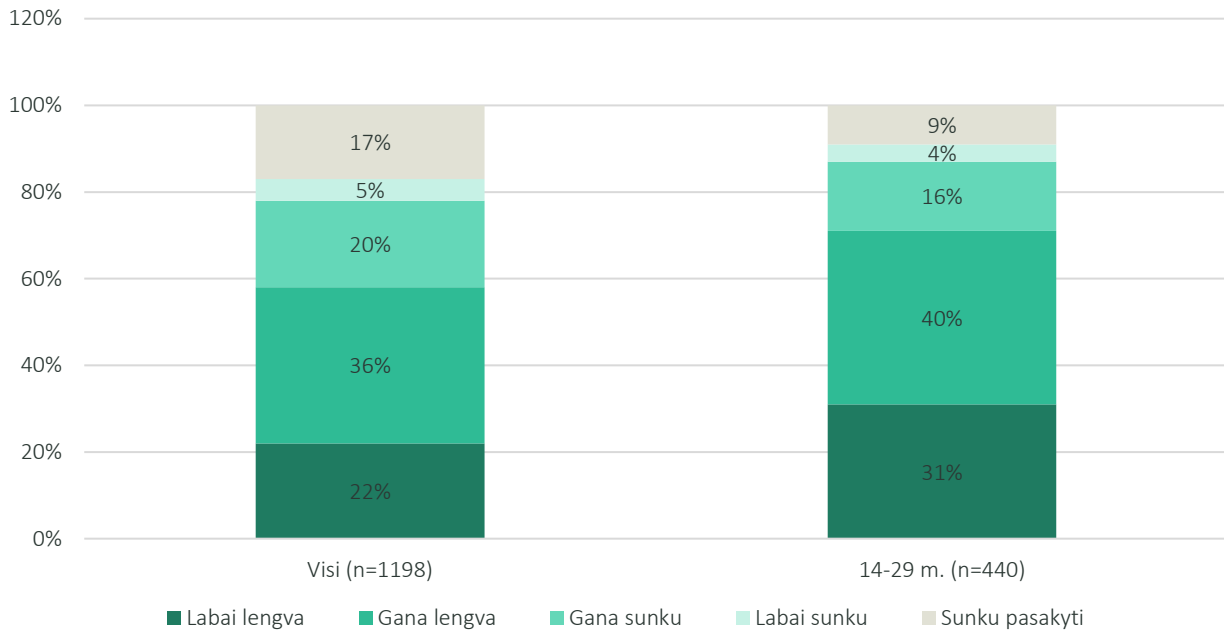


2 paveikslas. Populiariausi nelegalaus turinio prieigos būdai Lietuvoje, 2024 m.

Šaltinis: parengta Konsultanto, remiantis Kultūros ministerijos duomenimis²⁵

Iš toliau pateiktos diagramos pastebima, jog apie ketvirtadalis gyventojų nurodo negalintys lengvai atskirti legalaus ir nelegalaus turinio šaltinių. Be to, atsakydami į klausimą apie legalių ir nelegalių šaltinių naudojimą skirtingose turinio kategorijose, 13–28 proc. naudotojų rinkosi variantą „sunku pasakyti“. Žinių trukumas gali lemti gebėjimų atskirti nelegalų turinį nuo legalaus trūkumą ir taip prisidėti prie piratavimo masto.

²⁵ Lietuvos Respublikos kultūros ministerija, Lietuvos gyventojų nelegalaus turinio vartojimo lygio nustatymo tyrimas, 2024m. Prieiga internetu: https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.kulturostyrimai.lt%2Fwp-content%2Fuploads%2F2024%2F10%2FLietuvos-gyventoju-nelegalaus-turinio-vartojimo-lygio-nustatymo-tyrimas_Santrauka_2024.pdf&psig=AOvVaw3MghNTtLV2OUBBamkt3No2&ust=1740728977480000&source=images&cd=vfe&opi=89978449&ved=0CAQqn5wMahcKEwiYsbP0ruOLaxUAAAAAHQAAAAQBA



3 paveikslas. Gebėjimas atskirti legalią ir nelegalią prieigą prie internetinio turinio. Klausimas: Kiek Jums asmeniškai lengva ar sunku atskirti, ar internetinė prieiga prie Jūsų naudojamo turinio (filmų, muzikos, el. knygų ir t. t.) yra legali ar piratinė? (Visi respondentai, N žr. diagramoje), 2024 m.

Šaltinis: sudaryta konsultanto remiantis Kultūros ministerijos duomenimis²⁶

Atsižvelgiant į Kultūros ministerijos tyrimo rezultatus per pastaruosius 12 mėnesių nelegalų turinį iš viso naudojo 40 proc. tyrimo dalyvių. 26 proc. apklaustųjų vartojo bent vienos kategorijos nelegalų turinį kelis kartus per mėnesį ar dažniau. 14 proc. yra priskiriami prie „nereguliaraus pirato“ kategorijos ir vartoja bent vienos kategorijos nelegalų turinį kartą per mėnesį. Vertinant lyčių piratavimo tendencijas, 44 proc. vyrų respondentų prisipažįsta, kad naudojo nelegalų turinį, moterų nelegalų turinį naudojo rečiau – 36 proc. (bendras Lietuvos gyventojų rodiklis – 40 proc.).

Toliau pateikiama glausta nelegalų turinį per pastaruosius 12 mėn. vartojusių ir jo nevartojusių respondentų analizė pagal sociodemografinius požymius:

- Dažniausiai nelegaliu turiniu naudojosi 14–29 m., rečiausiai – 45–64 m. amžiaus grupei priklausantys respondentai.
- Pastebima, jog piratavimo lygis aukštesnis yra didmiesčiuose (48 proc.) ir Vilniuje (46 proc.), lyginant su miesteliais ir kaimo vietovėmis (31 proc.).
- Matoma koreliacija tarp piratavimo ir darbo užmokesčio dydžio – aukštesnis darbo užmokestis koreliuoja su žemesniais piratavimo rodikliais.

Nelegalaus turinio platforma *Filmai.in* buvo dažniausiai tyrimo dalyvių minima nelegalaus turinio svetainė – respondentai paklausti ar žino nelegalių svetainių pavyzdžių – ją nurodė 31 proc. respondentų (kitos dažniausiai minimos nelegalaus turinio svetainės – *Linkomanija* bei *torentai*). Šis klausimas buvo užduodamas siekiant sužinoti ar respondentai žino nelegalaus turinio svetainių, tačiau neimplikuojant, jog jie būtinai jomis naudojami.

Akcentuotina, jog nelegalaus turinio platformas, tokias kaip *Filmai.in* ar *Linkomanija*, legaliomis laiko 4 proc. visų tyrimo dalyvių. 40 proc. apklaustųjų respondentų atsakė, jog atskirti nelegalų turinį yra gana sunku arba labai sunku.

²⁶ Lietuvos Respublikos kultūros ministerija, Lietuvos gyventojų nelegalaus turinio vartojimo lygio nustatymo tyrimas, 2024m. Prieiga internetu: https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.kulturostyrimai.lt%2Fwp-content%2Fuploads%2F2024%2F10%2FLietuvos-gyventoju-nelegalaus-turinio-vartojimo-lygio-nustatymo-tyrimas_Santrauka_2024.pdf&psig=AOvVaw3MghNTtLV2OUBBamkt3No2&ust=1740728977480000&source=images&cd=vfe&opi=89978449&ved=0CAQQn5wMahcKEwiYsbP0ruOLaxUAAAAAHQAAAAQBA

Daugiau nei pusė visų tyrimo dalyvių (58 proc.) ir 71 proc. konkrečiai 14–29 metų amžiaus grupės atstovų nurodė, kad jie labai lengvai arba palyginti lengvai gali atskirti, ar jų naudojama prieiga prie internetinio turinio yra legali. Pastebima, kad 14–29 metų amžiaus grupė bendrai internetinį turinį vartoja dažniau nei vyresni gyventojai – jie dažniau negu kitos amžiaus grupės internete klausosi muzikos, žaidžia vaizdo žaidimus ar naudojami mokamomis kompiuterinėmis programomis. Kaip ir visi tyrimo dalyviai, 14–29 metų amžiaus asmenys nelegalaus turinio dažniausiai ieško per „Google“ paieškos sistemą ar kitas paieškos sistemas arba tiesiogiai prisijungia prie jiems žinomos NVS svetainės ir nelegalų turinį dažniausiai žiūri ar klauso šiose svetainėse. Ši amžiaus grupė dažniau nei kitos respondentų grupės yra linkusi naudotis iš kitų asmenų gautais mokamo turinio platformų prieigų slaptažodžiais ar programinės įrangos licencijomis. Apibendrinant galima pastebėti, jog kad jaunimas, lyginant su kitomis amžiaus grupėmis, yra sąlyginai labiau technologiškai išprusęs, šie asmenys linkę įdėti daugiau pastangų pasiekti nelegalų turinį nei visi tyrimo dalyviai.

Atlikus kiekybinę pirminių Kultūros ministerijos tyrimo duomenų analizę buvo specifiskai pasirinkta tikslinė grupė iš bendros populiacijos. Tikslinė grupė buvo atrinkta remiantis tuo, kokius atsakymus respondentai pasirinko atsakant į ROD2 ir ROD6 klausimus. Atsakymai į ROD2 klausimą nurodo, koks yra bendras nelegalaus turinio vartojimo lygis pasirinktoje imtyje (1198 respondentai), o ROD6 klausimo atsakymai rodo, kaip gerai / blogai respondentai sugeba atskirti nelegalų turinį nuo legalaus. Sujungus šių dviejų klausimų atsakymus į vieną respondentų grupę gaunami 383 respondentai, kurie dalinasi dvejomis bendromis charakteristikomis – vartoja nelegalų turinį („naudojau dalį legalaus, dalį piratinio turinio / naudoju tik/daugiausia piratinį turinį“) ir tuo pačiu pasirinko, jog jiems yra labai sunku arba gana sunku atskirti nelegalų turinį nuo legalaus. Šių dviejų charakteristikų junginys sukuria prielaidą, jog respondentas – potencialiai naudojami nelegaliu turiniu dėl to, nes negali / nemoka atskirti nelegalaus turinio, nors būtų linkęs rinktis legalaus turinio vartojimo būdus.

Tam, jog būtų galima susidaryti kuo detalesnį šios galimybių studijos tikslinės grupės – nelegalaus turinio naudotojo bei asmens, sunkiai atskiriančio nelegalų turinį internete, portretą, buvo pasirinkta ir kiti – papildomi elementai, kurie padeda pažvelgti į nelegalaus turinio naudotojus iš gilesnio socialinio ekonominio pjūvio. Šie atsakymai į toliau pateiktus klausimus padeda peržvelgti, kas lemia tikslinės grupės atstovą rinktis nelegalaus turinio alternatyvas.

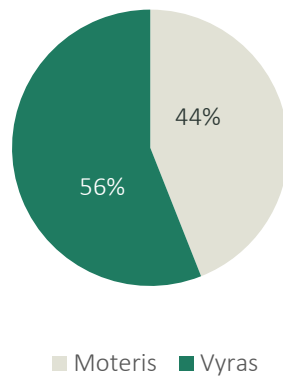
Respondentai, atsakę, kad vartoja nelegalų turinį, ir kad sunkiai atskiria nelegalų ir legalų turinį (tikslinė tyrimo grupė), buvo vertinami pagal toliau pateiktus rodiklius:

- **GENDER** – lytis (moteris ir vyras);
- **AGEGR1** – amžius;
- **OCP1** – užimtumas (dirba, nedirba);
- **D12R** – internetu naudojimosi įgūdžiai;
- **K7_1-9** – legalaus ir nelegalaus turinio vartojimas pagal turinį;
- **K11_1-9** – nelegalaus turinio pasirinkimo priežastys.

Socialiniai faktoriai (amžius, lytis) padedantis susidaryti individo demografinį vaizdą, o likusieji indikatoriai – internetu naudojimosi įgūdžiai, legalaus ir nelegalaus turinio vartojimas pagal turinį, nelegalaus turinio pasirinkimo priežastys – padės giliau suprasti technologinio sprendimo poreikį bei įgyvendinimo galimybes.

LYTIS

Toliau pateiktoje diagramoje pateikiami duomenys pagal tikslinės grupės respondentų subjektyvius atsakymus į prieš tai minėtus klausimus (bendras nelegalaus turinio vartojimo lygis ir nebėgėjimas atskirti legalių ir nelegalių internetinio turinio prieigų). Šie respondentų atsakymai yra agreguoti atitinkamai pagal lytį.



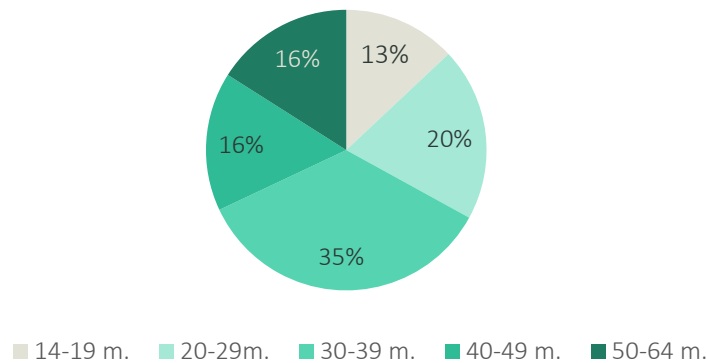
4 paveikslas. Respondentai pagal lytį, kurie sunkiai atskiria nelegalų turinį nuo legalaus ir tuo pačiu atsakė į klausimą, jog naudojami nelegaliu turiniu, 2024 m.

Šaltinis: parengta konsultanto remiantis Kultūros ministerijos duomenimis²⁷

Visoje Kultūros Ministerijos tyrimo respondentų imtyje (1198) 48 proc. moterų naudoja nelegalų turinį, vyrų – 52 proc. Tuo tarpu pritaikius prieš tai minėtus specialius tikslinei grupei pritaikytus indikatorius – nelegalaus turinio vartojimą ir silpnus įgūdžius atpažįstant legalų nuo nelegalaus turinio internete – rezultatai šiek tiek skiriasi – tikslinėje grupėje santykinai daugiau vyrų.

AMŽIAUS GRUPĖS

Toliau pateiktoje diagramoje pateikiami duomenys, kaip Kultūros Ministerijos tyrime respondentai, skirtingose amžiaus grupėse, naudoja piratinį turinį bei sunkiai geba atskirti legalius nuo nelegalių internetinio turinio šaltinius.



5 paveikslas. Respondentų dalis, kurie sunkiai atskiria nelegalų / legalų turinį ir vartoja nelegalų turinį pagal amžių, 2024 m.

Šaltinis: parengta konsultanto remiantis Kultūros ministerijos duomenimis²⁸

Bendroje imtyje respondentų pasiskirstymas yra toks:

- 28 proc. – 50–64 m.;
- 24 proc. – 30–39 m.;
- 21 proc. – 40–49 m.;

²⁷ Lietuvos Respublikos kultūros ministerija, Lietuvos gyventojų nelegalaus turinio vartojimo lygio nustatymo tyrimas, 2024m. Prieiga internetu: https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.kulturostyrimai.lt%2Fwp-content%2Fuploads%2F2024%2F10%2FLietuvos-gyventoju-nelegalaus-turinio-vartojimo-lygio-nustatymo-tyrimas_Santrauka_2024.pdf&psig=AOvVaw3MghNTtLV2OUBBamkt3No2&ust=1740728977480000&source=images&cd=vfe&opi=89978449&ved=0CAQQn5wMahcKEwiYsbP0ruOLAxUAAAAAHQAAAAQBA

²⁸ Ten pat

- 17 proc. – 20–29 m.;
- 10 proc. – 14–19 m.

Didžiausia dalis respondentų, besirenkančių naudoti nelegalų turinį ir negebantys atskirti legalių šaltinių nuo nelegalių yra 30–39 m. amžiaus grupė, kuri ir užima 35 proc. Skirtumas tarp tikslinės grupės šioje amžiaus grupėje (35 proc.) bei šios amžiaus grupės dalies bendroje populiacijoje (24 proc.), yra didžiausias – 11 proc. maksimalios paklaidos riboje. Tai indikuoja, jog skirtumas yra reikšmingas, o žmonės šioje amžiaus grupėje sunkiai atskiria nelegalų turinį ir naudojami nelegaliu turiniu.

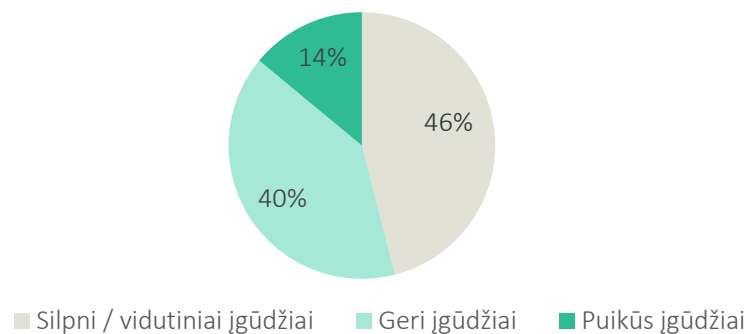
Antroje vietoje pagal respondentų skaičių tikslinėje grupėje yra 20–29 m. amžiaus individai, kurie užima 20 proc. Bendroje tyrimo imtyje ši amžiaus grupės respondentų yra 17 proc. Tarp jų nėra didesnio nei 3 proc. skirtumo, kas yra maksimali paklaidos riba, todėl skirtumas skaitomas, kaip nereikšmingas. Taip pat yra ir su pirmąją, 14–19 m. amžiaus grupe, kurių dalis tikslinėje grupėje yra 13 proc., o bendroje imtyje – 10 proc.

Reikšmingas (didesnis nei maksimali paklaidos riba – 3 proc.) skirtumas tarp dviejų likusių amžiaus grupių tikslinėje grupėje lyginant su bendra populiacija yra 40-49 m. ir 50-64 m. amžiaus grupėje. Skirtumai tarp šių amžiaus grupių lyginant su bendra populiacija yra šie:

- 40-49 m. tikslinėje grupėje – 16 proc., bendroje imtyje 21 proc. – 5 proc. skirtumas.
- 50-64 m. tikslinėje grupėje 16 proc., o lyginant su bendra imtimi – 28 proc., skirtumas yra 12 proc.

NAUDOJIMOSI INTERNETU ĮGŪDŽIAI

Toliau pateikiami duomenys remiantis Kultūros Ministerijos 2024 m. tyrimo rezultatais, kuriuose pateikiami respondentų tikslinėje grupėje (žmonės, kurie sunkiai atskiria nelegalų turinį nuo legalaus ir kartu vartoja nelegalų turinį).



6 paveikslas. Naudojimosi internetu įgūdžiai tikslinėje respondentų grupėje, 2024 m.

Šaltinis: parengta konsultanto remiantis Kultūros Ministerijos duomenimis²⁹

Bendroje tyrimo populiacijoje pagal internetu naudojimosi įgūdžius žmonių pasiskirstymas yra toks:

- Silpni / vidutiniai įgūdžiai – 37 proc.
- Geri įgūdžiai – 40 proc.
- Puikūs įgūdžiai – 23 proc.

Reikšmingas skirtumas matomas silpnų / vidutinių bei gerų įgūdžių tikslinės grupėje (žmonės, kurie sunkiai atskiria nelegalų turinį nuo legalaus ir kartu vartoja nelegalų turinį) lyginant su bendra populiacija. 37 proc. žmonių

²⁹ Lietuvos Respublikos kultūros ministerija, Lietuvos gyventojų nelegalaus turinio vartojimo lygio nustatymo tyrimas, 2024m. Prieiga internetu: https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.kulturostyrimai.lt%2Fwp-content%2Fuploads%2F2024%2F10%2FLietuvos-gyventoju-nelegalaus-turinio-vartojimo-lygio-nustatymo-tyrimas_Santrauka_2024.pdf&psig=AOvVaw3MghNTtLV2OUBBamkt3No2&ust=1740728977480000&source=images&cd=vfe&opi=89978449&ved=0CAQQn5wMahcKEwiYsbP0ruOLAxUAAAAAHQAAAAQBA

bendroje populiacijoje turi silpnus ir vidutinius įgūdžius turi, tikslinėje grupėje silpnus ir vidutinius internetu naudojimosi įgūdžius turi 9 procentais didesnė dalis (46 proc.)

Puikius įgūdžius bendroje populiacijoje turi 23 proc. žmonių, o tikslinėje grupėje puikius internetu naudojimosi įgūdžius turi 9 proc. mažesnė žmonių dalis (14 proc.).

Toliau pateiktoje lentelėje išskiriami dažniausiai naudojamas nelegalus audiovizualinis turinys pagal turinio tipą. Pažymėtina, kad šio tyrimo maksimalios paklaidos riba yra 3 proc.

1 lentelė. Legalaus ir nelegalaus turinio vartojimas pagal turinį visoje respondentų imtyje, tikslinėje grupėje ir specialioje imtyje

| Nr. | Rodiklio pavadinimas Tyrimo – K7_1-9 | Pasirinkimo variantai | Visa imties dalis procentai | Tikslinė grupė (asmenys, kurie naudoja nelegalų turinį, bet sunkiai atskiria nelegalų turinį – ROD6-1, ROD2-1) | Nelegalų turinį naudojantys asmenys (ROD2-1) |
|-----|---|--|-----------------------------|--|--|
| 1. | Filmai, serialai, televizijos laidos, vaizdo įrašai (išskyrus sporto transliacijas) | (1) Naudojau tik legalų turinį | 43% | 16% | 17% |
| | | (2) Naudojau dalį legalaus, dalį piratinio turinio | 23% | 60% | 58% |
| | | (3) Naudojau tik / daugiausia piratinį turinį | 7% | 15% | 17% |
| | | (4) Sunku pasakyti | 16% | 5% | 5% |
| | | Neatsakė | 4% | 4% | 4% |
| 2. | Muzika (išskyrus muzikos vaizdo įrašus, natas) | Naudojau tik legalų turinį | 11% | 24%* | 27% |
| | | Naudojau dalį legalaus, dalį piratinio turinio | 57% | 49%* | 52% |
| | | Naudojau tik / daugiausia piratinį turinį | 3% | 12%* | 8% |
| | | Sunku pasakyti | 16% | 9% | 7% |
| | | Neatsakė | 13% | 6% | 6% |
| 3. | Sporto transliacijos | Naudojau tik legalų turinį | 41% | 39% | 38% |
| | | Naudojau dalį legalaus, dalį piratinio turinio | 7% | 14%* | 18% |
| | | Naudojau tik / daugiausia piratinį turinį | 2% | 9%* | 5% |
| | | Sunku pasakyti | 11% | 14%* | 7% |
| | | Neatsakė | 39% | 24%* | 32% |
| 4. | Dramos kūriniai | Naudojau tik legalų turinį | 21% | 16% | 16% |
| | | Naudojau dalį legalaus, dalį piratinio turinio | 5% | 13% | 13% |
| | | Naudojau tik / daugiausia piratinį turinį | 2% | 6% | 4% |
| | | Sunku pasakyti | 11% | 17%* | 10% |
| | | Neatsakė | 62% | 48%* | 56% |
| 5. | Rašytinis turinys | Naudojau tik legalų turinį | 36% | 34%* | 31% |
| | | Naudojau dalį legalaus, dalį piratinio turinio | 8% | 17%* | 21% |
| | | Naudojau tik / daugiausia piratinį turinį | 3% | 11%* | 8% |
| | | Sunku pasakyti | 12% | 9% | 9% |

| Nr. | Rodiklio pavadinimas Tyrimo – K7_1-9 | Pasirinkimo variantai | Visa imties dalis procentai | Tikslinė grupė (asmenys, kurie naudoja nelegalų turinį, bet sunkiai atskiria nelegalų turinį – ROD6-1, ROD2-1) | Nelegalų turinį naudojančias asmenys (ROD2–1) |
|-----|--|--|-----------------------------|---|---|
| 6. | Muzikos natos | Neatsakė | 40% | 28% | 30% |
| | | Naudojau tik legalų turinį | 10% | 6%* | 10% |
| | | Naudojau dalį legalaus, dalį piratinio turinio | 3% | 11%* | 8% |
| | | Naudojau tik / daugiausia piratinį turinį | 2% | 9%* | 4% |
| | | Sunku pasakyti | 5% | 5% | 5% |
| | | Neatsakė | 80% | 69%* | 72% |
| 7. | Mokomasis audiovizualinis turinys | Naudojau tik legalų turinį | 45% | 42% | 44% |
| | | Naudojau dalį legalaus, dalį piratinio turinio | 5% | 16%* | 13% |
| | | Naudojau tik / daugiausia piratinį turinį | 2% | 8%* | 4% |
| | | Sunku pasakyti | 10% | 11%* | 8% |
| | | Neatsakė | 38% | 23%* | 30% |
| 8. | Vaizdo žaidimai | Naudojau tik legalų turinį | 37% | 33%* | 37% |
| | | Naudojau dalį legalaus, dalį piratinio turinio | 8% | 17% | 19% |
| | | Naudojau tik / daugiausia piratinį turinį | 3% | 8% | 8% |
| | | Sunku pasakyti | 10% | 10%* | 6% |
| | | Neatsakė | 42% | 32% | 30% |
| | | Naudojau tik legalų turinį | 47% | 40% | 42% |
| 9. | Kompiuterinės programos | Naudojau dalį legalaus, dalį piratinio turinio | 10% | 26% | 25% |
| | | Naudojau tik / daugiausia piratinį turinį | 4% | 13% | 11% |
| | | Sunku pasakyti | 9% | 6% | 6% |
| | | Neatsakė | 29% | 15% | 16% |
| | | Naudojau tik legalų turinį | 47% | 40% | 42% |

Šaltinis: Sudaryta Konsultanto, remiantis Kultūros Ministerijos tyrimu, 2024 m.³⁰

* – reprezentuoja reikšmingą (didesnį nei maksimalios paklaidos riba – 3 proc.) skirtumą tarp tikslinės grupės atsakymo ir spec. imties

Atsižvelgiant į lentelėje pateiktus duomenis, galima daryti išvadą, kad tikslinės grupės respondentai iš esmės nesiskiria nuo vidutinio nelegalaus turinio naudotojo Lietuvoje. Reikšmingesni skirtumai pastebimi kalbant apie šias turinio rūšis:

- Muzika (išskyrus muzikos vaizdo įrašus, natas)
- Sporto transliacijos

³⁰ Lietuvos Respublikos kultūros ministerija, Lietuvos gyventojų nelegalaus turinio vartojimo lygio nustatymo tyrimas, 2024m. Prieiga internetu: https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.kulturostyrimai.lt%2Fwp-content%2Fuploads%2F2024%2F10%2FLietuvos-gyventoju-nelegalaus-turinio-vartojimo-lygio-nustatymo-tyrimas_Santrauka_2024.pdf&psig=AOvVaw3MghNTtLV2OUBBamkt3No2&ust=1740728977480000&source=images&cd=vfe&opi=89978449&ved=0CAQq5wMahcKEwiYsbP0ruOLaxUAAAAAHQAAAAQBA

- Dramos kūriniai
- Muzikos natos
- Mokomasis audiovizualinis turinys

Toliau lentelėje pateikiami duomenys pagal visos respondentų imties, tikslinės grupės bei specialios tikslinės grupės atsakymų rezultatus, atsakant į klausimą, kodėl respondentai renkasi nelegalų turinį.

2 lentelė. Nelegalaus turinio vartojimo pasirinkimo priežastys visoje respondentų imtyje, tikslinėje grupėje ir sepcialioje imtyje

| Nr. | Rodiklio pavadinimas Tyrimo – K7_1-9 | Pasirinkimo variantai | Visa imties dalis procentai | Tikslinė grupė (asmenys, kurie piratauja, bet sunkiai atskiria nelegalų turinį – ROD6-1, ROD2-1) | Spec. imtis – pirataujantys asmenys (ROD2-1) |
|-----|---|--------------------------|--------------------------------|--|--|
| 1. | Nenoriu mokėti už tai, ką galiu gauti nemokamai | (0) Ne | 26% | 67% | 66% |
| | | (1) Taip | 13% | 33% | 34% |
| | | Neatsakė | 60% | 0% | 0% |
| 2. | Legaliai pirkti turinį man yra per brangu | (0) Ne | 22% | 62%* | 55% |
| | | (1) Taip | 18% | 38%* | 45% |
| | | Neatsakė | 60% | 0% | 0% |
| 3. | Naudoju tam tikrą turinį gana retai ir nenoriu mokėti už tai, kuo pasinaudosiu vos kelis kartus | (0) Ne | 27% | 67% | 68% |
| | | (1) Taip | 13% | 33% | 32% |
| | | Neatsakė | 60% | 0% | 0% |
| 4. | Legaliuose šaltiniuose nerandu norimo turinio | (0) Ne | 26% | 72%* | 67% |
| | | (1) Taip | 13% | 28%* | 33% |
| | | Neatsakė | 60% | 0% | 0% |
| 5. | Piratinuose šaltiniuose galiu rasti daugiau įvairesnio turinio | (0) Ne | 28% | 79%* | 70% |
| | | (1) Taip | 12% | 21%* | 30% |
| | | Neatsakė | 60% | 0% | 0% |
| 6. | Noriu peržiūrėti turinį kuo greičiau, nelaukdamas (-a), kol jis pasirodys legaliuose šaltiniuose | (0) Ne | 30% | 77% | 76% |
| | | (1) Taip | 10% | 23% | 24% |
| | | Neatsakė | 60% | 0% | 0% |
| 7. | Turinį iš nelegalių šaltinių galiu naudoti pakartotinai bet kuriame įrenginyje | (0) Ne | 35% | 87% | 88% |
| | | (1) Taip | 5% | 13% | 12% |
| | | Neatsakė | 60% | 0% | 0% |
| 8. | Noriu išbandyti turinį prieš jį pirkdamas (-a) iš legalios svetainės | (0) Ne | 34% | 82%* | 86% |
| | | (1) Taip | 5% | 18%* | 14% |
| | | Neatsakė | 60% | 0% | 0% |
| 9. | Trūksta legalaus turinio man gerai suprantama arba mano gimtąja kalba | (0) Ne | 29% | 72% | 74% |
| | | (1) Taip | 10% | 28% | 28% |
| | | – | 60% | 0% | 0% |

Šaltinis: Sudaryta Konsultanto, remiantis Kultūros Ministerijos tyrimu, 2024 m.

* – reprezentuoja reikšmingą (didesnį nei maksimalios paklaidos riba – 3 proc.) skirtumą tarp tikslinės grupės atsakymo ir spec. imties

Galima pastebėti, kad ženkliesni skirtumai tarp tikslinės grupės ir vidutinio nelegalaus turinio naudotojo pasimato šiose kategorijose:

- Legaliai pirkti turinį man yra per brangu – rečiau nurodoma kaina, kaip priežastis rinktis nelegalų turinį;

- Legaliuose šaltiniuose nerandu norimo turinio – dažniau nurodomas legalaus turinio trūkumas, kaip priežastis rinktis piratines internetines svetaines;
- Piratiniuose šaltiniuose galiu rasti daugiau įvairesnio turinio – dažniau nurodomas didesnis pasirinkimas piratiniuose šaltiniuose;
- Noriu išbandyti turinį prieš jį pirkdamas (-a) iš legalios svetainės – rečiau nurodomas noras išbandyti turinį prieš perkant jį.

Apibendrinant atliktą analizę galima išskirti šias įžvalgas Kuriamam technologiniam sprendimui:

- Lietuva išsiskiria nelegalaus turinio vartojimo mastu Europos kontekste. 4 iš 10 Lietuvos gyventojų pripažįsta naudojančius nelegalų turinį. Tikrasis piratavimo mastas gali būti didesnis (žmonės gali vengti prisipažinti).
- Galima išskirti 6 pagrindinius nelegalaus turinio sklaidos ir vartojimo modelius, tačiau 3 pagrindiniai – a) svetainės, kur nelegaliai transliuojamas audiovizualinis turinys; b) torrent technologijos pagalba parsisiunčiamas turinys ir c) tiesiogiai parsisiunčiamas turinys.
- Dažniausiai nelegalų turinį sklaidžiančios svetainės yra pasiekiamos per paieškos sistemas (pavyzdžiui, Google).
- Tikslinė Kuriamo technologinio sprendimo auditorija tik neženkliai išsiskiria iš vidutinio nelegalaus turinio naudotojo. Tikslinėje auditorijoje žmonės dažnai susiduria su iššūkiais randant jiems reikiamą legalų turinį, pasižymi prastesniais naudojimosi internetu įgūdžiais.

2. Galimų alternatyvų sudarymas

Šiame skyriuje yra apibendrinama atlikta užsienio šalių analizė, konsultacijų su suinteresuotomis pusėmis rezultatai ir suformuluojamos Kuriamo technologinio sprendimo alternatyvos (variantai).

2.1. Analizės tikslų ir metodikos apibrėžimas

TS nurodo, kad šios Studijos objektas – inovatyvaus technologinio sprendimo, galinčio identifikuoti nelegalų audiovizualinį turinį internete, įspėti apie tai naudotoją ir jam pasiūlyti norimą legalų turinį arba pasiūlyti iš esmės naują priegią prie legalaus turinio (technologinis sprendimas). Atsižvelgiant į papildomas konsultacijas, atliktas su Užsakovu, buvo patikslintas Studijos objektas, inovatyvaus technologinio sprendimo, sampratas – technologinis sprendimas yra suprantamas plačiau, kaip bet koks technologinis sprendimas, kuris galėtų prisidėti prie legalaus turinio vartojimo.

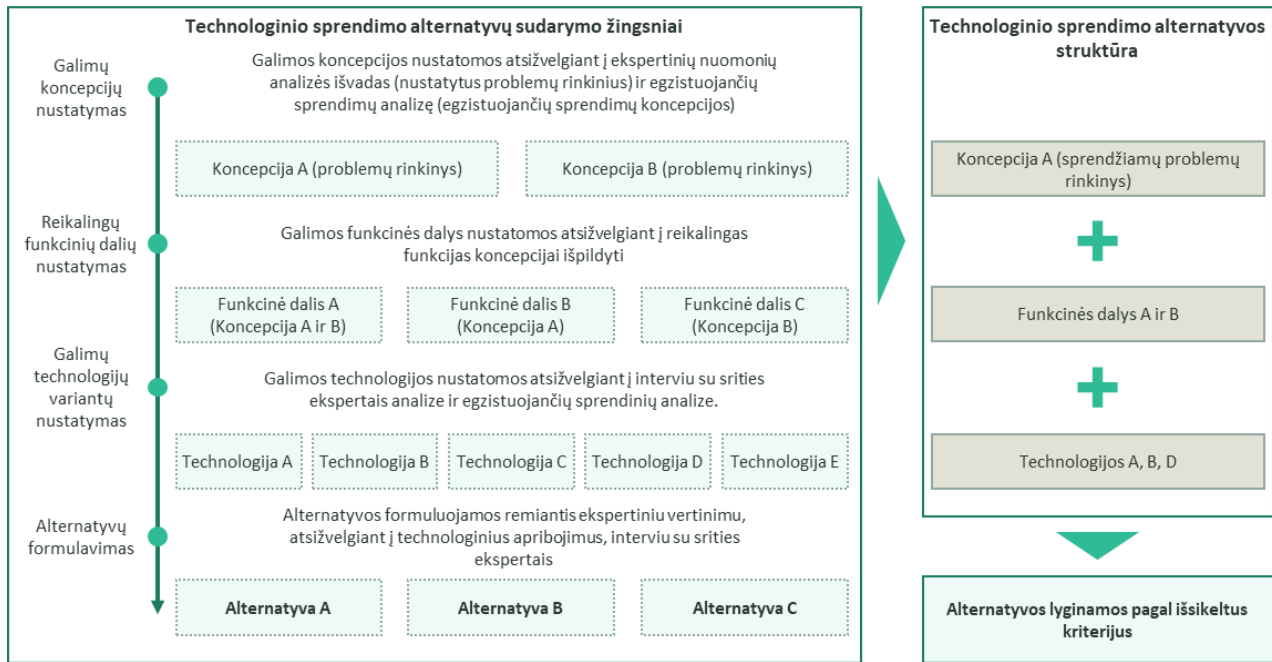
Šio skyriaus tikslas – optimalios technologinio sprendimo alternatyvos Lietuvos atvejui pasirinkimas. Pažymėtina, kad „alternatyva“ technologinio sprendimo kontekste, atsižvelgiant į praplėstą technologinio sprendimo sampratą, gali būti suprantama skirtingai. Toliau aprašomi skirtingi konceptai, skirti alternatyvų formulavimui:

- **Koncepcija (sprendžiamos problemos)** – atsižvelgiant į praplėstą technologinio sprendimo sampratą, galimos skirtingos technologinio sprendimo koncepcijos. Skirtingos koncepcijos gali spręsti skirtingas problemas (pavienės arba kelias), kurios yra susijusios su nelegalaus turinio sklaida ir naudojimu.
- **Funkcinės dalys** – galimos technologinio sprendimo koncepcijos, kai yra sprendžiama daugiau nei viena problema, technologinis sprendimas gali turėti skirtingas funkcines dalis. Pavyzdžiui, funkcinė dalis A skirta nelegalaus turinio nustatymui ir technologinė dalis B skirta legalaus šaltinio pasiūlymui. Šis išskyrimas yra svarbus, nes tos pačios funkcinės dalys gali būti sujungiamos į skirtingas kombinacijas.
- **Technologijos (funkcinių dalių išpildymo) variantai** – ta pati funkcinė dalis gali būti išpildoma taikant skirtingas technologijas. Pavyzdžiui, nelegalaus turinio nustatymo funkcinė dalis gali būti išpildoma internetinės svetainės duomenų palyginimo su duomenų bazėje esančiais internetinių svetainių, kur platinamas nelegalus turinys, sąrašais, būdu (paprasto sulyginimo algoritmai) arba taikant DI internetinės svetainės savybių analizei. Kiekviena iš skirtingų technologijų, kuria galima išpildyti funkcinę dalį, vadinama technologijos variantu.
- **Technologinio sprendimo alternatyva** – technologinio sprendimo alternatyva vadinamas sprendinys, kuris sujungia koncepciją (sprendžiamas problemas), funkcines dalis ir technologijas (funkcinių dalių išpildymo) variantus. Atsižvelgiant į tai, kad technologinis sprendimas ateityje (po pirmosios versijos išpildymo) gali būti tobulinamas ir toliau vystomas, kiekvienos technologinio sprendimo alternatyvos atveju yra numatomos galimos papildomos funkcinės dalys.

Prieš tai aprašyti konceptai yra sudaromi tokiais būdais:

- Galimos koncepcijos (sprendžiamos problemos) sudaromos atsižvelgiant į **nustatytas problemas**, pagal tai, kaip **egzistuojantys arba galimi sprendiniai sprendžia tokias arba panašias problemas**. Problemos ir galimi jų sprendimai (ekspertu vertinimu) nustatomi atliekant ekspertinių nuomonių analizę. Jos metu ekspertų išsakytos problemos ir galimi sprendimai yra grupuojami, sujungiami į problemų priežasčių–sprendimų (intervencijos logikos) schemas. Skirtingos intervencijų logikos yra formuluojamos į skirtingas koncepcijas. Koncepcijos yra validuojamos jas palyginant su egzistuojančių sprendimų koncepcijomis.
- Funkcinės dalys yra nustatomos atsižvelgiant į **elementų, būtinų koncepcijos išpildymui, analizę**. Atliekant koncepcijų elementų analizę yra nustatomos funkciškai atskiros, tiesiogiai nesusietos koncepcijų dalys. Jeigu skirtingų koncepcijų išpildymui reikalingos identiškos funkcinės dalys, jos yra sujungiamos.
- Technologijos (funkcinių dalių išpildymo) variantai yra nustatomi remiantis **egzistuojančių sprendimų taikomų technologijų analize** ir **ekspertiniu interviu medžiagos analize**.
- Technologinio sprendimo alternatyvos sudaromos, atsižvelgiant į logiškai galimas koncepcijų išpildymo alternatyvas (koncepcijų, funkcinių dalių, technologijos variantų kombinacijos).

Toliau pateiktame paveiksle pateikiama studijos I etapo metodiką vizualizuojanti schema.



7 paveikslas. Studijos I etapo metodiką vizualizuojanti schema
Šaltinis: sudaryta Konsultanto

Sudarytomis alternatyvoms yra sudaromi galimo **vystymo aprašymai**. Tokiuose aprašymuose išskiriamos nebūtinai alternatyvos įgyvendinimui funkcinės dalys, kurios galėtų būti diegiamos ateityje, nustatant, kad įgyvendintas sprendimas veiksmingai įgyvendina sprendimo koncepciją. Vystymo aprašymai sudaromi atsižvelgiant į kitų alternatyvų funkcinių dalių pritaikymo alternatyvai analize. Į alternatyvos vystymo aprašymą įtraukiamos tos kitų alternatyvų funkcinės dalys, kurios galėtų būti pritaikomos alternatyvos koncepcijai.

Sudarytos alternatyvos yra lyginamos pagal išskeltus kriterijus. Yra keliami tokie lyginimo kriterijai:

- **Sudėtingumas, rizikos dėl negebėjimo technologiškai išpildyti** – nustatomas technologinio išpildymo naujumo / inovatyvumo lygis. Vertinimas sudaromas pritaikant vieną iš šių charakteristikų: a) „Nesudėtingas“ – vertinimas priskiriamas alternatyvoms, kurios įgyvendinimui taikomi plačiai paplitusios technologijos; b) „Sudėtingas“ – vertinimas priskiriamas alternatyvoms, kuriuose reikia taikyti technologijas, kurios nėra plačiai taikomos, reikalauja retų ir pažangių IRT srities specialistų kompetencijų; c) „Inovatyvus“ – vertinimas priskiriamas alternatyvoms, kurių įgyvendinimas reikalautų pažangių technologijų pritaikymo, t. y. nėra randama bent vienos iš nagrinėjamų technologijų pritaikymo panašiai koncepcijai išpildyti.
- **Pradinės investicijos** – remiantis prienamomis rinkos kainomis yra nustatomas santykinis pradinių investicijų dydis. Investicijų dydis nurodomas nominaliais orientaciniais dydžiais, palankesnis vertinimas priskiriamas alternatyvoms, pasižyminčioms mažesnėmis sąnaudomis.
- **Palaikymo sudėtingumas, palaikymo išlaidos** – vertinimas priskiriamas atsižvelgiant į 2 komponentus – tikėtinos sąsajų su išorinėmis sistemomis palaikymo sąnaudos ir tikėtinos žmogiškųjų išteklių sąnaudos. Palankesnis vertinimas priskiriamas alternatyvoms, pasižyminčioms mažesnėmis palaikymo sąnaudomis.
- **Vartotojo patirtis** – vertinimas priskiriamas atsižvelgiant į tikėtiną naudotojų patirtį naudojantis alternatyvos technologiniu sprendiniu. Atsižvelgiant į tai, kad skirtingos alternatyvos gali reikšmingai skirtis, kiekvienos alternatyvos atveju yra atliekamas atskiras vertinimas, pagrindžiantis nustatomą vertinimą.

Priklausomai nuo sudarytų alternatyvų specifikos gali būti taikomi papildomi kriterijai.

2.2. Technologinių sprendimų pritaikymas užsienio šalyse

Toliau skyriuje kaip gerųjų praktikų pavyzdžiai pateikiamos užsienio šalyse jau įgyvendintų technologinių sprendimų versijos. Toliau apibendrinamos funkcijos, nustatytos atliekant užsienio šalių analizę.

3 lentelė. Funkcijų pavadinimai, veikimo principas, bei skiriamas ženklas tekste

| Eil. nr. | Funkcijos sutrumpinimas - pavadinimas | Funkcija | Skiriamasis ženklas |
|----------|---|--|---------------------------|
| 1. | Nustatymo arba atpažinimo funkcija | Gebėjimas atpažinti bei nustatyti nelegalų turinį internete arba iš anksto talpinti savo duomenų bazėje / turėti sąsają su nelegalaus turinio svetainių duomenų baze ir, remiantis šia informacija, atpažinti nelegalų turinį. | Spalva – žalia. |
| 2. | Pranešimo funkcija | Funkcijos tikslas gebėti informuoti klientą / programos naudotoją, jog pastarasis pateko į nelegalaus turinio svetainę. Ši funkcija gali būti įgyvendinama iššokančio tipo pranešimu naršyklėje arba atidarius nelegalaus turinio svetainę | Spalva – mėlyna. |
| 3. | Legalaus turinio alternatyvų pasiūlymas | Atpažinęs ir informavęs naudotoją apie tai, jog jis bando nelegaliai pasiekti turinį, įrankis naudotojui galėtų pasiūlyti legalaus turinio svetainių sąrašą (tam reikėtų gauti tiekėjų, kurie sutiktų prisidėti prie šios alternatyvos ir įtraukti savo organizacijos vardą į legalių svetainių sąrašą, sutikimą). | Spalva – tamsiai geltona. |
| 4. | Blokavimo funkcija | Institucijos arba įrankiai, turintys teisinį mandatą blokuoti nelegalų turinį platinančias / talpinančias svetaines. | Spalva – raudona. |
| 5. | Vartotojų savarankiškas pranešimo atsakingoms institucijoms | Suteikiama teisė interneto naudotojams pastebėjus nelegalų turinį internete pranešti institucijoms. Ši funkcija siekia įtraukti naudotojus į pranešimo procesą pastebėjus nelegalų turinį internete | Spalva – oranžinė |

Šaltinis: parengta Konsultanto

Atsižvelgiant į tai, kad dalis galimų technologijų nėra naudojamos panašiais atvejais, pirmiausiai yra aprašomi konkretūs veikiančios sprendimai, toliau nagrinėjami ne veikiančios sprendimai, tačiau technologijos.

2.2.1. Veikiančių technologinių sprendimų pavyzdžiai

Šiame skyriuje nagrinėjami veikiančios technologiniai sprendimai, kurie dalinai ar pilnai gali būti naudingi kuriant technologinį sprendimą.

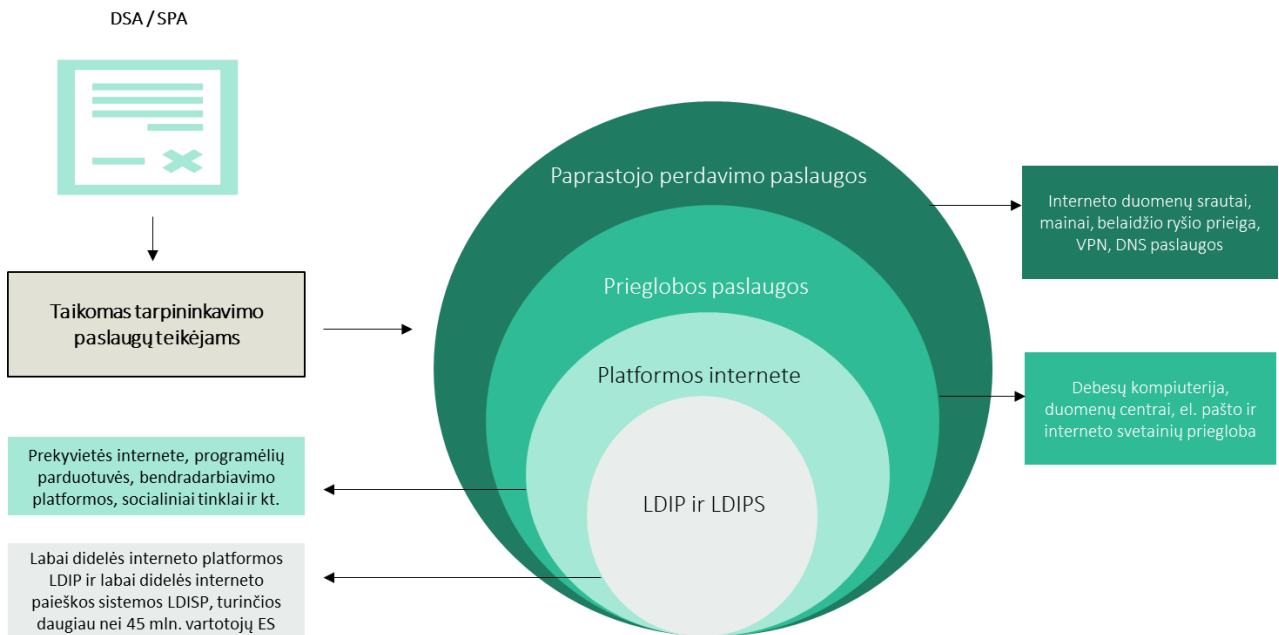
SKAITMENINIŲ PASLAUGŲ AKTO SISTEMA

Naudinga kalbant apie: naudotojų savarankišką raportavimą tarnyboms; blokavimo funkciją

Skaitmeninių paslaugų aktas (toliau – SPA) sukurtas 2022 metais Europos Komisijos siekiant saugoti naudotojus ir jų pagrindines teises internete, nustatant aiškias ir proporcingas taisykles. SPA skatinamos inovacijos, augimas ir konkurencingumas, sudaromos palankesnės sąlygos mažesnių platformų, mažų ir vidutinių įmonių (toliau – MVĮ) ir pradedančiųjų įmonių plėtrai. SPA reguliuoja interneto tarpininkus ir platformas, pavyzdžiui, prekyvietes, socialinius tinklus, dalijimosi turiniu platformas, programėlių parduotuves, internetines kelionių ir apgyvendinimo platformas. Pagrindinis jos tikslas – užkirsti kelią neteisėtai ir žalingai veiklai internete ir dezinformacijos sklaidai.³¹ SPA veikimo principas yra toks, jog naudotojai internete bei tam tikros įpareigtos institucijos „patikimi pranešėjai“ (angl. *trusted flaggers* toliau – patikimi pranešėjai) susidūrę su nelegaliu, nepagarbiu bei pavojingu turiniu internete gali paprastai informuoti apie jas talpinančias svetaines. Pagal SPA patikimi pranešėjai yra atsakingi už galimai neteisėto turinio aptikimą ir įspėja interneto platformas. Juos skiria nacionaliniai skaitmeninių paslaugų koordinatoriai. Jų pateiktiems pranešimams turi būti teikiama pirmenybė, nes tikimasi, kad jie bus tikslesni nei vidutinio naudotojo pateikti pranešimai.³²

³¹ European Commission, The Digital Service Act. Prieiga internetu: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en

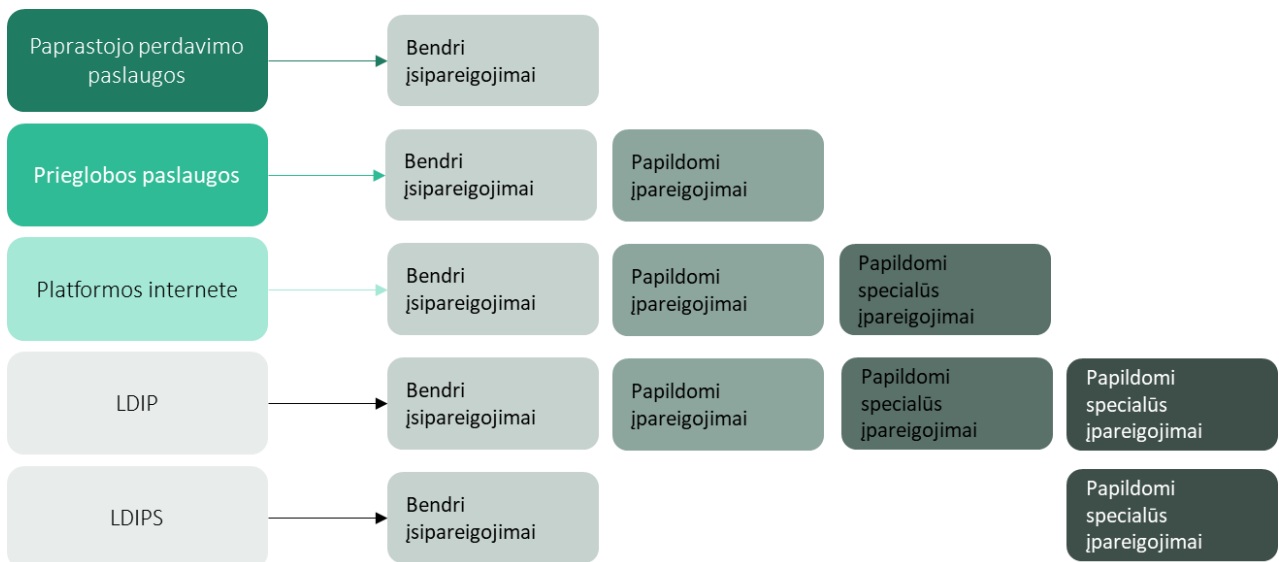
³² European Commission, „Trusted flaggers under the Digital Services Act (DSA)“, 2025. Prieiga internete: <https://digital-strategy.ec.europa.eu/en/policies/trusted-flaggers-under-dsa>



8 paveikslas. Skaitmeninių paslaugų akto taikymo gairės, 2024 m.

Šaltinis: sudaryta Konsultanto remiantis SPA aktu³³

SPA numatyta daugiapakopė įpareigojimų tarpininkavimo paslaugų teikėjams sistema. Tai reiškia, kad be bendrųjų įpareigojimų, taikomų visoms tarpininkavimo paslaugoms, tam tikrų tipų tarpininkavimo paslaugoms taikomi ir papildomi ar specialūs įpareigojimai. Pavyzdžiui, prieglobos (angl. *hosting*) paslaugų teikėjams taikoma daugiau įpareigojimų nei paprastojo perdavimo paslaugų teikėjams; prieglobos paslaugų kategorijos įpareigojimai taikomi interneto platformų paslaugų teikėjams ir t.t. Pakopinė SPA įpareigojimų sistema pateikta toliau schemos pavidalu:



9 paveikslas. Skaitmeninių paslaugų akto taikymo gairės, 2024 m.

Šaltinis: sudaryta Konsultanto remiantis SPA aktu³⁴

Pagal įsipareigojimų nustatytus reikalavimus paslaugų teikėjai privalo kontroliuoti savo veiklą internetiniame puslapyje ar sistemoje.

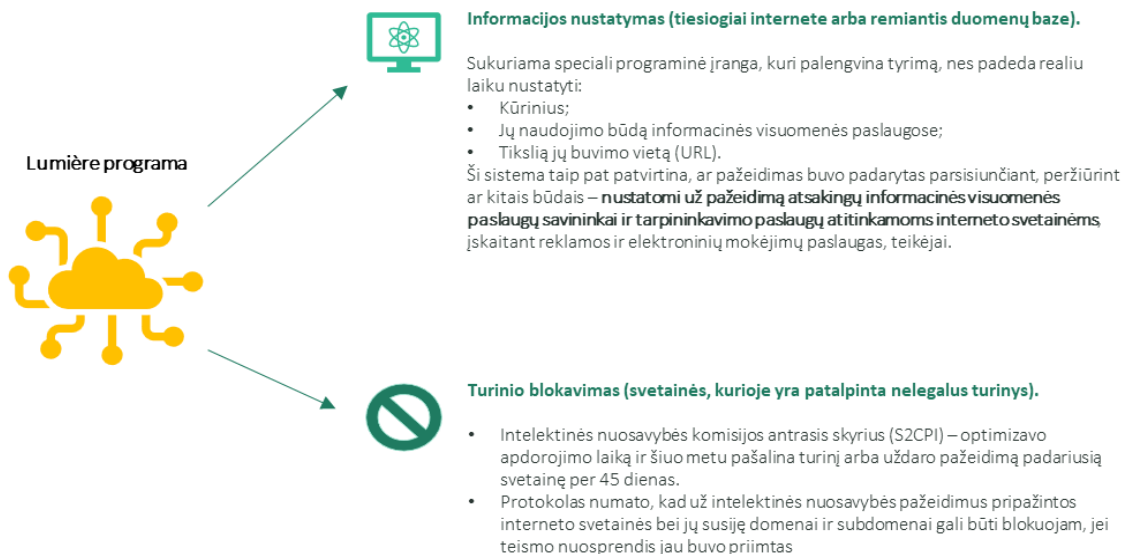
³³ Skaitmeninių paslaugų akto taikymo gairės, 2024 m. Prieiga internetu: file:///C:/Users/Mano/Desktop/OneDrive%20-%20Smart%20Continent/0386NEKU%20Nelegalaus%20turinio%20studija/Darbinis/04%20Saltiniai/SPA-taikymo-gaires-paslaugu-teikejams_2024.pdf

³⁴ Ten pat

LUMIÈRE ĮRANKIS. IŠPANIJOS ATVEJIS

Naudinga kalbant apie: **informacijos nustatymą**; **blokavimo funkciją**.

2022 m. spalio mėnesį Kultūros ir sporto ministerijos kartu su Ispanijos profesionalia futbolo lyga – „La Liga“ pasirašyta bendradarbiavimo susitarimas dėl „La Liga“ sukurtos programinės įrangos „Lumière“ naudojimo. Šio įrankio naudojimas padeda veiksmingiau tirti intelektinės nuosavybės teisių pažeidimus bei optimizuoti jų vykdymo užtikrinimo procesus. Įranga palengvina tyrimą, nes padeda nustatyti kūrinius, jų naudojimo būdą informacinės visuomenės paslaugose ir tikslią jų buvimo vietą (URL adresą). Ji taip pat patvirtina, ar pažeidimas buvo padarytas turinį parsisiunčiant, peržiūrint ar kitais būdais – nustatomi už pažeidimą atsakingų informacinių paslaugų savininkai ir tarpininkavimo paslaugų atitinkamoms interneto svetainėms, įskaitant reklamos ir elektroninių mokėjimų paslaugas, teikėjai.



SSKT – skaitmeninis ir suskaitmenintas kultūros turinys

10 paveikslas. „Lumière“ programos veikimo principas

Šaltinis: sudaryta Konsultanto remiantis World intellectual property organization 2022 m.³⁵

„Lumière“ sudaro sąlygas veiksmingiau valdyti procedūrų vykdymo užtikrinimo procesus, nes sumažina laiko, išteklių ir reikalingų resursų kiekį, todėl naudojant „Lumière“ turinio pašalinimas arba interneto svetainės uždarymas dabar užtrunka 45 dienas.

„GOOGLE SAFE BROWSING“ NARŠYKLĖ („GOOGLE“ SAUGAUS NARŠYMO SISTEMA)

Naudinga kalbant apie: **informacijos nustatymą**; **pranešimą**.

Google saugioji naršyklė kasdien padeda apsaugoti daugiau kaip penkis milijardus prietaisų, rodydama naudotojams įspėjimus, kai jie bando naršyti pavojingose svetainėse arba atsisiųsti pavojingus failus. Saugi naršyklė taip pat praneša svetainių valdytojams, kai jų svetainėse veikia kenkėjai, ir padeda diagnozuoti bei išspręsti šią problemą, kad svetainių lankytojai naršytų saugiau. Saugaus naršymo apsaugos priemonės veikia visuose Google produktuose ir užtikrina saugesnį naršymą visame internete.³⁶ Google naudotojams yra pritaikoma saugaus naršymo technologija, kurioje įdiegta naršyklė, padedanti patikrinti internetinių svetainių

³⁵ WIPO, „National initiatives to address online ip infringements. Contributions prepared by the Republic of Korea and Spain“, 2022 m. Prieiga internetu: https://www.wipo.int/edocs/mdocs/enforcement/en/wipo_ace_15/wipo_ace_15_5.pdf.

³⁶ Google safe browsing. Prieiga internete: <https://safebrowsing.google.com/>

būseną pagal URL adresą. Aptikus nesaugią svetainę, rodomas pranešimas, įspėjantis naudotoją apie nesaugų turinį.³⁷

„Google Safe Browsing“ sustiprintos apsaugos režimas naudojami iš anksto sukurta duomenų baze, patikromis realiu laiku bei pasitelkiant DI pagalbą, klasifikuojant kenkėjiškus URL adresus ir tinklalapius. Toliau pateikiama detalesnė mechanizmo veikimo informacija. Remiantis „Chrome enterprise“³⁸ „Google Safe Browsing“ sistema atnaujina savo kenkėjiškų / kenksmingo turinio svetainių sąrašą kas 30 minučių naudodama naujai aptiktas kenkėjiškas programas ir sukčiavimo svetaines. Tai įgyvendinama pasitelkiant maišos (angl. *hash*) pagrindu atliktus patikrinimus. „Google Safe Browsing“ prieš tai minėtas sąrašas nelaiko visų nesaugių interneto adresų (URL) – tai būtų pernelyg brangu ir užimtų per daug įrenginio atminties. Vietoje to, URL, kuris gali būti labai ilgas, yra paverčiamas į unikalų, fiksuoto dydžio simbolių rinkinį naudojant kriptografinę maišos funkciją (SHA-256). Šis unikalus fiksuoto dydžio simbolių rinkinys ir leidžia sąrašą saugoti efektyviai net ir ribotoje atmintyje.³⁹ Todėl, kai administratorius arba galutinis saugios naršyklės naudotojas įgalina / instaliuoja patobulintą „Google Safe Browsing“ versiją, „Chrome“ naršyklė realiuoju laiku tikrina kiekvieną tinklaraštį. Be to, šioje naršyklėje saugomas svetainių, kurios yra žinomos kaip saugios, sąrašas, jis taip pat yra naudojamas tikrinant svetainių patikimumą.

Nesaugios / kenkėjiškos svetainės prisitaikė – šiandien dauguma jų veikia trumpiau nei 10 minučių. Tai reiškia, kad iki tol, kol vietiniame įrenginyje atnaujinamas žinomų nesaugių svetainių sąrašas, daugelis jų jau spėja pasinaudoti proga ir padaryti žalos, jei naudotojai tuo metu apsilanko tokiose svetainėse. Be to, „Google Safe Browsing“ kenksmingų svetainių sąrašas sparčiai auga. Ne visi įrenginiai turi pakankamai resursų šiam augančiam sąrašui palaikyti, taip pat ne visada gali gauti ir taikyti naujinius tokiu dažniu, kuris būtinas visapusei apsaugai užtikrinti. „Google Safe Browsing“ patobulintoje apsaugos veiksenoje – „Enhanced Safe Browsing“⁴⁰ jau dabar naudojamos technologijos, padedančios užbėgti tokioms grėsmėms už akių – tai tikrinimas pagal sąrašus realiu laiku ir DI pagrįsta kenksmingų URL bei tinklalapių klasifikacija. Ši tikrinimo realiuoju laiku galimybė apsaugo nuo veidrodinių kenkėjiškų programų, kurių organizatoriai kas keletą minučių kuria naujus tinklaraščių adresus (angl. URL). Šis sustiprintos apsaugos režimas buvo sukurtas kaip pasirenkamoji funkcija, leidžianti naudotojams nuspręsti, ar dalintis daugiau su saugumu susijusiais duomenimis mainais į stipresnę apsaugą. Ši apsaugos forma įrodė, kad tikrinimas realiu laiku suteikia reikšmingos naudos, todėl nuspręsta ją pritaikyti ir standartiniame apsaugos režime naudojant naują API versiją – tokia, kuri nesidalija naudotojų lankomų svetainių URL su „Google“.⁴¹ Ši funkcija, dalindamasi duomenimis realiuoju laiku su „Google Safe Browsing“, gali aktyviai apsaugoti naudotojus nuo pavojingų svetainių. Jei naudotojas yra prisijungęs prie savo „Chrome“ ir kitų „Google“ naudojamų programų („Gmail“, „Drive“ ir kt.) paskyros, tai leidžia užtikrinti geresnę apsaugą visose „Chrome“ programų paskyrose su kuriomis susiduriama internete. Kitaip tariant, „Enhanced Safe Browsing“ į naršyklę tiesiogiai perkelia pažangiausias „Google“ saugumo priemonių žinias.

Saugus naršymas taip pat apsaugo naudotojus nuo piktnaudžiavimo plėtiniais ir kenkėjiška programine įranga. „Chrome“ nuskaito naršyklėje įdiegtus plėtinius ir lygina juos su kenkėjiškais / piktnaudžiaujančiais plėtiniais, įtrauktais į „Google safe browsing“ sąrašą. Jei šie sutampa, „Chrome“ išjungia plėtinį, informuoja naudotoją ir kartais pateikia parinkčių, kaip pašalinti arba vėl įjungti plėtinį.⁴²

Panašiu metodu „Google safe browsing“ veikia ir su į kompiuterinę sistemą atsiųstais failais iš „Chrome“ naršyklės. Kai failas yra atsiunčiamas, naršyklė patikrina jį pagal potencialiai pavojingų failų tipų, pvz., vykdomųjų failų ir

³⁷ Google saugaus naršymo svetainių būseną. Prieiga internetu: <https://transparencyreport.google.com/safe-browsing/search>

³⁸ Chrome enterprise, The Browser is the New Frontline Defense for Endpoint Security, „How Chrome browser can play a central role in your enterprise security strategy“. Prieiga internetu: <https://services.google.com/fh/files/misc/chromebrowsersecuritylayerpaper.pdf>

³⁹ Google security blog, Jasika Bawa et al., „Real-time, privacy-preserving URL protection“, 2024 m. Prieiga internetu: <https://security.googleblog.com/2024/03/blog-post.html>

⁴⁰ Google chrome žinynas, „Kaip „Chrome“ saugaus naršymo funkcija užtikrina jūsų naršymo duomenų privatumą“. Prieiga internetu: <https://support.google.com/chrome/answer/13844634?hl=lt&zipy=%2Ckaip-veikia-saugaus-nar%C5%A1ymo-funkcija>

⁴¹ Google security blog, Jasika Bawa et al., „Real-time, privacy-preserving URL protection“, 2024 m. Prieiga internetu: <https://security.googleblog.com/2024/03/blog-post.html>

⁴² Chrome enterprise, The Browser is the New Frontline Defense for Endpoint Security, „How Chrome browser can play a central role in your enterprise security strategy“. Prieiga internetu: <https://services.google.com/fh/files/misc/chromebrowsersecuritylayerpaper.pdf>

dažniausiai naudojamų dokumentų tipų, sąrašą. Jei failo saugumo patikrinti neįmanoma, „Chrome“ siunčia informaciją į „Google“ serverius ir nustato, ar failas yra saugus. Jei atsakymas yra neigiamas, naudotojui rodomas įspėjimas. Galima šią „Google safe browsing“ naršyklę dar labiau patobulinti įgalinus funkciją – „Enhanced Safe Browsing“ (patobulintas saugus naršymas), tuomet apsauga nuo pavojingų svetainių ir atsisiuntimų gerokai padidėja.

Apibendrinant, kiekvieną kartą, kai naudotojas bando pereiti į „Google Safe browsing“ pavojingų svetainių sąrašą esantį tinklalapij, „Chrome“ naršyklė parodo įspėjimą su rizikos paaiškinimu ir mygtuku, kuriuo naudotojas grąžinamas į saugų tinklalapį. 2019 m. duomenimis „Chrome“ pateikė daugiau nei milijardą tokių įspėjimų. Šis įrankis yra skirtas aptikti kenkėjiškas, virusais apkrėstas svetaines⁴³:

- Tikrinamos svetainės pagal jų URL adresus, kurie toliau yra lyginami su „Google Safe browsing“ sistemoje esančiomis kenkėjiškų svetainių URL;
- Nuolatos (kas 30–60 minučių) atnaujinami kenkėjiškų svetainių URL „Google Safe browsing“ sistemos sąrašai;
- Tikrinamos ne tik elektroninės svetainės, bet ir į instaliavimą kompiuterinėje sistemoje orientuoti dokumentai lyginant juos su potencialiai pavojingų failų tipų sąrašu;
- Informuoja naudotoją dėl atitinkamai potencialių pavojų turinčių svetainių ir parsisiunčiamų duomenų išsiunčiant įspėjimą žinutę;
- „Enhanced Safe browsing“ technologijos, padedančios efektyviau tikrinti informaciją realiuoju laiku pagal turimus kenkėjiškų svetainių sąrašus ir dirbtiniu intelektu pagrįstą kenksmingų URL bei tinklalapių klasifikaciją. Šiame procese naudojama papildoma informacija, kad būtų galima signalizuoti konkretesnę įspėjimą. Šis metodas apima pavojingų svetainių, atsisiuntimų ir nepatikimų plėtinių analizę.⁴⁴

EOL ĮRANKIS. PRANCŪZIJS ATVEJIS

Naudinga kalbant apie: **informacijos nustatymą; pranešimą; legalaus turinio alternatyvų pasiūlymas**

2022 m. sausio 1 d. Prancūzijoje įsigaliojo naujas – griežtesnis nei prieš tai galiojęs autorines teises ginantis įstatymas⁴⁵. Šiuo įstatymu įsteigta nauja Arcom institucija – ji nepriklausoma Prancūzijos valdžios institucija. Ji yra atsakinga už garsinį, vaizdo turinį bei šio tipo turinio platinimo teises. Ypatingas dėmesys šalyje skiriamas kovai su piratavimu ir neteisėtomis veidrodinėmis svetainėmis. Veidrodinės svetainės yra nelegalių svetainių, kurios jau yra užblokuotos tam paskirtų institucijų nuosprendžiu, antrininkės. Jos paprastai skleidžia tą patį turinį, tačiau naudoja skirtingus adresus, todėl jas sunku blokuoti.

Arcom buvo pavesta sudaryti juodąjį svetainių, kurios pažeidžia autorių teises, sąrašą. Įstatymas taip pat numato autorių teisių turėtojų veidrodinių svetainių blokavimo mechanizmą, grindžiamą modeli, kuris jau taikomas neapykantą kurstantį turinį talpinančioms svetainėms. Autorių teisių turėtojų prašymu Arcom turi įgaliojimą prašyti blokuoti svetaines, kuriose visiškai arba iš dalies atgaminamas svetainių, dėl kurių jau priimtas teismo sprendimas uždrausti svetainės veiklą, turinys. Garso ir vaizdo kūrinių naudojimo sporto renginiuose teisių turėtojai dabar gali inicijuoti laikinąsias apsaugos priemones, jei srautinio duomenų siuntimo svetainės šurkščiai ir pakartotinai pažeidžia jų teises. Teismas turės teisę nurodyti užblokuoti arba panaikinti nuorodas į tokias svetaines atitinkamų sporto varžybų laikotarpiu ne ilgiau kaip dvylikai mėnesių. Autorių teisių turėtojų prašymu Arcom gali taikyti blokavimo priemones ir veidrodinėms svetainėms, kurios nurodymo priėmimo metu dar nebuvo nustatytos. Tai apima ir automatizuotas sistemas, skirtas stebėti interneto srautą, identifikuoti pažeidimus ir imtis atitinkamų veiksmų prieš pažeidėjus.

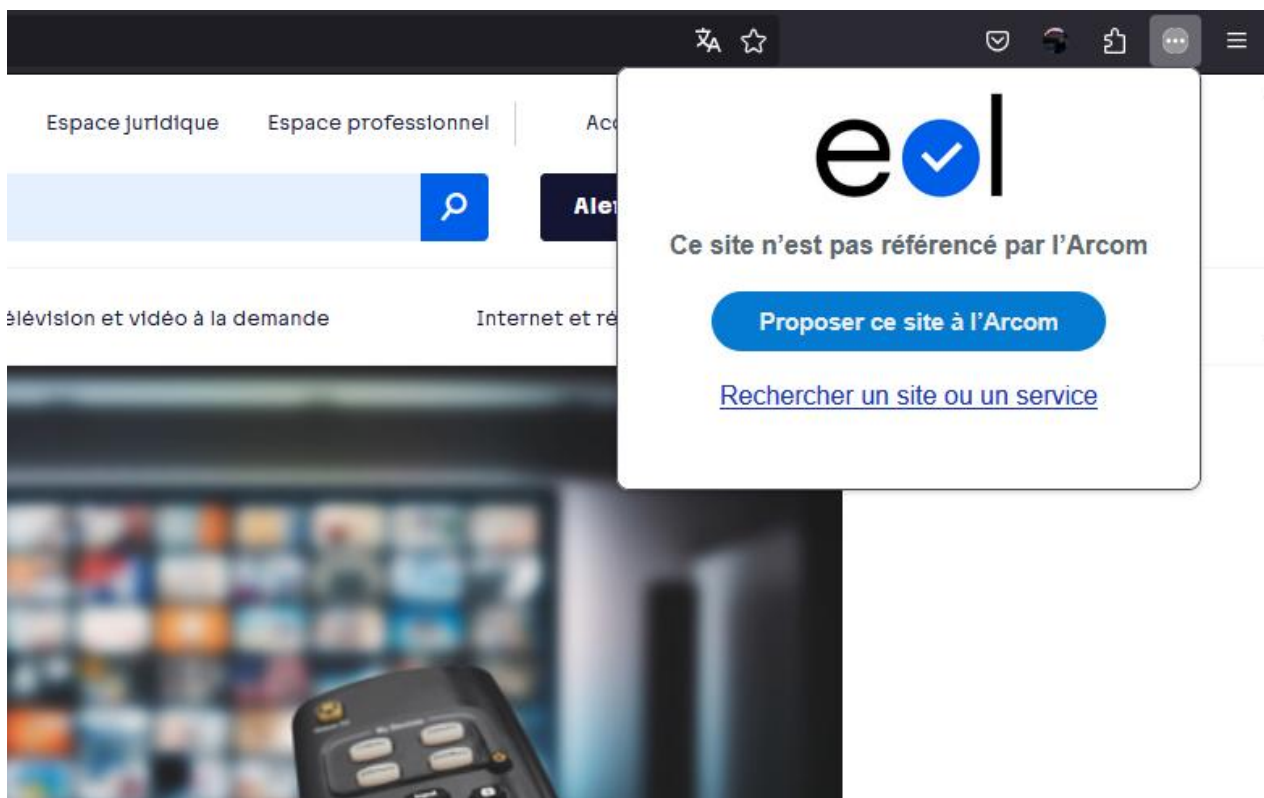
Prancūzija taip pat yra vienintelė valstybė, kurioje veikia Kuriamo technologinio sprendimo koncepciją pilnai atitinkantis įrankis – EOL įskiepis. Naudojant EOL įskiepį naršymo metu galima sužinoti, ar svetainėje dominuoja legalus ar nelegalus turinys. EOL taip pat atitinka Bendrojo duomenų apsaugos reglamento (toliau – BDAR) reikalavimus, kadangi neįrašo ir nesiunčia jokių savo naudotojų naršymo duomenų Arcom ar trečiosioms šalims.

⁴³ Google security blog, Jasika Bawa et al., „Real-time, privacy-preserving URL protection“, 2024 m. Prieiga internetu: <https://security.googleblog.com/2024/03/blog-post.html>

⁴⁴ Google chrome žinynas, „Kaip „Chrome“ saugaus naršymo funkcija užtikrina jūsų naršymo duomenų privatumą“. Prieiga internetu: <https://support.google.com/chrome/answer/13844634?hl=lt#zippy=%2Ckaip-veikia-saugaus-nar%C5%A1ymo-funkcija>

⁴⁵ ARCOM, Prieiga internetu: <https://www.arcom.fr/espace-juridique>

Jis tik lygina URL su autorių teises atitinkančių svetainių, nurodytų Arcom sąrašu. Šį technologinį įrankį galima parsisiųsti į „Google Chrome“, „Microsoft Store“, „Mozilla Firefox“ naršyklės (tik kompiuteriams).⁴⁶



11 paveikslas. EOL įskiepis, įdiegtas Mozilla Firefox naršyklėje
Šaltinis: Konsultanto atlikta ekrano nuotrauka

Atsiliepimų apie šio įrenginio veikimo efektyvumą viešoje internetinėje erdvėje nėra rasta, tikėtina, dėl to, kad įrenginys yra gana naujas ir dar nėra masiškai naudojamas. Įskiepio versiją Mozilla Firefox naršyklėje parsisiuntė vos 14 naudotojų. Pagrindinė įskiepio problema – mažas padengiamumo lygis – tai reiškia, kad dažniausiai įskiepis nežino, ar internetinė svetainė, kuriame apsilankyta, yra legali ar ne.

PLATFORMA JUSTWATCH

Naudinga kalbant apie: **legalaus turinio alternatyvų pasiūlymą.**

Lietuvos analogai: Naudok legaliai, kuriama E-kultūra platforma; Europoje: Agorateka.

„JustWatch“ platformos tikslas – padėti naudotojams greičiau surasti legalų audiovizualinį turinį, transliuojamą legaliose platformose. Naudojantis šia platforma nereikia atskirai tikrinti skirtingų turinio programų ir platformų, norint rasti pageidaujamą turinį.⁴⁷ „JustWatch“ platformoje pateikiamas turinys, kuris yra randamas, pavyzdžiui, „Netflix“, „Disney Plus“, „Hulu“ ir panašiose platformose. Svetainė galima naudotis bet kurioje naršyklėje ir išmaniojo telefono programėlėje, kurią palaiko „iOS“ ir „Android“ operacinės sistemos, taip pat „Fire TV“ įrenginiuose.⁴⁸ Ši svetainė yra tinkamas pavyzdys, kaip naudotojams, ieškantiems audiovizualinio turinio internete, efektyviai pasiūlyti legalų turinį ir sutrumpinti jo paieškos trukmę.

⁴⁶ARCOM, „Avec EOL, l’offre légale culturelle en un clin d’œil“. Prieiga internetu: https://www.arcom.fr/internet-et-reseaux-sociaux/avec-eol-loffre-legale-culturelle-en-un-clin-doeil?utm_source=chatgpt.com

⁴⁷ TechRadar, „What is JustWatch? The TV streaming service guide explained“, 2020. Prieiga internetu: <https://www.techradar.com/news/what-is-justwatch-the-tv-streaming-service-guide-explained>

⁴⁸ Ten pat

12 paveikslas. JustWatch paieškos rezultatas
Šaltinis: Konsultanto atlikta ekrano nuotrauka

Pažymėtina, kad JustWatch atsižvelgia į regioninius apribojimus, t.y. gali pasiūlyti šaltinį, kuris yra prieinamas konkrečiau naudotojo regione. Pagrindinis JustWatch trūkumas – svetainėje galima rasti tik filmų ir serialų peržiūrai skirtus legalius šaltinius. Kitų formatų kurinių paieškai reikėtų naudoti kitokias svetaines.

Panašaus pobūdžio paieškos platformos yra įgyvendintos ir Lietuvoje. **Naudoklegaliai.lt** yra nacionalinis portalas, leidžiantis surasti muziką, filmus ir TV laidas, elektronines knygas, vaizdo žaidimus ir sporto renginių legalias svetaines.⁴⁹ Portalas veikia Kultūros ministerijos Visuomenės informavimo ir autorių teisių politikos grupės iniciatyva, kurios tikslas – skatinti teisėtą produktų naudojimą, siekiant skatinti tiek kultūrinę įvairovę, tiek kūrybinių industrijų plėtrą.⁵⁰

⁴⁹ Naudok legaliai!. Prieiga internete: <https://naudoklegaliai.lt/lt/about>

⁵⁰ Ten pat

Naudok legaliai!

Atsigaivink legaliu turiniu

Lithuanian

A- A+

Pradžia Apie Teisėtos pasiūlos svetainės DUK Statistiniai duomenys Kontaktiniai duomenys

Paieška

Turinio tipas

- Muzika
- Televizija ir filmai
- E. knygos
- Vaizdo žaidimai
- Sporto renginiai

Formatus

- Browser/Cloud
- Catch up TV Video on demand
- Debesija
- Tiesiogiai į pulą
- Atsisiuntimas

15 Teisėtos pasiūlos svetainės

Rūšiuoti pagal

Abėcėlės tvarka

Jango Muzika

Review & Daugiau informacijos

Junorecords Muzika

Review & Daugiau informacijos

13 paveikslas. Naudoklegaliai.lt paieškos rezultatas
Šaltinis: Konsultanto atlikta ekrano nuotrauka

Pagrindinis svetainės trūkumas – nėra galimybės surasti konkretaus turinio vieneto legalų šaltinį. Pateikiamas tik pagal skirtingas kategorijas sugrupuotas legalių šaltinių sąrašas. Nors taip pat padeda, ypač naudotojams, kuriems sunku atskirti legalų ir nelegalų šaltinį, naudotojas turės arba pats pereiti per visus išvardintus šaltinius, arba paiešką pratęsti Google ar kituose paieškos įrankiuose. Pratęsus paiešką Google įrankyje, naudotojas vėl turės savarankiškai atskirti legalius ir nelegalius turinio šaltinius. Tai yra pagrindinė problema, kuri neleidžia svetainei tapti patogiu ir plačiai naudojamu įrankiu.

Papildomai, Lietuvoje yra kuriama „E–kultūros“ platforma – vieningas suskaitmeninto ir skaitmeninio kultūros turinio, elektroninių paslaugų ir turinio sklaidos portalas. Inicatyva pradėta siekiant didinti kultūros prieinamumą ir pakartotinį naudojimą, sukuriant bendrą kultūros įstaigų skaitmeninių duomenų platformą, diegiant integralius organizacinius ir technologinius sprendimus. Pagrindinė „E–kultūros“ portalo kūrimo priežastis – žemas kultūros skaitmenizacijos lygis ir nepakankamas ar nepatrauklus skaitmeninio / skaitmeninto kultūros turinio prieinamumas. Projektas turėtų būti baigtas įgyvendinti 2026 m. balandžio mėnesį.⁵¹

OXYLABS SPRENDIMAI

Naudinga kalbant apie: [informacijos nustatymą](#).

Lietuvos rinkoje jau yra sėkmingai veikiantis IT įrankis, kuris pasitelkdamas DI technologijos pagalbą siekia aptikti žalingą turinį internete. Tai yra „Oxylabs“ įmonės sukurta unikali DI valdoma tinklapio duomenų kopijavimo (angl. „web scraping“) priemonė.⁵² „Oxylabs“ yra viena iš lyderiaujančių interneto duomenų rinkimo platformų pasaulyje. Įmonių grupė padeda verslui spręsti pagrindinius viešųjų duomenų rinkimo iššūkius. Tarp jos klientų –

⁵¹Lietuvos nacionalinė Martyno Mažvydo biblioteka, „E–kultūros“ platforma. Prieiga internetu: <https://www.lnb.lt/projektai/programos-ir-projektai/elektronines-paslaugos/ekultura-platforma-vieningas-suskaitmeninto-ir-skaitmeninio-kulturos-ir-audiovizualinio-turinio-elektroniniu-paslaugu-ir-sklaidos-portalas>

⁵² AiThORITY, AI Technology insights, AiT analyst, „Now, An AI-Driven Tool to Make Internet Safe by Detecting Illegal Online Content“, 2022 m. Prieiga internetu: <https://aithority.com/machine-learning/ai-driven-tool-to-make-internet-safe-by-detecting-illegal-online-content/>

daugiau nei 2 000 įmonių, įskaitant kelias dešimtis į „*Fortune Global 500*“ sąrašą patenkančių didžiausių JAV kompanijų.⁵³

Tinklapių duomenų kopijavimas – tai procesas, kai naudojant DI iš svetainės yra išgaunamas turinys ir duomenys. Skirtingai nuo ekrano nuskaitymo, kai kopijuojami tik ekrane rodomi pikseliai, tinklapių duomenų kopijavimo metu išgaunamas pagrindinis HTML kodas, o kartu ir duomenų bazėje saugomi duomenys. Tada šis įrankis gali atkartoti visą svetainės turinį kitoje vietoje.⁵⁴

„*Oxylabs*“ bendradarbiauja kartu LR ryšių reguliavimo tarnyba (toliau – RRT) ir LRTK. RRT – nacionalinė institucija, reguliuojanti elektroninių ryšių, pašto ir geležinkelių rinkas pagal Europos Sąjungos direktyvas ir Lietuvos Respublikos įstatymus. Viena iš RRT misijų - apsaugoti internetą nuo neteisėto ar žalingo turinio.⁵⁵ „*Oxylabs*“ automatizuotas įrankis skenuoja Lietuvos IP adresų erdvę ir ieško potencialiai žalingų vaizdų. Tuomet įtartiną turinį vienetai perduodami į karštąją liniją, kad juos peržiūrėtų RRT specialistai. Šis „*Oxylabs*“ DI įrankis padeda RRT aptikti neteisėtą turinį, susijusį su vaikų seksualinio išnaudojimo medžiaga internete. Per pirmuosius jo naudojimo mėnesius buvo nustatyta 19 interneto svetainių, pažeidžiančių nacionalinius ar ES teisės aktus, užregistruota 11 skundų Žurnalistų etikos inspektoriumi, pateikti 8 pranešimai policijai ir pradėti 2 ikiteisminiai tyrimai.⁵⁶

Šis ir panašus įrankis gali būti naudojamas masiškai interneto erdvės skanavimui siekiant nustatyti įtarimų keliančias internetines svetaines. Visgi, kaip interviu pažymėjo LRTK atstovas, šis įrankis neišsprendžia visų problemų, nes žmogus vis tiek turi peržiūrėti rezultatus, nors ir palengvina žmonių darbą. Įrankis yra ypač naudingas svetainių kopijų paieškai, tačiau su naujų svetainių aptikimu gali būti problemų, nes nėra aiškių kriterijų, kurios taikant įrankis gali būti naudojamas paieškai.

TERAMIND

Naudinga kalbant apie: [informacijos nustatymą](#).

Teramind yra platforma, skirta naudotojų, įdiegusių Teramind programą, elgesio analizei, darbuotojų sekimui ir rizikos viduje mažinimui.⁵⁷ Programos tikslas yra vidinių grėsmių aptikimas, duomenų praradimo prevencija, produktyvumo analizė ir verslo procesų optimizavimas naudojant pažangią naudotojų elgsenos analizę. Toliau šiame skyriuje pateikiama informacija, kokių principu ši sistema veikia ir ar toks techninis modelis galėtų teigiamai pasitarnauti Technologinio sprendimo kūrime.

Teramind diegimui reikalingas Teramind agento įdiegimas – tai gali būti matoma (aktyvi) arba paslėpta (tyloji) versija. Teramind Agent (toliau – agentas) tai savarankiška Windows ir macOS programa, kuri fiksuoja naudotojo veiklą galutiniame įrenginyje (kompiuteryje) ir siunčia šią informaciją į Teramind serverį. Agentas siunčia surinktą informaciją į Teramind serverį, kuris apdoroja duomenis, parengia analizę bei vykdo kitas sistemos funkcijas. Be to, jis veikia kaip pagrindinė naudotojo sąsaja su serveriu – serverio nustatymai konfigūruojami Teramind valdymo skydeliu (angl. *Dashboard*, toliau – valdymo skydelis).⁵⁸ Naršyklėje veikiantis stebėsenos ir valdymo skydelis suteikia galimybę peržiūrėti, kas vyksta organizacijoje:

- Matyti stebėsenos ataskaitas;
- Analizuoti produktyvumą;

⁵³ Rekvizitai. Lt, Oxylabs, UAB, Įmonės aprašymas. Prieiga internetu: https://rekvizitai.vz.lt/imone/teso_lt/

⁵⁴ Imperva a Thales company, Web scraping. Prieiga internetu: <https://www.imperva.com/learn/application-security/web-scraping-attack/>

⁵⁵ AIThority, AI Technology insights, AiT analyst, „Now, An AI-Driven Tool to Make Internet Safe by Detecting Illegal Online Content“, 2022 m. Prieiga internetu: <https://aithority.com/machine-learning/ai-driven-tool-to-make-internet-safe-by-detecting-illegal-online-content/>

⁵⁶ AIThority, AI Technology insights, AiT analyst, „Now, An AI-Driven Tool to Make Internet Safe by Detecting Illegal Online Content“, 2022 m. Prieiga internetu: <https://aithority.com/machine-learning/ai-driven-tool-to-make-internet-safe-by-detecting-illegal-online-content/>

⁵⁷ Teramind, „How does Teramind work?“, 2024 m. Prieiga internetu: <https://kb.teramind.co/en/articles/8790894-how-does-teramind-work>

⁵⁸ Teramind, „How does Teramind work?“, 2024 m. Prieiga internetu: <https://kb.teramind.co/en/articles/8790894-how-does-teramind-work>

- Konfigūruoti naudotojų prieigas bei kurti taisykles, kurios automatiškai užkerta kelią saugumo incidentams;
- Aptikti elgsenos nukrypimus.

Taip pat šiame skydelyje galima valdyti visus agento nustatymus ir diegimo infrastruktūrą.

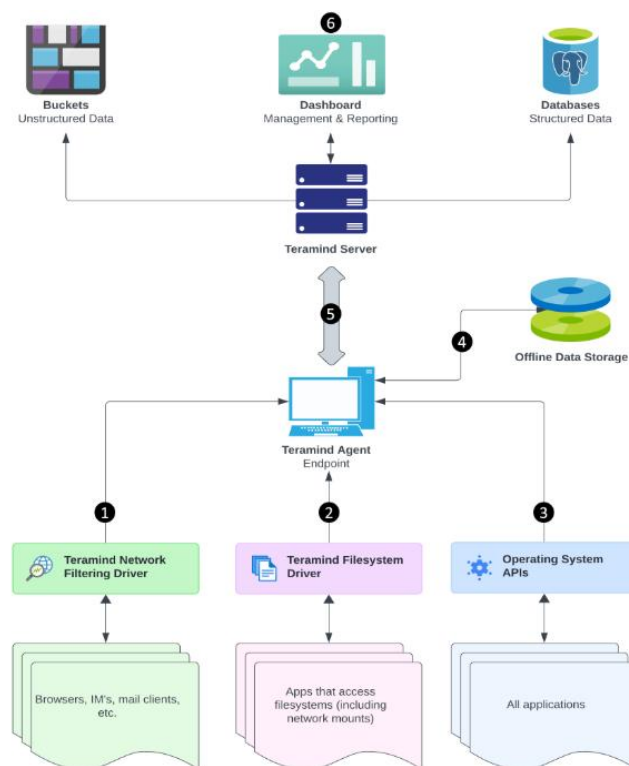
Naudodamas tinklo filtravimo tvarkyklę (angl. *proxy*), agentas gali analizuoti visą tinklo srautą galutiniame įrenginyje. Agentas aptinka aukšto lygio veiklas (pavyzdžiui, išsiųstus el. laiškus, aplankytus tinklalapius, momentinius pranešimus ir kt.), išgauna visą meta-informaciją iš pirminio tinklo srauto ir sukuria stebėsenos įvykius.

Naudodamas failų sistemos filtravimo tvarkyklę, agentas stebi ir analizuoja visas failų lygmens operacijas, vykstančias kompiuteryje. Agentas aptinka aukšto lygio veiklas (pavyzdžiui, failo sukūrimą, kopijavimą ir kt.), išgauna visus metaduomenis ir generuoja stebėsenos įvykius.

Taip pat agentas naudoja kitas operacinės sistemos API, kad galėtų stebėti programų elgseną ir naudotojų veiklą bei kurti stebėsenos įvykius. Operacinės sistemos API (programų programavimo sąsaja) – tai operacinės sistemos teikiamų funkcijų, protokolų ir priemonių rinkinys, leidžiantis programoms sąveikauti su operacine sistema ir naudotis jos paslaugomis.

Kai nėra tiesioginio ryšio su serveriu, agentas laikinai saugo sugeneruotus stebėsenos įvykius vidinėje atmintyje. Kai ryšys atkuriamas, agentas perskaito saugotus įvykius ir perduoda juos į serverį.

Agentas taip pat gauna konfigūraciją, stebėsenos nustatymus, elgsenos politiką ir taisykles iš serverio ir taiko juos galutiniame įrenginyje. Valdymo skydelis suteikia administratoriams ir privileijuotiems naudotojams galimybę konfigūruoti sistemą bei agento nustatymus, kurti elgsenos politikas ir taisykles bei peržiūrėti ataskaitas.⁵⁹



14 paveikslas. Teramind sistemos veikimo schema

Šaltinis: Konsultanto atlikta ekrano nuotrauka

⁵⁹ Teramind, „How does Teramind work?“, 2024 m. Prieiga internetu: <https://kb.teramind.co/en/articles/8790894-how-does-teramind-work>

Apibendrinant, nors šis įrankis sukurtas stebėti įmonių, įsigijusių šią programą, darbuotojų veiklą internetinėje erdvėje dėl skirtingų priežasčių, tačiau panašaus pobūdžio kompiuterinė sistema galėtų būti dedikuota naudotojo elgesio stebėsenai, nustatant ar yra siunčiamas / naudojamas nelegalus turinys.

Panašios programos yra ActivTrak ir Veriato.

Pagrindinis tokios sistemos trūkumas – naudotojas leidžia sistemos administratoriui stebėti iš esmės visą veiklą savo įrenginyje. Dėl šios priežasties abejotina, kad tokiu principu veikianti sistema galėtų būti praktiškai pritaikoma kovos su nelegaliu turiniu srityje.

2.2.2. DI integracijos galimybių analizė

Atsižvelgiant į TS reikalavimus siekti pasiūlyti pažangias technologijas taikančio kuriamo technologinio sprendimo koncepciją, šiame skyriuje aprašomi moksliniai straipsniai ir praktiniai pavyzdžiai, susiję su DI pritaikymu kovai su nelegaliu turiniu internete.

Jungtinių Tautų tarptautinio nusikalstamumo ir teisingumo tyrimų centro tinklaraštyje paskelbtas *Marek Grzegorzcyk* straipsnis „How AI is leading the fight against online child abuse“⁶⁰ teigia, jog DI pagrįsti įrankiai gali padėti efektyviau ir tiksliau nustatyti ir pašalinti seksualinės prievartos prieš vaikus medžiagą (toliau – PPVM) nei vien tik žmonės moderatoriai. Būtent technologijos, ypač DI, taip pat gali atlikti svarbų vaidmenį padedant siekti reguliavimo tikslų pažabojant žalingą interneto turinį. Pavyzdžiui, DI algoritmai gali analizuoti vaizdų ir vaizdo įrašų turinį ir pažymėti potencialiai žalingą medžiagą, kad ją galėtų toliau peržiūrėti moderatoriai žmonės (žiūrėti toliau *Vivian Lai et al.* tyrimas). Tai gali padėti sumažinti žmonių moderatorių darbo krūvį ir padidinti kenksmingo turinio aptikimo ir pašalinimo greitį. Be turinio moderavimo, DI taip pat gali padėti sekti ir nustatyti asmenis, dalyvaujančius platinant ir vartojant PPVM.⁶¹ Analizuodami elgsenos ir bendravimo internete modelius, DI algoritmai gali padėti nustatyti ir surasti asmenis, kurie gali būti susiję su žalingo turinio kūrimu ar platinimu. „AI for Safer Children“ (liet. DI Vaikų saugumui) iniciatyva siekiama padėti teisėsaugos institucijoms išnaudoti DI potencialą ir sukurti pasaulinį DI centrą „AI for Safer Children Global Hub“ (liet. – DI saugesniems vaikams pasaulinis centras) – unikalią centralizuotą ir saugią platformą teisėsaugos institucijoms.⁶²

Tyrime *Vivian Lai* ir kitų tyrimu „Human-AI Collaboration via Conditional Delegation: A Case Study of Content Moderation“⁶³ atkleidžiama prielaida, jog nepaisant įspūdingų rezultatų daugelyje lyginamųjų duomenų rinkinių, DI modeliai veikiantys be žmogaus įsikišimo vis dar gali daryti klaidų, ypač tarp duomenų, kurie nebuvo naudojami DI apmokymo metu (angl. *out-of-distribution*) pavyzdžių. Tokių duomenų pavyzdžiai yra duomenų taškai, kurie labai skiriasi nuo mokymo duomenų, naudotų DI modeliui kurti. Tai reiškia, kad DI modelis mokymo etape nebuvo susidūręs su panašiais pavyzdžiais, o tai gali sukelti netikėtų veikimo problemų, kai DI modelis bando klasifikuoti ar prognozuoti šiuos naujus pavyzdžius. Atviras klausimas išlieka, kaip vis dar netobuli DI modeliai gali būti veiksmingai naudojami bendradarbiaujant su žmonėmis.⁶⁴ Šiame tyrime siūloma alternatyva yra žmogaus ir DI bendradarbiavimas – sąlyginis delegavimas. Tyrimas rodo, kad sąlyginis delegavimas gali gerokai pagerinti DI modelių našumą atliekant turinio moderavimo užduotis. Tai metodas, kai žmogus ir DI bendradarbiauja, kad prieš

⁶⁰ UNICEF, Marek Grzegorzcyk, „New! How AI is leading the fight against online child abuse“, 2023 M. Prieiga internetu: <https://unicri.org/News/AI-for-Safer-Children-%20article-Emerging-Europe>

⁶¹ UNICEF, Marek Grzegorzcyk, „New! How AI is leading the fight against online child abuse“, 2023 M. Prieiga internetu: <https://unicri.org/News/AI-for-Safer-Children-%20article-Emerging-Europe>

⁶² UNICEF, Marek Grzegorzcyk, „New! How AI is leading the fight against online child abuse“, 2023 M. Prieiga internetu: <https://unicri.org/News/AI-for-Safer-Children-%20article-Emerging-Europe>

⁶³ Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems, Vivian Lai et al., „Human-AI Collaboration via Conditional Delegation: A Case Study of Content Moderation“, Association for Computing Machinery, NY, United States, article no. 54, p. 1-18, 2022. Prieiga internetu: <https://dl.acm.org/doi/10.1145/3491102.3501999>

⁶⁴ Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems, Vivian Lai et al., „Human-AI Collaboration via Conditional Delegation: A Case Study of Content Moderation“, Association for Computing Machinery, NY, United States, article no. 54, p. 1-18, 2022. Prieiga internetu: <https://dl.acm.org/doi/10.1145/3491102.3501999>

DI modelio diegimą nustatytų patikimus regionus, t.y., stipriausias DI veikimo vietas.⁶⁵ Patikimi regionai tyrime reiškia konkrečias DI modelio įvesties erdvės sritis, kuriose modelio prognozės laikomos patikimomis. Šios sritys nustatomos remiantis modelio veiklos rezultatais ir duomenų, pagal kuriuos sistema buvo apmokyta (angl. *in-distribution*), savybėmis. Patikimi regionai gali būti operacionalizuoti naudojant raktiniais žodžiais grindžiamų taisyklių rinkinį, pagal kurį veiktų galutinis DI modelis. Pastebėtina, kad užduotis žmonėms sukurti sąlyginio delegavimo taisykles yra šiek tiek panaši į tai, ką jau daro daugelis socialinės žiniasklaidos moderatorių, rašydami rankinio automatizavimo taisykles, kad susidorotų su didžiuliu komentarų kiekiu.⁶⁶ Apskritai, tyrimas rodo, kad sąlyginis delegavimas yra perspektyvus žmogaus ir DI bendradarbiavimo metodas, leidžiantis naudotojams išlaikyti DI sprendimų kontrolę, kartu panaudojant tiek žmogaus sprendimo, tiek DI gebėjimų privalumus. Kaip ir minėta prieš tai, kai DI modelis susiduria su duomenimis, kurie skiriasi nuo DI duomenų apmokymo priemonės (angl. *out-of-distribution* – metodas naudojamas, kaip DI apmokomas atskirti / apdoroti tam tikrus duomenis ir vėliau sugeba analizuoti tos pačios kilmės duomenis ir išlaiko nemažą tikslumą), našumas sumažėja, o sąlyginis delegavimas gali ne visiškai kompensuoti šį sumažėjimą.⁶⁷ Todėl ateityje reikia ištirti, kaip toliau optimizuoti šį bendradarbiavimą, ir sukurti geresnes turinio moderavimo priemones. Tačiau šį metodą – DI ir žmogaus bendradarbiavimą galima pritaikyti turinio moderavimo užduotims tuo pačiu ir nelegalaus turinio analizei internete.

Toliau straipsnio „*Artificial Intelligence as a Service for Immoral Content Detection and Eradication*“⁶⁸ autoriai pabrėžia, jog dėl padidėjusio aktyvumo internete (ypač COVID-19 pandemijos metu, kai dėl fizinių barjerų padažnėjo bendravimas internetu) kartu gerokai padaugėjo ir amoralaus / nelegalaus turinio. Tai kelia rimtų problemų naudotojams, nes šio tipo turinys apima priekabiavimą ir patyčias internete. Todėl šiame tyrime daugiausia dėmesio skiriama DI kaip paslaugos (AlaaS – DI agentas kaip paslauga) naudojimui amoralaus turinio aptikimui ir naikinimui, pabrėžiant jo pritaikomumą ir veiksmingumą optimizuojant rezultatus filtruojant didelius kiekius duomenų.

DI kaip paslaugos (toliau – AlaaS) funkcijos:

- **DI GALIMYBIŲ TEIKIMAS NAUDOJANT DEBESIJOS PASLAUGAS.** Tai leidžia organizacijoms naudoti DI priemones, nereikalaujant jų kurti pačioms, todėl jos tampa prieinamos ir ekonomiškai efektyvios įvairioms užduotims valdyti, įskaitant turinio moderavimą.
- **KLASIFIKACIJA IR ATPAŽINIMAS.** naudojant įvairius klasifikatorius, tokius kaip atraminių vektorių mašinos (SVM), sprendimų medžiai ir „*Naive Bayes*“, AlaaS padidina turinio aptikimo tikslumą. Šie klasifikatoriai gali suskirstyti turinį į skirtingus tipus, pavyzdžiui, amoralų, kibernetinių patyčių ar neutralų, o tai padeda geriau valdyti sąveiką internete.
- Aptariami mechanizmai apima **KOMPIUTERINIO MOKYMOŠI METODUS**, pavyzdžiui, atraminių vektorių mašinas ir sprendimų medžius, skirtus amoraliam turiniui socialinės žiniasklaidos platformose klasifikuoti ir valdyti.
- **SEMANTINĖ ANALIZĖ.** AlaaS gali atlikti nuotaikos / konteksto ir semantinę analizę, kuri padeda suprasti turinio kontekstą ir emocijų toną.
- **ANALIZĖ REALIU LAIKU.** Sistemos realiu laiku inicijuoja veiksmus tam tikrame laiko intervale. Socialinės žiniasklaidos turinys gaunamas iš įvairių šaltinių. Didžioji dalis dizaino yra pagrįsta išskaidytu sistemos išdėstymu. Debesis palaiko visa apimančią darbo vietų sąveiką įvairiuose regionuose, susietą per organizuotas topologijas, ir užtikrina duomenų perdavimą be klaidų. Tokios sistemos yra efektyviai parengtos taip, kad duomenys iš vieno šaltinio į kelis kilometrus nutolusį gavėją perduodami vos per kelias sekundes, todėl informacija apdorojama greitai ir beveik realiuoju laiku.

⁶⁵ Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems, Vivian Lai et al., „Human-AI Collaboration via Conditional Delegation: A Case Study of Content Moderation“, Association for Computing Machinery, NY, United States, article no. 54, p. 1-18, 2022. Prieiga internetu: <https://dl.acm.org/doi/10.1145/3491102.3501999>

⁶⁶ Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems, Vivian Lai et al., „Human-AI Collaboration via Conditional Delegation: A Case Study of Content Moderation“, Association for Computing Machinery, NY, United States, article no. 54, p. 1-18, 2022. Prieiga internetu: <https://dl.acm.org/doi/10.1145/3491102.3501999>

⁶⁷ Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems, Vivian Lai et al., „Human-AI Collaboration via Conditional Delegation: A Case Study of Content Moderation“, Association for Computing Machinery, NY, United States, article no. 54, p. 1-18, 2022. Prieiga internetu: <https://dl.acm.org/doi/10.1145/3491102.3501999>

⁶⁸ Fadia Shah et al., *Artificial Intelligence as a Service for Immoral Content Detection and Eradication*, 2022 m. Prieiga internetu: <https://scispace.com/pdf/artificial-intelligence-as-a-service-for-immoral-content-20u8yach.pdf>

Šios sistemos trūkumai yra:

- Priklausomybė nuo duomenų kokybės: AlaaS labai priklauso nuo tvarkomų duomenų kokybės. Jei mokymo duomenyse yra šališkumo ar netikslumų, DI gali duoti nepatikimus rezultatus;
- Žmogaus kalbos sudėtingumas: Žmogaus kalbos supratimas iš esmės yra sudėtingas dėl niuansų, slengo ir konteksto. AlaaS gali būti sunku aptikti sarkazmą, humorą ar kultūrinės nuorodas, dėl kurių gali būti neteisingai įvertintas turinys;
- Kintantis amoralaus turinio pobūdis: Amoralaus turinio tipai gali greitai keistis, veikiami socialinių tendencijų ir įvykių. AlaaS sistemos turi būti nuolat atnaujinamos ir perkvalifikuojamos, kad neatsilikėtų nuo šių pokyčių;
- Reikalaujantis gausių resursų: AlaaS diegimas gali reikalauti didelės skaičiavimo galios ir saugyklos, ypač dirbant su dideliais duomenų rinkiniais. Tai gali būti kliūtis mažesnėms organizacijoms, kurios gali neturėti reikiamos infrastruktūros tokioms sistemoms palaikyti.⁶⁹

Apibendrinat DI išskiriamos šios silpnosios pusės:

- DI technologija negali veikti be žmogaus arba teisinių institucijų reguliacijos ir priežiūros;
- DI ne visada pateikia tikslus duomenis – reikėtų tai įvertinti iš ištestuoti prieš įdiegiant bet kokį DI metodą praktikoje, todėl reikia įsitikinti koki yra DI gebėjimai testavimuose;
- Iškyla etinės ir duomenų saugumo problemos susijusios su asmens privatumu, cenzūra, saviraiškos laisve;
- Reikiamybė investuoti nemažai resursų DI apmokymui ir naujinimui, taip pat informacijos talpinimui, kad DI veiktų kokybiškai.

Apibendrinat DI išskiriamos šios stipriosios pusės:

- Palengvina fizinį žmogaus darbą – dirbant kartu su DI pasiekiami geresni rezultatai;
- Padeda apdoroti didelius kiekius informacijos realiu laiku pigiau nei tą patį darbą atliktų žmonių komanda.

⁶⁹ Fadia Shah et al., Artificial Intelligence as a Service for Immoral Content Detection and Eradication, 2002 m. m. Prieiga internetu: <https://scispace.com/pdf/artificial-intelligence-as-a-service-for-immoral-content-20u8yach.pdf>

2.3. Ekspertinių nuomonių analizė

Įgyvendinant konsultacijas su suinteresuotomis pusėmis buvo atlikti 10 interviu (dalis respondentų atsakymus pateikė raštu). Iš viso interviu dalyvavo 15 asmenų (toliau – ekspertų). Ekspertų kvalifikacija grindžiama tuo, kad jie buvo deleguoti organizacijų, kurios dirba srityse, susijusiose su nelegalaus turinio problematika. Atitinkamai, vertinama, kad asmenis (ekspertus) delegavusios organizacijos savo atstovus paskyrė atsižvelgiant į jų kompetencijas. Respondentai buvo suskirstyti į 3 skirtingas grupes: autorinių teisių turėtojus atstovaujančios organizacijos (toliau – ATTA), audiovizualinio turinio paslaugų teikėjai (toliau – ATPT) ir informacijų bei technologinių įmonių atstovai (toliau – IRT). Respondentų (ekspertų) sąrašas pateikiamas 1 priede.

BENDROS ĮŽVALGOS APIE PIRATAVIMĄ LIETUVOJE IR GALIMYBĘ SU JUO KOVOTI

Respondentų paprašius įvardinti daugiausiai problemų Lietuvos kūrėjams keliančius paplitusius **technologinius piratavimo modelius**, kurių pagalba nelegalus turinys pasiekia naudotoją ir priešingai – naudotojas pasiekia nelegalų turinį, respondentai įvardijo šiuos:

- nelegaliai transliuojamas turinys internetinėje svetainėje;
- lygiarangių ryšio technologijos;
- nelegalaus turinio parsisiuntimas į savo įrenginį iš internetinės svetainės;
- nelegalus legalaus turinio kopijų atlikimas.

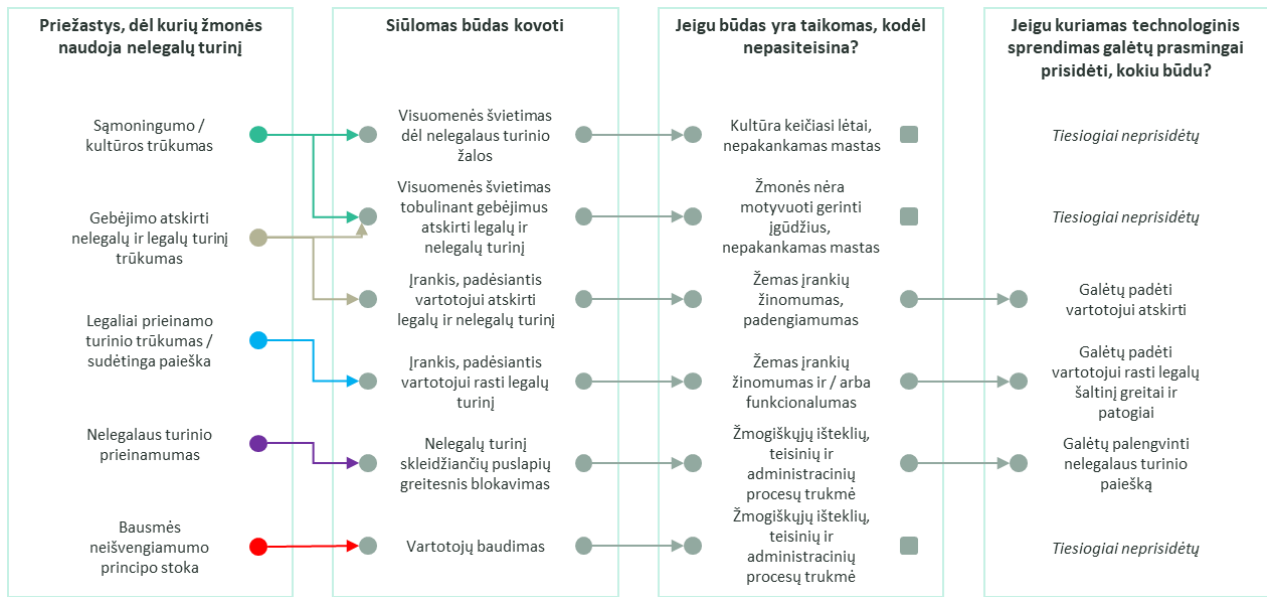
Maždaug pusė respondentų teigė, jog vienas iš svarbiausių būdų efektyviai kovoti su piratavimu yra **prevencija per švietimą**. Kadangi piratavimas priklauso nuo paklausos, naudotojų sąmoningumas ir atsakomybė galėtų išaugti supratęs, kokią žalą kelia piratavimas. Vienas iš respondentų nurodė Šveicariją kaip pavyzdį šalių, kurioms ši problema yra mažiau aktuali dėl aukšto sąmoningumo ir išsivystymo lygio. Kaip respondentas pabrėžė, Šveicarija nesiima jokių specialių švietimo ar blokavimo mechanizmų piratavimo mažinimui, nes jų valstybės visuomenei tai nėra būdingas reiškinys. Tai reiškia, jog visuomenės sąmoningumas bei sąžiningumas yra vienas svarbiausių aspektų siekiant mažinti piratavimą.

Kaip veiksmingiausią būdą kovoje prieš piratavimą minėjo **visuomenės informavimą / dėmesį patraukiančius įspėjimus** asmeniui bandant vartoti nelegalų turinį (bausmės neišvengiamumo veiksnys). Tai ypač aktualu, nes susiduriama su problema, kai ne visi naudotojai pajėgia lengvai atskirti, koks turinys yra legalus, o koks – ne. Tam tikrais atvejais netgi nelegalų turinį talpinančios svetainės prašo mokesčio už prieigą prie turinio, kas gali kelti įspūdį, jog turinys prieinamas legaliai, todėl įspėjimas padėtų naudotojams atskirti legalų turinį nuo nelegalaus.

Respondentų nuomone **dėl nuobaudų veiksmingumo kovojant su piratavimu internete išsiskyrė**. Dalis respondentų teigė, kad baudos yra veiksmingas būdas kovoti su piratavimu internete, o bausti reikėtų ir naudotojus, ir platintojus. Kita dalis teigė, jog pirmiausiai reikėtų bausti nelegalaus turinio naudotojus ir skeptiškai vertino naudotojus, kurie teigė esą nežinoję, kad turinį vartojo nelegaliai. Tretieji sakė, jog naudotojas turi mažiausiai įtakos nelegalaus turinio paplitimui internete, nes jis nėra atsakingas už platinimą, todėl nuobaudų griežtinimas turėtų būti nukreiptas į asmenis, kurie kelia nelegalų turinį į internetą. Be to buvo teigiama, kad įspėjimas, jog naudotojams, nelegaliai kaupiantiems ar vartojantiems skaitmeninį turinį, gali būti skiriama administracinė bauda už sąmoningą nelegalaus turinio vartojimą galėtų paskatinti naudotojus naudoti legalų turinį.

Beveik visi respondentai pabrėžė, jog greičiausiai ir efektyviausią rezultatą duotų **tinklapių, svetainių, kuriose talpinamas nelegalus turinys, blokavimas** ir kad tai turėtų būti esminis įrankis kovojant su nelegaliu turiniu. Visi minėję šį būdą pabrėžė suprantantys, jog šios priemonės veiksmingumas dažnai yra ribotas dėl nelegalaus turinio sklaidėjų inovatyvumo technologinėje sferoje. Dalis respondentų aiškiai artikuliuoja problemą – nelegalaus turinio sklaidos verslas yra labai pelninga veikla, todėl jos apsunkinimas nėra pakankamas įrankis, kad atgrasytų nuo veiklos tęsimo. Svetainių, kurios transliuoja / įkelia nelegalų turinį, blokavimas yra technologiškai sudėtingas procesas dėl teisinių apribojimų, resursų trūkumo bei infrastruktūrinių barjerų.

Toliau pateikiama schema, atvaizduojanti ryšius tarp išsakytų problemų, priežasčių ir galimų sprendimų (žr. toliau pateiktą paveikslą).



15 paveikslas. Ekspertinių nuomonių pagrindu sudaryta problemų, priežasčių ir galimų sprendimų schema
Šaltinis: sudaryta Konsultanto

Atitinkamai, galima išskirti kelias problemų–sprendimų grupes, kurios gali tapti pagrindu kuriamo technologinio sprendimo koncepcijoms (žr. 2.4.1. skyrių):

- Daliai visuomenės sunku atskirti legalų ir nelegalų turinį, kuriamas technologinis sprendimas galėtų padėti tokiems asmenims atskirti legalų ir nelegalų turinį.** Pažymėtina, kad ne visi ekspertai mano, kad tokia grupė žmonių yra pakankamai didelė, kad būtų galima pateisinti tokio technologinio sprendimo įgyvendinimo sąnaudas. Egzistuoja ir papildomos sėkmės sąlygos, aprašytos toliau skyriuje. Papildomai, egzistuoja rizika dėl neatsargaus (klaidingo) legalų turinį talpinančių svetainių įvertinimo kaip nelegalų turinį talpinančių svetainių (klaidingai teigiamas rezultatas), detaliau tai aprašyta 2.4.1. skyriuje.
- Daliai visuomenės sunku rasti legalų turinio šaltinį, kas yra susiję su legalių šaltinių fragmentacija (yra daug legalių šaltinių, tačiau norimas turinys gali būti prieinamas tik viename iš jų).** Kuriamas technologinis sprendimas galėtų veikti kaip duomenų bazė / paieškos mechanizmas, kuriame, kitaip nei įprastuose paieškos mechanizmuose, būtų talpinami tik legalų turinį talpinantys šaltiniai. Pažymėtina, kad tokios sistemos egzistuoja ir veikia praktikoje – iš kitos pusės, ne visos sistemos yra gerai pritaikytos Lietuvai, trūksta padengiamumo, kyla klausimų dėl naudotojų patirties.
- Viena iš priežasčių, dėl kurių stringa nelegalaus turinio talpinančių svetainių blokavimo procesai, yra tai, kad jų identifikavimui ir stebėsenai reikalingas didelis žmogiškųjų išteklių kiekis, kadangi tokio turinio internetinės svetainės sparčiai dauginasi.** Kuriamas technologinis sprendimas galėtų palengvinti tokių internetinių svetainių aptikimo greitį. Atsižvelgiant į interviu su LRTK medžiagą, šiuo metu LRTK naudoja didelį spektrą pažangių įrankių nelegalų turinį talpinančių internetinių svetainių aptikimui. Papildomai, atsižvelgiant į interviu su INAC, tokius įrankius naudoja (tyrimų, analizės ir skundų rengimo tikslais) ir privačios organizacijos, palengvinančios valstybės institucijų darbą. Kuriamas technologinis sprendimas šiuo atveju galėtų prisidėti prie asmenų savanorystės – tokiu atveju technologinis sprendimas pirmiausiai būtų platforma skundų pateikimui. Pažymėtina, kad kyla rizika dėl piktnaudžiavimo tokiu įrankiu iš nelegalaus turinio skleidėjų pusės (melagingų pranešimų siuntimas, manipuliavimas), detaliau tai aprašyta 2.4.1. skyriuje.

Šios problemų grupės yra naudojamos koncepcijų formavimui (plačiau žr. 2.4.1. skyrių).

ĮŽVALGOS DĖL KURIAMO TECHNOLOGINIO SPRENDIMO PAVYZDŽIO

Ekspertams buvo pasiūlyta įvertinti, kaip galėtų veikti techninėje specifikacijoje nurodytas technologinio sprendimo pavyzdys – „technologinis sprendimas, gebantis *identifikuoti nelegalų audiovizualinį turinį internete, įspėti apie tai naudotoją ir jam pasiūlyti norimą legalų turinį*. Toks sprendimas būtų diegiamas savarankiškai“.

Paklausus, ar respondentai yra girdėję apie jau veikiančius panašių technologinių sprendimų pavyzdžius, nei vienas iš apklaustų organizacijų atstovų teigė nežinantys apie panašiam tikslui naudojamų technologinių sprendimų

pavyzdžius. Respondentų buvo pateiktas vienas iš pavyzdžių MIRKT – Medijų ir informacinio raštingumo iniciatyva, kuri skatina skaitytojus, interneto naudotojus tikrinti duomenų šaltinių patikimumą, atskleidžia nepatikimų bei nelegalių šaltinių žalą, tačiau tai – ne technologinis sprendimas, o švietimo iniciatyva.⁷⁰ Buvo paminėta ir „Agorateka“ iniciatyva, vykdoma Europos mastu bei nacionalinis portalas Lietuvoje „Naudok legaliai“. Šių iniciatyvų tikslas panašus – padėti naudotojams rasti legalaus turinio svetaines internete, sutrumpinti legalaus turinio ir šių svetainių paieškos laiką bei padėti atskirti legaliai turinį talpinančias svetaines nuo nelegaliai talpinančių.

Taip pat buvo užsiminta, kad kiekviena šalis turi savo įrankius, kuriuos naudoja ribojant prieigą prie nelegalių svetainių. Pavyzdžiui, Portugalijos, Ispanijos ir Prancūzijos nacionaliniai reguliuotojai (atitinkamo LRTK Lietuvoje), užblokavus prieigą prie tam tikros svetainės, naudotojus nukreipia į savo portalą, kur pateikia legalių šaltinių alternatyvas.

Pradėjus diskusiją apie tai, ar, respondentų nuomone, kuriamas technologinis sprendimas būtų naudingas siekiant sumažinant piratavimo lygį Lietuvoje, atsakymai pasiskirstė į tris grupes: požiūris neutralus, skeptiškas, palaikantis.

Neutralus požiūris

Neutralų požiūrį palaikantys asmenys teigė, jog reikėtų vykdyti daugiau informacinių kampanijų, šviečiant, kas yra legalus turinys ir kodėl blogai jį naudoti – reikalingos didelės pastangos, norint pakeisti visuomenės mąstymą nelegalaus turinio aspektu, todėl nemanoma, jog kuriamas technologinis sprendimas turėtų daug naudoti be papildomų sąlygų išpildymo (viešinimas, visuomenės švietimas).

Interviu taip pat teigta, kad technologinio įskiepio efektyvumas reikšmingai priklausys ir nuo jo veikimo principo: kaip kuriamas technologinis sprendimas rinkis informaciją apie legalias ir nelegalias svetaines, pagal kokius požymius atskirs šias svetaines, ar tai bus teisiškai jau uždraustos svetainės, ar tik potencialiai nelegalios, ar savo veiklos pradžios nedeklaravusios svetainės. Šiuolaikinės technologijos suteikia galimybę įvertinti svetainės legalumą pagal tam tikrus vizualinius požymius, pasitelkus DI pagalbą. Vis dėlto sunku nustatyti, ar platforma iš tikrųjų yra nelegali pasitelkiant tik DI pagalbą ir skenuojant vizualiai pagal svetainės skiriamuosius bruožus. Nors DI leistų automatizuoti ir taip pagerinti įrankio darbą, tačiau nustatyti svetainės patikimumui nepakanka remtis tik vizualiais bruožais (tam reikalingas tam tikras teisinis pagrindas), tad kyla rizika, jog tokiu būdu surinkta informacija nebus visiškai tiksli. Daugiau patikimumo tokiam įrankiui suteiktų duomenų bazių informacijos ir DI pajėgumų sujungimas. Taip pat šią problemą būtų galima išspręsti pritaikant legalių skaitmeninio turinio svetainių skiriamąjį ženklą „virtualaus lipduko“ pavidalu, kurį legalaus turinio svetainės galėtų patalpinti savo portaluose. Respondentai teigė, jog tokio skiriamojo ženklo naudojimą neturėtų būti sudėtinga realizuoti Lietuvos mastu.

Taip pat dvejojama dėl šio įrankio veiksmingumo legaliai veikiančiose svetainėse, kuriose yra talpinama ir nelegalaus turinio. Pavyzdys – „Youtube“ platforma, kurioje dalis medžiagos įkelta pažeidžiant autorių teises. Iškyla klausimas, kaip bus informuojami naudotojai dėl nelegalaus turinio produktų legaliose svetainėse.

Skeptiškas požiūris

Respondentai pabrėžia, kad iki šiol didžiausias efektas kovojant su piratinio turinio mažinimu internete pasiektas pritaikant LRTK baudas fiziniams asmenims. Manoma, jog naudotojai irgi yra atsakingi už piratinio turinio sklaidą internete, tą rodo jų iniciatyva lankytis nelegalaus turinio tinklapiuose, taip sukuriant paklausą piratavimui. Teigiama, kad todėl Lietuvoje reikalinga taikyti bausmes tiek platintojams, tiek naudotojams. Skeptiškai vertinamas asmenų „negebėjimas“ atskirti legalaus turinio nuo nelegalaus, kadangi informacinių technologijų raštingumas šalyje yra išaugęs ir pakankamai daug viešumoje kalbama nelegalaus turinio tema. Dalis respondentų mano, jog Kultūros ministerijos 2024 m. tyrimo rezultatai dėl šališko respondentų įsivertinimo nesuteikia rimto pagrindo manyti, jog vis dar egzistuoja reikšminga visuomenės dalis, nesugebanti atpažinti nelegalaus turinio. Argumentuojama, jog tyrimo rezultatai gali būti sąmoningai iškraipyti tų respondentų, kurie tikriausiai žino, kaip atskirti legalias svetaines, bet sąmoningai renkasi nelegalius – nemokamus – audiovizualinius produktus, o atsakydami į tyrimo klausimus renkasi priešingą variantą dėl siekio atitikti socialines normas.

⁷⁰ Prieiga internetu: <https://mirkbt.bibliotekavisiems.lt/apie-mirkbt/>

Taip pat respondentai pastebėjo, kad tam tikrais atvejais legaliose platformose ieškomas turinys nėra siūlomas nei vienoje legalaus turinio platformoje, pavyzdžiui, tokiais atvejais, jei turinio produktas labai senas ir panaikintas iš transliavimo platformų. Tokiu atveju naudotojui rasti norimo turinio legaliai nepadėtų net išsamus legalių šaltinių alternatyvų sąrašas. Todėl išlieka technologinio sprendimo spraga – klausimas, kaip šis įrankis galėtų suteikti pagalbą naudotojui, ieškančiam tokio turinio, kurio nėra legalių svetainių gretose arba apskritai nebėra talpinama internete.

Respondentų paminėtas ir socialinių tinklų turinys, kuris, įdiegus technologinį sprendimą naršyklėje, liktų neapimtas, nes toks įrankis efektyviausiai veiktų tik internetinėse svetainėse, o ne programėlėje. Teigta, kad šiai problemai (bent iš dalies spręsti) galėtų būti pritaikyta mobilioji aplikacija, kuri atliktų platesnio masto duomenų rinkimą – mobiliosiomis programėlėmis, socialiniais tinklais ir paieškos sistemomis – tačiau tokios programėlės sukūrimas susidurtų su papildomomis problemomis (brangiau kainuotų, didėtų rizikos dėl duomenų apsaugos ir t.t.). Taip pat teigiama, jog net šiam technologiniam sprendimui atsiradus, tikėtina, jog nelegalaus turinio skleidėjai greitai adaptuosis, kaip kad vyksta su iki šiol taikytais nelegalaus turinio blokavimo mechanizmais (greitai randamas sprendimas, kaip apeiti technologinį įrankį).

Palaikantis požiūris

Šio požiūrio besilaikantys respondentai teigė, kad kuriamo Technologinio sprendimo pritaikymas galėtų padaryti poveikį naudotojams, kurie nori ir yra pasiryžę mokėti už legalų turinį ir būtent programos pranešimo funkcija galėtų sukelti didesnį sąmoningumo lygį.

Nepaisant teigiamo požiūrio buvo atkreipiamas dėmesys į tai, kad naudotojai dažniausiai nėra linkę lengvai pateikti informaciją apie save ir suteikti prieigą prie savo mobilaus įrenginio – į tai reiktų atsižvelgti, kuriant technologinį sprendimą. Papildomai, toks įrankis būtų naudingas tik tada, jei būtų patikimas (tikslus) ir pasižymėtų aukštu padengiamumo laipsniu, jeigu veiks neefektyviai – strigs įspėjimai, nebus patrauklus, neperduos naudotojui žinutės tinkamu ir suprantamu būdu – naudos nesukurs ir poveikis nepasireikš.

Nepaisant išsiskyrusių nuomonių dėl technologinio įrankio veiksmingumo, dalyviai akcentavo tai, jog daug kas priklauso nuo pasirinkto šio įrankio veikimo principo: ar tai bus programėlė, ar įskiepis, kokias įspėjamas žinutes šis Technologinis sprendimas siųs, kiek pateikiamas informuojantis tekstas bus įtraukus ir įtikinantis, pagal kokius požymius bus agreguojamos legalios ir nelegalios turinio svetainės ir t.t.

Siūloma į šio įrankio plėtrą įtraukti ir transliavimo platformas bei agentūras, kurios galėtų reklamuoti šį sprendimą savo klientams. Taip pat siūloma kuriant šį technologinį sprendimą įtraukti ATPT bei kitas institucijas ir taip didinti įrankio populiarumą. Bendradarbiaujant su institucijomis tokioms, kaip LRTK technologinio sprendimas tikėtina veiktų efektyviau, nes būtų naudojamosi LRTK išteklių – nelegalių svetainių bei šių svetainių veidrodinių svetainių sąrašai, URL adresai ir t.t. O įtraukus ATPT ir išnaudojant jų auditoriją reklamai tai pat tikimasi, jog technologinis sprendimas būtų supažindintas su legalaus turinio naudotojais internete, o tai technologiniam sprendimui suteiktų daugiau patikimumo.

PAPILDOMOS ĮŽVALGOS KURIAMAM TECHNOLOGINIAM SPRENDIMUI, NEPRIKLAUSOMAI NUO KONCEPCIJOS

Kuriamo technologinio sprendimo pranašumas galėtų būti konkurencingas, jeigu sujungtų jau egzistuojančių skirtingų technologinių sprendimų funkcijas vienoje vietoje arba jeigu būtų išpildytas patrauklesne forma.

Papildomai, toks technologinis sprendimas galėtų telkti suinteresuotas puses kovai su nelegaliu turiniu, kuri šiuo metu yra pakankamai fragmentuota. Kitaip, nei jau egzistuojantys blokavimo mechanizmai, kurių tikslas yra blokuoti neautorizuotos veiklos svetaines, talpinančias nelegalaus turinio vienetus, įrankis būtų teisiškai mažiau įpareigojantis, nes atliktų patariamąją funkciją naudotojui.

Įrankis kuriamas visuomenės daliai, kuriai priklauso sąmoningi, patikimi turinio naudotojai, kurie vartoja nelegalių turinį tik todėl, nes negeba atskirti nelegalaus turinio svetainių arba neranda legalaus turinio alternatyvų. Todėl šis kuriamas technologinis įrankis neapims blokavimo mechanizmų.

Technologinio sprendimo efektyvumo užtikrinimui būtina nuolatinė ir veiksminga įrankio sklaida ir viešinimas. Būtina integruoti įrankio viešinimą į esamas kovos su piratavimu veiklas – pavyzdžiui, minėti įrankį visuomenės švietimo kampanijų metu, integruoti įrankį į nelegalių portalų blokavimo internetinių svetainių pranešimus;

užtikrinti, kad įrankis nekeltų įtarimų dėl asmeninių duomenų apsaugos / naudotojų anonimiškumo. Tai reikėtų užtikrinti tiek techniškai (taikant šiuolaikines duomenų apsaugos technologijas), tiek išoriškai (pavyzdžiui, sukuriant galimybę patogiai išjungti įrankį, jeigu naudotojas nori dalį savo veiklos internete palikti konfidencialia). Nors kuriamas technologinis sprendimas ir taip bus įpareigotas laikytis duomenų saugos įstatymų bei nerinks naudotojų duomenų, tačiau psichologinis naudotojo užtikrintumas ir pasitikėjimas kuriamu technologiniu sprendimu turi būti jam pačiam suprantamas ir matomas. Kitaip spėjama, jog naudotojas, apskritai, bus nesusidomėjęs įsidiegti tokio įrankio savo mobiliajame arba kompiuteryje.

2.4. Technologinių sprendimų lyginamoji analizė

Šiame skyriuje, atsižvelgiant į 2.1. skyriuje pristatytą metodiką, yra parengiamos kuriamo technologinio sprendimo alternatyvos. Prieš pradėdant planuoti alternatyvas, svarbu atsižvelgti į Inovacijų agentūros įvykdytos rinkos konsultacijos rezultatus. Rinkos konsultacijoje dalyvavo 4 rinkos dalyviai: UAB „Corner Case Technologies“, MB „Vilantis“, UAB „Oxylabs“, UAB „Dizaino kryptis“.⁷¹ Visi respondentai paminėjo, jog didžiausia kliūtis įgyvendinant efektyvų, prieš nelegalų turinį kovojantį, technologinį sprendimą, turėtų kilti įgyvendinant pirmąją dalį, kurioje pasirenkama, koku būdu technologinis sprendimas rinks duomenis apie nelegalų turinį internete. Buvo pabrėžiama, kad tiek viena, tiek kita alternatyva turi turėti integracines sąsajas su informacijos šaltiniais (duomenų bazėmis, kompetentingų institucijų, pavyzdžiui LRTK, patvirtintais interneto svetainių, paslaugų teikėjų sąrašais ar pan.), kuriuose kaupiami duomenys apie nelegalų / legalų audiovizualinį turinį internete; šie duomenys turi būti pakankami ir patikimi, kad veiktų atitinkamas funkcionalumas.

Toliau pateikiamas konsultacijoje dalyvavusių įmonių pasiūlymų aprašymas lentelės formoje.

4 lentelė. Rinkos konsultacijų metu pateikti pasiūlymai

| Aprašymo dalis | Pasiūlymas A | Pasiūlymas B | Pasiūlymas C |
|-------------------------------|---|--|--|
| Sprendimo būdas | Naršyklės įskiepis | Legalaus turinio platforma, kurią sudarytų: 1. Internetinė svetainė legalaus turinio paieškai arba lietuviško turinio tiekėjų pritraukimui į JustWatch; 2. Nelegalaus turinio identifikavimo įrankis; 3. Naršyklės įskiepis naudotojui, sujungiantis pirmas dvi dalis. | Siūlomą sprendimą sudarytų 3 dalys: 1. Nelegalių tinklapių sąrašas (reikalingas įrankis identifikuoti nelegalius tinklapius ir procesui juos įtraukti į sąrašą); 2. Naršyklėje veikiantis įskiepis arba operacinės sistemos lygmeniu veikiantis sprendimas įspėjantis naudotoją apie nelegalų turinį; 3. Sprendimas nurodantis, kur turinį galima vartoti legaliai. |
| Pastabos ir pasiūlymai | 1. Pradiniame etape DI intelekto panaudojimas išplečia sprendimo sąmatą, todėl siūlytina pradėti naudoti paprastus algoritmus ir tik vėliau plėtoti prototipą su DI. Svetainių vaizdo palyginimas yra sudėtingesnis sprendimas. 2. Siūlymas orientuotis į pagrindinį funkcionalumą be papildomų funkcijų. 3. Siūlymas apsiriboti viena naršykle ir patikrinti, o tik vėliau plėsti, nors logiškiausia Firefox ir Chrome, susifokusuojant į konkrečią naudotojų grupę. | 1. Svarbu ne tik blokuoti svetaines, tačiau ir pasiūlyti, kaip patogiai rasti turinį – pastūmėti naudotojus link jo. Kitu atveju, naudotojai ras būtų, kaip apeiti blokavimus ir pasiekti turinį. 2. Iki šiol unifikotos lietuviškos platformos, kurioje būtų galima rasti legalų ir lietuvišką, ir užsienietišką audiovizualinį turinį, nėra, nes tokios platformos sukūrimas brangus ir jį sudėtinga komercializuoti – Lietuvos rinka yra per maža. Labai svarbu, kad kuriamas įrankis būtų patogus naudotojui – kitaip jie juo nesinaudos. | 1. Naršyklės įskiepij sukurti yra paprasčiau, todėl siūloma koncentruotis į jį. |

Šaltinis: parengta Konsultanto

Toliau skyriuose yra parengiamos kuriamo technologinio sprendimo koncepcijos, aprašomos funkcinės dalys, pasiūlomi galimi technologinio išpildymo variantai. Galiausiai parengiamos alternatyvos – alternatyvos yra palyginamos pagal nustatytus kriterijus 3. skyriuje.

⁷¹ Inovacijų agentūra GovTechlab, Rinkos konsultacija – „Kaip padidinti naudotojo sąmoningumą ir galimybes atskirti internete vartojamą legalų audiovizualinį turinį nuo piratinio?“, kopija yra prieinama Konsultantui.

2.4.1. Galimos koncepcijos

Atsižvelgiant į nustatytas problemas 2.3. skyriuje, galima išskirti tokias problemų grupės kuriamam technologiniam sprendimui:

- Pirmą problemų grupę: daliai visuomenės sunku atskirti legalų ir nelegalų turinį, kuriamas technologinis sprendimas galėtų padėti tokiems asmenims atskirti legalų ir nelegalų turinį.
- Antrą problemų grupę: daliai visuomenės sunku rasti legalų turinio šaltinį iš dalies dėl legalių šaltinių fragmentacijos (yra daug legalių šaltinių, tačiau norimas turinys gali būti prieinamas tik viename iš jų).
- Trečią problemų grupę: viena iš priežasčių, dėl kurių stringa nelegalų turinį talpinančių svetainių blokavimo procesai, yra nelegalų turinį talpinančių internetinių svetainių greitam aptikimui reikalingų žmogiškųjų išteklių poreikis. Kuriamas technologinis sprendimas galėtų padidinti tokių internetinių svetainių aptikimo greitį.

Dėl trečios problemų grupės sprendimo kyla abejonių dėl jų sprendimo tikslingumo, kuriam technologinio sprendimo kontekste. Atsižvelgiant į interviu su LRTK medžiaga, šiuo metu LRTK naudoja didelį spektrą pažangių įrankių nelegalų turinį talpinančių internetinių svetainių aptikimui. Abejotina, ar įrankių, tokių kaip Oxylabs sprendimai interneto skanavimui (plačiau žr. 2.2.1. skyrių), būtų tikslingi, nes rinkoje egzistuojantys sprendimai yra praktiškai veikiantys, o jų trūkumų sprendimas yra technologiškai sudėtingas procesas, reikalaujantis mokslinių tyrimų ir eksperimentinės plėtros (toliau – MTEP) veiklų įgyvendinimo. Dėl šios priežasties nesiūloma vystyti koncepcijos įrankio, kuris galėtų atlikti tas pačias funkcijas kaip rinkoje egzistuojantys sprendimai.

Iš kitos pusės, atsižvelgiant į interviu su LRTK medžiaga, pirmos problemų grupės sprendimas galėtų pasitarnauti LRTK darbui. Įrankis, kuris gali įspėti apie nelegalų turinį taip pat galėtų būti naudojamas kaip įrankis greitai ir patogiai pranešti apie galimai nelegalų turinį talpinančias svetaines. Tokiu būdu būtų sukurta platforma, kuri leistų nelegalaus turinio problemoms neabejingiems žmonėms tiek gauti patarimus dėl nelegalaus turinio, tiek patiems prisidėti prie nelegalaus turinio nustatymo procesų.

Pirmą ir antrą problemų grupę galima sujungti į integruotos platformos koncepciją – įrankis, kuris padėtų nustatyti nelegalų turinį ir rasti legalius turinio šaltinius.

Atitinkamai, formuojamos tokios koncepcijos nustatytų problemų sprendimui:

- **KONCEPCIJA A:** technologinis sprendimas, kuris gebėtų nustatyti, kad naudotojas bando peržiūrėti nelegalų turinį ir informuoti jį. Technologiniame sprendime turėtų būti įgyvendintos nelegalaus turinio nustatymo ir naudotojo informavimo funkcinės dalys. Technologinio sprendimo formatas galėtų būti programa arba naršyklės plėtinys (įskiepis). Technologinį sprendimą naudotojai diegtų savanoriškai. Technologinio sprendimo tikslinės auditorijos – sąmoningi, tačiau nelegalų turinį sunkiai gebantys atskirti naudotojai (vyresnio amžiaus naudotojai ir bendrai žemesnį žinių ir įgūdžių lygį turintys naudotojai) bei valstybės institucijų ir viešos prieigos kompiuterius administruojančios institucijos (bibliotekos, mokyklos ir t. t.). Panašūs sprendimai – Google Safe Browsing, EOL įskiepis.
- **KONCEPCIJA B:** technologinis sprendimas, kuris veiktų kaip integruotas paieškos įrankis. Technologiniame sprendime turėtų būti įgyvendintos turinio paieškos ir legalaus turinio duomenų bazės (nuosavos ir / arba susietos su egzistuojančiomis duomenų bazėmis). Technologinio sprendimo formatas galėtų būti internetinė svetainė arba naršyklės plėtinys (įskiepis). Pasirinkus naršyklės plėtinio (įskiepio) formatą, tokį įskiepį naudotojai diegtų savanoriškai. Technologinio sprendimo tikslinės auditorijos – sąmoningi, tačiau ieškant nelegalų turinį su sunkumais susiduriantys naudotojai. Panašūs sprendimai – JustWatch, Naudoklegaliai.lt.
- **KONCEPCIJA C:** technologinis sprendimas, kuris sujungtų prieš tai aprašytas dvi koncepcijas. Pagrindinis skirtumas – toks sprendimas negalėtų veikti vien internetinės svetainės (kaip koncepcija B) formatu – būtinas išpildymas naršyklės įskiepio arba programos formatu.

Atsižvelgiant į prieš tai aprašytas koncepcijas, kitame skyriuje išskiriamos tokių koncepcijų išpildymui reikalingos funkcinės dalys.

2.4.2. Konceptijų išpildymo funkcinės dalys

Atsižvelgiant į prieš tai aprašytas koncepcijas toliau pateikiamas reikalingų funkcinų dalių sąrašas:

- **FUNKCINĖ DALIS I:** Naršymo srauto atpažinimas naudotojo sistemoje. Ši funkcinė dalis reikalinga koncepcijų A ir C išpildymui. Galimi skirtingi funkcinės dalies išpildymo variantai (žr. 2.4.3. skyrių).
- **FUNKCINĖ DALIS II:** Nelegalaus turinio naudotojo naršymo sraute nustatymas. Ši funkcinė dalis reikalinga koncepcijų A ir C išpildymui. Galimi skirtingi funkcinės dalies išpildymo variantai (žr. 2.4.3. skyrių).
- **FUNKCINĖ DALIS III:** Vartotojo perspėjimas apie aptiktą nelegalų turinį. Ši funkcinė dalis reikalinga koncepcijų A ir C išpildymui. Galimi skirtingi funkcinės dalies išpildymo variantai (žr. 2.4.3. skyrių).
- **FUNKCINĖ DALIS IV:** Legalaus šaltinio paieška. Ši funkcinė dalis reikalinga koncepcijų B ir C išpildymui. Galimi skirtingi funkcinės dalies išpildymo variantai (žr. 2.4.3. skyrių).
- **FUNKCINĖ DALIS V:** Legalaus šaltinio duomenų bazė arba sąsajos su tokiomis bazėmis. Ši funkcinė dalis reikalinga koncepcijų B ir C išpildymui. Galimi skirtingi funkcinės dalies išpildymo variantai (žr. 2.4.3. skyrių).
- **FUNKCINĖ DALIS VI:** Pranešimo dėl galimai nelegalaus turinio pateikimo sistema. Ši funkcinė dalis reikalinga koncepcijų A ir C išpildymui. Galimi skirtingi funkcinės dalies išpildymo variantai (žr. 2.4.3. skyrių).

Pažymėtina, kad tai yra tik būtinosios koncepcijų minimalistiniam išpildymui funkcinės dalys. Suformavus alternatyvas, parengiami vystymo aprašymai (žr. 2.4.4. skyrių).

Šioms funkcinėms dalims egzistuoja skirtingi technologinio išpildymo variantai – jie aprašomi kitame skyriuje.

2.4.3. Funkcinių dalių išpildymo technologijos

Toliau aprašomi funkcinų dalių išpildymo technologiniai variantai.

TECHNOLOGINIO SPRENDIMO FORMATO TECHNOLOGIJOS / FUNKCINĖ DALIS I NELEGALAUS TURINIO NAUDOTOJO NARŠYMO SRAUTE NUSTATYMAS (KONCEPCIJOS A IR C)

Galima išskirti 3 variantus technologinio sprendimo formatui:

- **Variantas 0/IA:** Įskiepis naršyklėje. Aktualus funkcinėi daliai I;
- **Variantas 0/IB:** Operacinės sistemos lygmeniu veikianti programa (kompiuteryje arba mobiliame įrenginyje). Aktualus funkcinėi daliai I;
- **Variantas 0C:** Internetinė svetainė.

Įskiepis naršyklėje yra pranašesnis variantas už programos formatą šiais aspektais:

- įskiepij paprasčiau sukurti ir palaikyti;
- įskiepij paprasčiau įdiegti;
- nepatyręs naudotojas gali lengviau išjungti ir įjungti įskiepij;
- duomenų rinkimas yra apribotas veikla naršyklėje, todėl kyla mažesnės rizikos dėl asmens duomenų saugumo, tad ir naudotojams kils mažiau dvejonų šiuo klausimu.

Operacinės sistemos lygmeniu veikiančios programos variantas yra pranašesnis sprendimas už įskiepij šiais aspektais:

- Kuriamas technologinis sprendimas galėtų stebėti veiklą ne tik naršyklėje, bet ir programėlėse. Nors tokie sprendimai egzistuoja ir praktikoje veikia, pavyzdžiui, Teramind (žr. 2.2.1. skyrių), tačiau verta pažymėti, kad tai kelia objektyvias rizikas dėl asmens duomenų naudojimo saugumo. Verta pažymėti, kad toks sprendimas nebūtinai galėtų užtikrinti visų įrenginyje naudojamų programėlių skanavimą.

Internetinės svetainės variantas yra galimas sprendimas tik koncepcijai B. Kitais atvejais nebūtų išpildoma funkcinė dalis I (Naršymo srauto atpažinimas naudotojo sistemoje).

Atsižvelgiant į tai, kad technologinį sprendimą būtų tikslinga vystyti etapais (pradėti nuo paprastesnės išpildymo versijos, tuomet pildyti technologinį sprendimą sudėtingiau išpildomais aspektais), įskiepis šiuo aspektu būtų pranašesnis sprendimas. Tai patvirtina ir rinkos konsultacija, kurią atliko Inovacijų agentūra.

Iš kitos pusės, įskiepis naršyklėje turi apribojimus:

- Nemaža dalis turinio vartojimo vyksta atskirose programėlėse (pavyzdžiui, socialinių tinklų programėlės) – todėl, jeigu būtų nuspręsta technologinį sprendimą sukurti įskiepio formoje – jis negalėtų padengti šios veiklos. Kita vertus, kaip buvo nustatyta 1-ame Studijos skyriuje, pagrindinę problemą kelia piratavimo modeliai, kur naudotojas apsilanko internetiniame puslapyje per naršyklę. Todėl vertinama, kad šis įskiepio varianto apribojimas, nors ir neužtikrintų visiško piratavimo ribojimo, tačiau būtų nukreiptas į pagrindinius šios veiklos kanalus – nelegalaus turinio naršyklėse.
- Įskiepiei naršyklėje mobiliuose įrenginiuose susiduria su apribojimais – ne visos naršyklės mobiliuose įrenginiuose sukuria galimybę įdiegti įskiepi ir / arba įskiepių diegimo procesas nėra patrauklus / aiškus naudotojui. Lietuvoje egzistuoja dvi pagrindinės mobiliųjų įrenginių operacinės sistemos – Apple iOS ir Google Android sistemos. Apple iOS numatytoji naršyklė palaiko įskiepių diegimą, tačiau jų diegimo procesas nėra patrauklus naudotojui (reikia įsidiesti programėlę, tuomet per nustatymus leisti šiai programėlei išplėsti naršyklės funkcijas). Numatytoji Google Android sistemos naršyklė „Google Chrome“ nepalaiko jokių įskiepių. Tarp populiarių palaikomų Google Android sistemų naršyklių galima išskirti „Firefox for Android“ ir „Samsung Internet“. Abiejų sistemų atveju dalis programinės įrangos kūrėjų pasirenka sukurti dedikuota naršyklę – pavyzdžiui, naršyklę su reklamų blokavimo funkcijomis, tačiau toks sprendimas brangesnis ir sudėtingesnis.

Atsižvelgiant į išvardintus abiejų sistemų apribojimus, siūloma pradiniuose technologinio sprendimo vystymo etapuose apsiriboti įskiepio naršyklėje sukūrimu. Tam būtų reikalingos šios įskiepių versijos:

- Windows sistemos (kompiuteriai): „Chrome“, „Firefox“;
- Apple sistemos: „Safari“ (kompiuteriams ir mobiliems įrenginiams skirtos versijos);
- Android sistemos: „Firefox for Android“.

FUNKCINĖ DALIS II – NELEGALAUS TURINIO NAUDOTOJO NARŠYMO SRAUTE NUSTATYMAS

Funkcinė dalis skirta koncepcijų A ir C išpildymui. Galima išskirti du galimus variantus nelegalaus turinio nustatymui:

- **Variantas IIA:** internetinės svetainės informacijos (URL adresas ir kita internetinės svetainės informacija) siuntimas į serverį sprendimui dėl šaltinio legalumo;
- **Variantas IIB:** internetinės svetainės informacijos ir turinio analizė įrenginyje.

Variantas IIA yra lankstesnis, nes nereikia atnaujinti įrankio, norint pakeisti / atnaujinti nelegalaus turinio nustatymo algoritmų, taip pat leidžia pasitelkti didelį kiekį informacijos iš duomenų bazių. Informacija duomenų bazėse gali būti pildoma pusiau automatiškai (t.y. pasitelkiant žmogiškuosius resursus).

Variantas IIB kelia daugiausiai iššūkių iš technologinės pusės. Šį variantą įgyvendinant reikėtų sukurti algoritmus, kurie galėtų be išorinės informacijos arba su minimaliu jos kiekiu atskirti nelegalų turinį nuo legalaus. Šiuo atveju didėtų tikimybė, kad nelegalaus turinio skleidėjai galėtų pritaikyti savo internetines svetaines taip, kad galėtų klaidinti kuriamo įrankio algoritmus.

Varianto IIA veikimo principas paprastas – įrankis surenka reikalingą internetinės svetainės informaciją ir ją perduoda serveriui. Įvyksta informacijos patikrinimas per serveryje nustatytus algoritmus ir yra grąžinamas rezultatas (pranešimas naudotojui).

Varianto IIB veikimo principas turėtų remtis išorinių svetainės požymių nustatymu. Pavyzdžiui, algoritmas galėtų bandyti nustatyti, ar puslapyje pateikiamas turinys nėra būdingas nelegalaus turinio portalams. Kaip tokių bruožų pavyzdį galima pateikti:

- Puslapyje dažnai minimi raktažodžiai, būdingi nelegalaus turinio portalams. Tokių raktažodžių pavyzdžiu galėtų būti „žiūrėti nemokamai“, „смотреть онлайн“ (rus. žiūrėti internetu), „free torrent download“ (angl. nemokamas torentų parsisiuntimas).
- Nėra nurodomi rekvizitai ir kontaktai.

- Nėra nurodomos licencijos arba nėra suteikiama galimybė pranešti apie turinio nelegalumą.
- Didelis kiekis specifinės reklamos (lošimų internetu ir pan.).
- Įtartini slapukai (angl. „cookie“).
- Kitos įtartinės technologijos.

Nors tokia sistema galėtų veikti (pavyzdžiui, Oxylabs sprendimai interneto skanavimui, plačiau žr. 2.2.1. skyrių), ypatingai jeigu būtų pasitelkti DI paremti sprendimai (DI algoritmai turėtų veikti serveryje), galima numanyti, kaip nelegalaus turinio skleidėjai galėtų tokius algoritmus apeiti: raktažodžiai galėtų būti pakeisti, galėtų būti nurodyti fiktyvūs rekvizitai ir t. t. Papildomai, remiantis interviu su LRTK praktikoje tokie sprendimai yra patikimi tik ieškant jau žinomų nelegalaus turinio svetainių kopijų. Priešingu atveju, sistemos patikimumas ženkliai suprastėja.

Svarbu pabrėžti, kad net ir tobulu atveju, yra tikimybė, kad įrankis, paremtas Variantu IIB, aktyvaus pranešimo naudotojui metu teiktų klaidingus rezultatus (tiek klaidingai teigiamus, tiek klaidingai neigiamus). Ypač aktualu tai būtų vartojant turinį iš užsienietišκών legalių šaltinių. Iš kitos pusės, Variantu IIA paremtas kuriamas įrankis susidurtų su kitokiais iššūkiams – duomenų bazės, nuo kurių yra priklausomas kuriamas įrankis, turėtų būti pildomos ir atnaujinamos pakankamai intensyviai, kad nenukentėtų įrankio padengiamumas.

Apibendrinant, tobulinant Variantu IIA paremtą įrankį, reikėtų vykdyti padengiamumo plėtrą, o tobulinant Variantu IIB paremtą įrankį, reikėtų siekti tobulinti įrankio tikslumą.

Vertinama, kad atsižvelgiant į įrankio tikslą (padėti naudotojui atskirti legalų ir nelegalų turinį), prioritetu turėtų būti laikomas įrankio tikslumas, o ne padengiamumas. Klaidingi įrankio pranešimai naudotojui galėtų atbaidyti naudotojus labiau, negu pranešimo naudotojui nebuvimas. Yra rizikos, kad klaidingi įrankio pranešimai naudotojui teisiniu požiūriu galėtų būti traktuojami kaip klaidinga informacija. Dėl šios priežasties, pirmiausiai yra svarstoma Variantas IIA, tačiau verta pažymėti, kad Variantu IIB galėtų būti pritaikoma kitam tikslui – Variantu IIA duomenų bazių pildymui.

Pasirinkus įgyvendinti Variantą IIA („Internetinės svetainės informacijos (URL adreso ir kitos internetinės svetainės informacijos) siuntimas į serverį sprendimui dėl šaltinio legalumo“) svarbu apsvarstyti serveriuose veikiančių duomenų bazių informacijos pildymo variantus. Galima išskirti keletą variantų, kurie galėtų būti kombinuojami:

- **Variantas IIA-1:** visiškai neautomatizuotas būdas, pildant nelegalių ir legalių šaltinių sąrašus, paremtas skundų gavimu, viešų šaltinių analize, bendradarbiavimu su autorių teisių turėtojais ir jiems atstovaujančiomis organizacijomis;
- **Variantas IIA-2:** pusiau automatizuotas būdas, paremtas „patikimų žymėtojų“ įsitraukimu, pildant nelegalių ir legalių šaltinių sąrašus;
- **Variantas IIA-3:** visiškai neautomatizuotas būdas, pildant legalių šaltinių sąrašus pagal konkrečius kūrinius, paremtas autorių teisių turėtojų ir jiems atstovaujančių organizacijų, įsitraukimu;
- **Variantas IIA-4:** pusiau automatizuotas būdas, paremtas pačio įrankio nustatytų įtartinų šaltinių sąrašų tikrinimu, pildant sąrašus šaltinių, dėl kurių kilę įtarimai pasiteisino (reikalauja Variantu IIB bent dalinio diegimo kartu su Variantu IIA).

Atsižvelgiant į tai, kad visi keturi variantai gali būti įgyvendinami kartu geriausiam rezultatui pasiekti, variantų silpnąsias ir stipriąsias puses svarbiau suprasti ne tam, kad būtų pasirinkta tik dalis variantų, bet tam, kad skirtingus variantus būtų galima suderinti geriausiu būdu. Tinkamai suderinus skirtingus variantus galima pasiekti didžiausią padengiamumą ir tikslumą, sumažinti sistemos palaikymo sąnaudas.

Variantas IIA-1 veikimo principas iš esmės nesiskiria nuo to, kaip veikia LRTK. Sudarant sąrašus internetinių svetainių blokavimui (dėl nelegalaus turinio arba kitų Lietuvos Respublikos įstatymuose numatytų priežasčių) yra pasitelkiamos šios strategijos:

- skundų nagrinėjimas;
- viešųjų šaltinių analizė, internetinės erdvės stebėjimas.

Pagrindinis skirtumas nuo LRTK veiklos šiuo atveju būtų sprendimo dėl svetainės įtraukimo į nelegalaus turinio sąrašus priėmimo greitis. Ypatingai, jeigu būtų pasirinkti mažiau kategoriški / tikslesni pranešimų naudotojui būdai (pavyzdžiui, „Šiame puslapyje pasiekimas turinys galimai yra nelegalus“ vietoje „Šis turinys yra nelegalus“),

sprendimą dėl svetainės įtraukimo galima būtų priimti per darbo dieną (palyginus, LRTK sprendimai gali užtrukti iki mėnesio, priklausomai nuo LRTK narių susirinkimo dažnio).

Papildomas skirtumas – LRTK veikla neapima pranešimo naudotojui apie tai, kad jų norimas peržiūrėti turinys yra legalus. Šiuo atveju technologinio sprendimo administratoriai pildytų ir legalaus turinio sąrašus, kad remiantis šio sąrašo informacija būtų galima 100 proc. garantuoti naudotojui, jog jis apsilankė legalaus turinio svetainėje.

Į šio varianto įgyvendinimą galima būtų įtraukti ir pačius technologinio sprendimo naudotojus, suteikiant naudotojams galimybę pranešti apie įtarimus dėl netikslaus kuriamo technologinio sprendimo rezultato. Tokius pranešimus reikėtų patikrinti kiekvienu atskiru atveju.

Šio varianto pagrindinė problema – didelis poreikis rankų darbui. Šį darbo krūvį galima dalinai perkelti savanoriškais pagrindais veikiantiems subjektams, pasitelkiant Variantą IIA-2.

Variantas IIA-2 atspindėtų SPA įtvirtinamą sistemą, kai atrinktomis organizacijoms būtų suteikiamas pasitikėjimo kreditas priimti sprendimus, mažinant piratavimo kanalus arba nelegalų turinį. Tokios sistemos taip pat yra plačiai naudojamos privačiose platformose (pavyzdžiui, „YouTube Priority Flagger“ programa⁷²).

Tokius naudotojus (Patikimus žymėtojus) galėtų atrinkti ir prieigą prie duomenų bazės pildymo jiems suteikti Kultūros ministerija arba kita organizacija, atsakinga už kuriamo technologinio sprendimo administravimą. Patikimi pranešėjai galėtų patys duomenų bazėse įtraukti svetaines į nelegalių arba legalių internetinių svetainių sąrašą, ribotų prieigos teisę (taigi, ir informacijos pildymo galimybes) prie šių duomenų bazių. Svarbu, kad jų pildomą informaciją būtų galima atskirti nuo kitų duomenų bazės pildymo būdų dėl to, kad:

- būtų tikslinga naudotojui pranešti, kad įrankis jam pateikia žinutę dėl internetinės svetainės nelegalumo, remiantis būtent Patikimo žymėtojo pranešimu. Tokiu būdu būtų suvaldoma dalis rizikos dėl nesąžiningos atskirų Patikimų žymėtojų veiklos, atsakomybę perkeltiant konkrečioms organizacijoms.
- būtų sudaryta galimybė stebėti Patikimų žymėtojų veiklos kokybę – atsekti kas, kada ir kodėl įtraukė puslapį į nelegalių internetinių svetainių sąrašą. Tai leistų vykdyti atsitiktinę Patikimų žymėtojų veiklos patikrą, numatant sankcijas už nesąžiningą arba nekokybišką darbą. Tai motyvuotų Patikimus žymėtojus atsakingai atlikti savo funkcijas.

Variantas IIA-3 spręstų kitą iššūkį, siekiant užtikrinti Kuriamo technologinio sprendimo tikslumą – kaip elgtis situacijose, kai internetinėse svetainėse, kuriuose dominuoja nelegalus turinys, atsiranda atviros licencijos turinys (pavyzdžiui, jeigu į Torrent platformas įkeliamas atvira licencija pažymėtas turinys) arba atvirkščiai, jeigu legaliuose šaltiniuose atsiranda nelegalus turinys (pavyzdžiui, jeigu į YouTube platformą turinys įkeliamas nelegaliai).

Pritaikius šį variantą kurinių autoriams arba jų atstovams būtų sudaryta galimybė deklaruoti legalius jų kūrinių peržiūros šaltinius. Atitinkamai, jeigu įrankis nustatytų, kad turinys yra paviešintas kitokioje platformoje, įrankis praneštų, kad toks turinys yra viešinamas nelegaliai.

Įgyvendinant variantą reikėtų sukurti atskirą procedūrą autoriaus arba jo atstovo autorizavimui. Šio varianto įgyvendinimui būtų reikalinga integracija su kūrinių duomenų bazėmis (siekiant išvengti atvejų, kai panašiai pavadinti kuriniai būtų supainiojami) arba kurti atskirą duomenų bazę (detaliau žr. toliau).

Pats Variantas IA turėtų būti papildytas galimybe nustatyti, prie kokio kūrinio yra suteikiama prieiga pasirinktame puslapyje. Toks papildomas funkcionalumas taip pat būtų būtinas ir toliau pateikto varianto įgyvendinimui.

Variantas IIA-4 išnaudotų analizuojamą informacijos srautą įtartinų, tačiau į duomenų bazę neįtrauktų, internetinių svetainių nustatymui, tokių svetainių sąrašo formavimui. Šį sąrašą turėtų peržiūrėti administratorius, kuris priimtų galutinį sprendimą dėl šaltinio legalumo. Tik po sprendimo dėl šaltinio legalumo priėmimo ir įtraukimo į nelegalių šaltinių sąrašą, įrankis pradėtų informuoti naudotojus apie šaltinio nelegalumą. Iki to laiko įrankis galėtų tik informuoti naudotoją, kad šiuo metu vyksta internetinės svetainės tikrinimas.

FUNKCINĖS DALIES III – VARTOTOJO PERSPĖJIMAS APIE APTIKTĄ NELEGALŲ TURINĮ

⁷² Prieiga internetu: <https://support.google.com/youtube/answer/7554338?hl=en>

Vartotojo informavimas apie aptiktą nelegalų turinį yra aiškiausia kuriamo technologinio sprendimo koncepcijos dalis. Pasirinkus Variantą IB (programėlės sukūrimas) informavimas veiktų operacinės sistemos pranešimų pagalba. Pasirinkus Variantą IA (įskiepio sukūrimas) informavimą tikslingiau būtų vykdyti per atsidarantį įskiepio langą arba pasikeičiančio įskiepio logotipo pagalba (tokiu būdu šiuo metu veikia EOL įskiepis). Tuo remiantis galima suformuluoti tokius variantus:

- **Variantas IIIA:** operacinės sistemos pranešimai;
- **Variantas IIIB:** iššokantis langas;
- **Variantas IIIC:** įskiepio logotipo pasikeitimas.

Variantai IIIB ir IIIC gali veikti kartu arba galima sukurti naudotojui galimybę įrankio nustatymuose pasirinkti tinkamiausia jam variantą. Iššokantis langas galėtų per daug trikdyti naršymo internete procesą, todėl siūloma Variantą IIIB taikyti tik tais atvejais, kai įrankis nustatė nelegalų turinį.

Ne mažiau svarbu yra nustatyti, kokio tipo pranešimus matys naudotojas. Priklausomai nuo pasirinktų nelegalaus turinio duomenų bazių pildymo variantų skirsis pranešimo naudotojui detalumas. Paprasčiausias diferencijavimas turėtų būti toks:

- pranešimas apie aptiktą nelegalų turinį;
- pranešimas apie aptiktą legalų turinį;
- pranešimas apie tai, kad įrankis negali priimti sprendimo dėl turinio legalumo.

Siekiant vystyti įrankio tikslumą ir padengiamumą, reikėtų įvesti diferencijavimą pagal šaltinį (ar pats šaltinis yra legalus / nelegalus) ir turinio vienetą (ar turinio vienetas yra viešinamas legaliai arba nelegaliai):

- Pranešimas apie tai, kad šaltinis yra legalus, tačiau yra pagrindo manyti, kad turinio vienetas patalpintas nelegaliai (autorius arba jo atstovas nenurodė šio šaltinio legalių šaltinių šiam kūriniai sąrašė);
- Pranešimas apie tai, kad šaltinis yra nelegalus, tačiau kurinio autorius arba jo atstovas nurodė, kad turinio vienetas ten patalpintas legaliai.
- Pranešimas apie tai, kad šaltinio legalumas nėra žinomas, tačiau autorius arba jo atstovas nurodė, kad turinys yra patalpintas legaliai.
- Pranešimas apie tai, kad šaltinio legalumas nėra žinomas, tačiau yra pagrindo manyti, kad turinio vienetas patalpintas nelegaliai (autorius arba jo atstovas nenurodė šio šaltinio legalių šaltinių šiam kūriniai sąrašė).

Galiausiai būtų tikslinga informuoti naudotoją apie teisinį ar kitokį neapibrėžtumą dėl konkretaus šaltinio. Tai turėtų būti tokio pobūdžio pranešimai:

- Pranešimas apie tai, kad šaltinis šiuo metu yra tikrinamas;
- Pranešimas apie tai, kad vyksta teismai ar kitokie teisiniai ginčai dėl turinio legalumo.

Galiausiai, pranešime svarbu nurodyti, kas yra priėmęs sprendimą dėl vienokio ar kitokio vertinimo – ar tai padarė Kultūros ministerija, ar Patikimi pranešėjai ir t.t.

FUNKCINĖS DALIES IV GALIMAS IŠPILDYMAS – LEGALUS ŠALTINIO PAIEŠKA

Galima išskirti 3 galimas prieigas prie alternatyvaus legalaus šaltinio pasiūlymo:

- **Variantas IVA:** automatizuotas sprendimas, kai sistema automatiškai nuskaity, kokį turinį nori peržiūrėti naudotojas, ir atlieka paiešką (išpildoma tik su Koncepcijomis A ir C);
- **Variantas IVB:** pusiau automatizuotas sprendimas, kai sistema tik pasiūlo pradėti paiešką (parodomas laukas paieškos raktažodžių įvedimui);
- **Variantas IVC:** neautomatizuotas sprendimas, kai įrankis tik pasiūlo nuorodas į internetines svetaines, kuriuose galima atlikti legalių šaltinių paiešką.

Vartotojui didesnis automatizacijos laipsnis gerina naudotojo patirtį, skatina naudotis įrankiu. Kita vertus, jau egzistuoja išvystyti sprendimai, kurie leidžia atlikti legalių šaltinių paiešką. Todėl nebent būtų pasirinkta kurti nuosavą legalių šaltinių duomenų bazę (žr. toliau), galimybė atlikti paiešką pačiame įrankyje nėra būtina.

FUNKCINĖ DALIS V: LEGALUS ŠALTINIO DUOMENŲ BAZĖ ARBA SĄSAJOS SU TOKIOMIS BAZĖMIS

Galiausiai, formuluojant technologinį sprendimą reikėtų pasirinkti, kokiomis duomenų bazėmis reikėtų naudotis, siūlant naudotojui legalų turinio šaltinį. Galima išskirti 3 būdus:

- **Variantas VA:** sąsajų su egzistuojančiomis duomenų bazėmis / platformomis sukūrimas per API;
- **Variantas VB:** nuosavos duomenų bazės sukūrimas;
- **Variantas VC:** DI pasitelkimas legalių šaltinių paieškai.

Variantas VA yra pranašus tuo, kad jau egzistuoja legalių kūrinių šaltiniai ir duomenų bazės / platformos tiek Lietuvoje, tiek užsienyje. Tarptautinis portalas JustWatch.com suteikia naudotojams galimybę rasti konkretaus kūrinio legalius šaltinius. Šio portalo trūkumas tas, kad jis orientuotas tik į filmus arba TV laidas. Lietuviškas šio tinklalapio atitikmuo – Naudoklegaliai.lt – leidžia ieškoti legalių šaltinių ne tik filmams ar TV laidoms, bet ir knygoms, žaidimams, muzikai. Naudoklegaliai.lt pagrindinis trūkumas – sistema leidžia rasti šaltinius, tačiau neleidžia atlikti paieškos tuose šaltiniuose. Kaip kitą panašiais funkcionalumais pasižyminčią duomenų bazę galima įvardinti kuriamą E-kultūrą portalą (šios sistemos apribojimai Studijos rengimo metu dar nėra iki galo žinomi). Minėti platformų apribojimai reiškia, kad ne visais atvejais įrankis galės rasti dominantį kūrinių legaliai prieinamose duomenų bazėse. Nepatenkinamas paieškos rezultatas gali sukelti naudotojo nepasitenkinimą, mažins tikimybę, kad naudotojas toliau naudosis įrankiu. Be to, įprastai prieiga prie tokių duomenų bazių yra mokama, dėl ko išaugtų įrankio palaikymo išlaidos.

Variantas VB šiuo atžvilgiu yra pranašesnis. Sudarius atskirą nuosavą duomenų bazę, ją pildyti bus galima savarankiškai. Tokiu atveju duomenų bazės pakankamumas priklausys nuo technologinio sprendimo kūrėjų ir administruojančios institucijos bei jų galimybių šią bazę pildyti. Svarbu pabrėžti, kad tokios duomenų bazės sukūrimas kainuotų brangiau, nors jos palaikymas galėtų būti pigesnis nei Varianto VIA ir Varianto VIC atvejais.

Variantas VC veiktų pasitelkiant DI paieškos atlikimui (pavyzdžiui, ChatGPT). Įgyvendinant tokį sprendimą reikėtų sukurti sąsają su DI platforma, analogiškai kaip ir Varianto VIA atveju. Toks sprendimas nesudurtų su duomenų bazių pakankamumo apribojimais, tačiau atsakymų tikslumas galėtų suprastėti. Kaip ir Varianto VIA atveju, už prieigą prie DI platformų reikėtų susimokėti.

API (angl. *Application Programming Interfaces*) yra realizuotos integracinės sąsajos su informaciniais šaltiniais (duomenų bazės, kompetentingų institucijų patvirtinti interneto šaltiniai, internetinės svetainės, paslaugų teikėjų sąrašai ir t.t.), kuriuose kaupiami duomenys apie nelegalų / legalų audiovizualinį turinį internete. Šie duomenys turi būti pakankami ir patikimi, kad veiktų reikiamas funkcionalumas. Technologinis sprendimas turi turėti aplikacijos programavimo sąsają (API) skirtą audiovizualinio turinio tiekėjams valdyti ir naujinti savo siūlomo turinio detales. Pavyzdžiui, integravus API „OpenAI“, kaina vienam mėnesiui, jeigu įskiepiau naudotųsi bent 10 000 naudotojų, bendra kaina siektų iki 10 000 eurų. Taip yra todėl, nes OpenAI paslaugos kaina priklauso nuo apdorojamos informacijos ženklų skaičiaus.⁷³ Jeigu įskiepis analizuoja tekstinį turinį, kur kiekviena užklausa apima apie 200 žodžių (~260 ženklų) ir jeigu įskiepis turi 10 tūkstančių aktyvių naudotojų, kurie sugeneruoja po 10 užklausų per dieną bendra mėnesio kaina apytiksliai skaičiuojama 8 536 eurų mėnesiui. Ši kaina buvo apskaičiuota OpenAI GTP-4 modeliui.⁷⁴ Vienos užklausos kainą apskaičiuoti sunku, nes nurodoma kainų grindys milijonui ženklų. Tačiau, jeigu viena užklausa apimtų ne daugiau nei 390 ženklus (vidutinio ilgio tekstas), užklausos kaina turėtų būti ne daugiau nei 0,002 dolerio centai.

FUNKCINĖS DALIES VI GALIMAS IŠPILDYMAS – PRANEŠIMO DĖL GALIMAI NELEGALAUS TURINIO PATEIKIMO SISTEMA

Įgyvendinant funkcinę dalį VI, dabartiniame etape nėra tikslinga išskirti konkrečios technologijos. Svarbiausia, kad pranešimo suformavimas būtų kuo labiau automatizuotas, egzistuoja vidinė naudotojų reitingavimo sistema, kuri leistų atskirti patikimus naudotojus nuo nepatikimų.

Atsižvelgiant į skirtingų funkcinę dalių išpildymo analizę, toliau skyrįje formuluojamos konkrečios alternatyvos.

⁷³ Truehost, Mysson, „OpenAI API pricing (deep dive and tips)“, 2025 m. Prieiga internetu: https://thetruehost.co.uk/openai-api-pricing/?utm_source=chatgpt.com

⁷⁴ Truehost, Mysson, „OpenAI API pricing (deep dive and tips)“, 2025 m. Prieiga internetu: https://thetruehost.co.uk/openai-api-pricing/?utm_source=chatgpt.com

2.4.4. Alternatyvų formavimas

Šiame skyriuje pristatomos suformuotos alternatyvos. Prie kiekvienos alternatyvos nurodoma pirmoje kuriamo technologinio sprendimo versijos koncepcija, funkcinės dalys, technologinio išpildymo variantai. Papildomai, aprašomos vystymo galimybės – kokios funkcinės dalys ir / arba technologinio išpildymo variantai galėtų būti realizuojami ateityje, patikrinus koncepcijos gyvybingumą.

ALTERNATYVA A1 – PAGALBININKAS NAUDOTOJUI ĮSKIEPIO FORMA (BE PAŽANGIŲ ALGORITMŲ, REMIANTIS DUOMENŲ BAZĖMIS)

Išpildoma Koncepcija A: technologinis sprendimas, kuris gebėtų nustatyti, kad naudotojas bando peržiūrėti nelegalų turinį ir informuoti jį. Technologiniame sprendime turėtų būti įgyvendintos nelegalaus turinio nustatymo ir naudotojo informavimo funkcinės dalys. Technologinio sprendimo formatas galėtų būti programa arba naršyklės plėtinys (įskiepis). Technologinį sprendimą naudotojai diegtų savanoriškai. Technologinio sprendimo tikslinės auditorijos – sąmoningi, tačiau nelegalų turinį sunkiai gebantys atskirti naudotojai (vyresnio amžiaus naudotojai ir, apskritai, žemesnį žinių ir įgūdžių lygį turintys naudotojai) bei valstybės institucijų ir viešos prieigos kompiuterius administruojančios institucijos (bibliotekos, mokyklos ir t. t.). Panašūs sprendimai – Google Safe Browsing, EOL įskiepis.

Realizuojamos funkcinės dalys:

- Funkcinė dalis I: Naršymo srauto atpažinimas naudotojo sistemoje.
- Funkcinė dalis II: Nelegalaus turinio naudotojo naršymo sraute nustatymas.
- Funkcinė dalis III: Vartotojo perspėjimas apie aptiktą nelegalų turinį.
- Funkcinė dalis VI: Pranešimo dėl galimai nelegalaus turinio pateikimo sistema.

Planuojami technologinio išpildymo variantai:

- Funkcinė dalis I: Įskiepis naršyklėje (Variantas O/IA);
- Funkcinė dalis II: internetinės svetainės informacijos (URL adresas ir kita internetinės svetainės informacija) siuntimas į serverį sprendimui dėl šaltinio legalumo (Variantas IIA). Duomenų bazės pildomos taikant šiuos variantus:
 - Variantas IIA-1: visiškai neautomatizuotas būdas, pildant nelegalių ir legalių šaltinių sąrašus, paremtas skundų gavimu, viešų šaltinių analize, bendradarbiavimu su autorinių teisių turėtojais ir jiems atstovaujančiomis organizacijomis;
 - Variantas IIA-2: pusiau automatizuotas būdas, paremtas „patikimų žymėtojų“ įsitraukimu, pildant nelegalių ir legalių šaltinių sąrašus.
- Funkcinė dalis III: iššokantis langas (Variantas IIIB);
- Funkcinė dalis VI: naudotojas gali pranešti, apie įtartą puslapį.

Vystymo galimybių aprašymas:

- Funkcinė dalis II gali būti papildyta šiais variantais:
 - Variantas IIA-3: visiškai neautomatizuotas būdas, pildant legalių šaltinių sąrašus pagal konkrečius kūrinius, paremtas autorinių teisių turėtojų ir jiems atstovaujančių organizacijų, įsitraukimu;
 - Variantas IIA-4: pusiau automatizuotas būdas, paremtas pačio įrankio nustatytų įtartų šaltinių sąrašų tikrinimu, pildant sąrašus šaltinių, dėl kurių kilę įtarimai pasiteisino (reikalauja Varianto IIB bent dalinio diegimo kartu su Variantu IIA).

ALTERNATYVA A2 – PAGALBININKAS NAUDOTOJUI PROGRAMOS FORMA (BE PAŽANGIŲ ALGORITMŲ, REMIANTIS PANAŠUMO NUSTATYMU)

Išpildoma Koncepcija A: technologinis sprendimas, kuris gebėtų nustatyti, kad naudotojas bando peržiūrėti nelegalų turinį ir informuoti jį. Technologiniame sprendime turėtų būti įgyvendintos nelegalaus turinio nustatymo ir naudotojo informavimo funkcinės dalys. Technologinio sprendimo formatas galėtų būti programa arba naršyklės plėtinys (įskiepis). Technologinį sprendimą naudotojai diegtų savanoriškai. Technologinio sprendimo tikslinės auditorijos – sąmoningi, tačiau nelegalų turinį sunkiai gebantys atskirti naudotojai (vyresnio amžiaus naudotojai ir, apskritai, žemesnį žinių ir įgūdžių lygį turintys naudotojai) bei valstybės institucijų ir viešos prieigos kompiuterius administruojančios institucijos (bibliotekos, mokyklos ir t. t.).

Kitaip nei Alternatyvos A1 atveju, vertinamas ne tik naršymo srautas, bet visa veikla kompiuteryje. Tam reikalinga programos forma.

Realizuojamos funkcinės dalys:

- Funkcinė dalis I: Naršymo srauto atpažinimas naudotojo sistemoje.
- Funkcinė dalis II: Nelegalaus turinio naudotojo naršymo sraute nustatymas.
- Funkcinė dalis III: Vartotojo perspėjimas apie aptiktą nelegalų turinį.
- Funkcinė dalis VI: Pranešimo dėl galimai nelegalaus turinio pateikimo sistema.

Planuojami technologinio išpildymo variantai:

- Funkcinė dalis I: Operacinės sistemos lygmeniu veikianti programa, kompiuteryje arba mobiliame įrenginyje (Variantas O/IB);
- Funkcinė dalis II: serverio, prie kurio jungiasi naudotojo sistema, informacijos siuntimas į serverį sprendimui dėl šaltinio legalumo (Variantas IIA). Duomenų bazės pildomos taikant šiuos variantus:
 - Variantas IIA-1: visiškai neautomatizuotas būdas, pildant nelegalių ir legalių šaltinių sąrašus, paremtas skundų gavimu, viešų šaltinių analize, bendradarbiavimu su autorinių teisių turėtojais ir jiems atstovaujančiomis organizacijomis;
 - Variantas IIA-2: pusiau automatizuotas būdas, paremtas „patikimų žymėtojų“ įsitraukimu, pildant nelegalių ir legalių šaltinių sąrašus.
- Funkcinė dalis III: operacinės sistemos pranešimai (Variantas IIIA);
- Funkcinė dalis VI: naudotojas gali pranešti, apie įtartą puslapį.

Vystymo galimybių aprašymas:

- Funkcinė dalis II gali būti papildyta šiais variantais:
 - Variantas IIA-3: visiškai neautomatizuotas būdas, pildant legalių šaltinių sąrašus pagal konkrečius kūrinius, paremtas autorinių teisių turėtojų ir jiems atstovaujančių organizacijų, įsitraukimu;
 - Variantas IIA-4: pusiau automatizuotas būdas, paremtas pačio įrankio nustatytų įtartų šaltinių sąrašų tikrinimu, pildant sąrašus šaltinių, dėl kurių kilę įtarimai pasiteisino (reikalauja Varianto IIB bent dalinio diegimo kartu su Variantu IIA).

Įgyvendinus šią alternatyvą būtų sukurta didžiulius kiekius asmeninių duomenų renkanti programa, todėl kyla rimtų abejonių dėl naudotojų pasiryžimo įsidiegti tokį sprendimą.

ALTERNATYVA B – LEGALIAUS TURINIO ŠALTINIŲ PAIEŠKOS SVETAINĖ

Išpildoma koncepcija B: technologinis sprendimas, kuris veiktų kaip integruotas paieškos įrankis. Technologiniame sprendime turėtų būti įtrauktos turinio paieškos ir legalaus turinio duomenų bazės (nuosavos ir / arba sąsajos su egzistuojančiomis duomenų bazėmis). Technologinio sprendimo formatas galėtų būti internetinė svetainė arba naršyklės plėtinys (įskiepis). Pasirinkus naršyklės plėtinio (įskiepio) formatą, tokį įskiepį naudotojai diegtų savanoriškai. Technologinio sprendimo tikslinės auditorijos – sąmoningi, tačiau ieškant nelegalų turinį su sunkumais susiduriantys naudotojai. Panašūs sprendimai – JustWatch, Naudoklegaliai.lt.

Realizuojamos funkcinės dalys:

- Funkcinė dalis IV: Legalaus šaltinio paieška.
- Funkcinė dalis V: Legalaus šaltinio duomenų bazė arba sąsajos su tokiomis bazėmis.

Planuojami technologinio išpildymo variantai:

- Išpildymo forma: Internetinė svetainė (Variantas OC);
- Funkcinė dalis IV: pusiau automatizuotas sprendimas, kai sistema tik pasiūlo pradėti paiešką, rodomas laukas paieškos raktažodžių įvedimui (Variantas IVB);
- Funkcinė dalis V: sąsajų su egzistuojančiomis duomenų bazėmis / platformomis sukūrimas per API (• Variantas VA).

Vystymo galimybių aprašymas:

- Funkcinė dalis V gali būti papildyta šiais variantais:
 - Variantas VB: nuosavos duomenų bazės sukūrimas;
 - Variantas VC: DI pasitelkimas legalių šaltinių paieškai.

Įgyvendinant šią alternatyvą būtų sukurtas lietuviškai rinkai pritaikytas JustWatch variantas. Alternatyvą galima įgyvendinti iš esmės išplečiant Naudoklegaliai.lt internetinės svetainės funkcionalumą.

ALTERNATYVA C1 – INTEGRUOTA PLATFORMA NELEGALAUS TURINIO VENGIMUI IR LEGALIAUS TURINIO PAIEŠKAI (JSKIEPIO FORMA)

Išpildoma koncepcija C: technologinis sprendimas, kuris sujungtų prieš tai aprašytas dvi koncepcijas. Pagrindinis skirtumas – toks sprendimas negalėtų veikti vien internetinės svetainės (kaip koncepcija B) formatu – būtinas išpildymas naršyklės įskiepio arba programos formatu.

Realizuojamos funkcinės dalys:

- Funkcinė dalis I: Naršymo srauto atpažinimas naudotojo sistemoje.
- Funkcinė dalis II: Nelegalaus turinio naudotojo naršymo sraute nustatymas.
- Funkcinė dalis III: Vartotojo perspėjimas apie aptiktą nelegalų turinį.
- Funkcinė dalis IV: Legalaus šaltinio paieška.
- Funkcinė dalis V: Legalaus šaltinio duomenų bazė arba sąsajos su tokiais bazėmis.
- Funkcinė dalis VI: Pranešimo dėl galimai nelegalaus turinio pateikimo sistema.

Planuojami technologinio išpildymo variantai:

- Funkcinė dalis I: Įskiepis naršyklėje (Variantas O/IA) ir svetainė (Variantas OC);
- Funkcinė dalis II: serverio, prie kurio jungiasi naudotojo sistema, informacijos siuntimas į serverį sprendimui dėl šaltinio legalumo (Variantas IIA). Duomenų bazės pildomos taikant šiuos variantus:
 - Variantas IIA-1: visiškai neautomatizuotas būdas, pildant nelegalių ir legalių šaltinių sąrašus, paremtas skundų gavimu, viešų šaltinių analize, bendradarbiavimu su autorinių teisių turėtojais ir jiems atstovaujančiomis organizacijomis;
 - Variantas IIA-2: pusiau automatizuotas būdas, paremtas „patikimų žymėtojų“ įsitraukimu, pildant nelegalių ir legalių šaltinių sąrašus.
- Funkcinė dalis III: iššokantis langas (Variantas IIIB);
- Funkcinė dalis IV: pusiau automatizuotas sprendimas, kai sistema tik pasiūlo pradėti paiešką (parodomas laukas paieškos raktažodžių įvedimui). Gražinami rezultatai su nuorodomis, kur galima legaliai žiūrėti konkretų turinio vienetą (Variantas IVB);
- Funkcinė dalis V: sąsajų su egzistuojančiomis duomenų bazėmis / platformomis sukūrimas per API (Variantas VA);
- Funkcinė dalis VI: naudotojas galima pranešti, apie įtartą puslapį.

Vystymo galimybių aprašymas:

- Funkcinė dalis II gali būti papildyta šiais variantais:
 - Variantas IIA-3: visiškai neautomatizuotas būdas, pildant legalių šaltinių sąrašus pagal konkrečius kūrinius, paremtas autorinių teisių turėtojų ir jiems atstovaujančių organizacijų, įsitraukimu;
 - Variantas IIA-4: pusiau automatizuotas būdas, paremtas pačio įrankio nustatytų įtartų šaltinių sąrašų tikrinimu, pildant sąrašus šaltinių, dėl kurių kilę įtarimai pasiteisino (reikalauja Varianto IIB bent dalinio diegimo kartu su Variantu IIA).
- Funkcinė dalis V gali būti papildyta šiais variantais:
 - Variantas VB: nuosavos duomenų bazės sukūrimas;
 - Variantas VC: DI pasitelkimas legalių šaltinių paieškai.

Įgyvendinus šią alternatyvą, būtų sukurtas alternatyvų A1 ir B hibridas. Iš vienos pusės tai reikštų, kad technologinis sprendimas būtų patogesnis naudotojui, siūlytų didesnį spektrą funkcijų. Iš kitos pusės, technologinio sprendimo įgyvendinimo ir palaikymo sąnaudos būtų didesnės.

ALTERNATYVA C2 – INTEGRUOTA PLATFORMA NELEGALAUS TURINIO VENGIMUI IR LEGALIAUS TURINIO PAIEŠKAI (PROGRAMOS FORMA)

Išpildoma koncepcija C: technologinis sprendimas, kuris sujungtų prieš tai aprašytas dvi koncepcijas. Pagrindinis skirtumas – toks sprendimas negalėtų veikti vien internetinės svetainės (kaip koncepcija B) formatu – būtinas išpildymas naršyklės įskiepio arba programos formatu.

Realizuojamos funkcinės dalys:

- Funkcinė dalis I: Naršymo srauto atpažinimas naudotojo sistemoje.
- Funkcinė dalis II: Nelegalaus turinio naudotojo naršymo sraute nustatymas.
- Funkcinė dalis III: Vartotojo perspėjimas apie aptiktą nelegalų turinį.
- Funkcinė dalis IV: Legalaus šaltinio paieška.
- Funkcinė dalis V: Legalaus šaltinio duomenų bazė arba sąsajos su tokiomis bazėmis.
- Funkcinė dalis VI: Pranešimo dėl galimai nelegalaus turinio pateikimo sistema.

Planuojami technologinio išpildymo variantai:

- Funkcinė dalis I: Operacinės sistemos lygmeniu veikianti programa, kompiuteryje arba mobiliame įrenginyje (Variantas O/IB) ir svetainė (Variantas OC);
- Funkcinė dalis II: serverio, prie kurio jungiasi naudotojo sistema, informacijos siuntimas į serverį sprendimui dėl šaltinio legalumo (Variantas IIA). Duomenų bazės pildomos taikant šiuos variantus:
 - Variantas IIA-1: visiškai neautomatizuotas būdas, pildant nelegalių ir legalių šaltinių sąrašus, paremtas skundų gavimu, viešų šaltinių analize, bendradarbiavimu su autorinių teisių turėtojais ir jiems atstovaujančiomis organizacijomis;
 - Variantas IIA-2: pusiau automatizuotas būdas, paremtas „patikimų žymėtojų“ įsitraukimu, pildant nelegalių ir legalių šaltinių sąrašus.
- Funkcinė dalis III: operacinės sistemos pranešimai (Variantas IIIA);
- Funkcinė dalis IV: pusiau automatizuotas sprendimas, kai sistema tik pasiūlo pradėti paiešką (parodomas laukas paieškos raktažodžių įvedimui). Gražinami rezultatai su nuorodomis, kur galima legaliai žiūrėti konkretų turinio vienetą (Variantas IVB);
- Funkcinė dalis V: sąsajų su egzistuojančiomis duomenų bazėmis / platformomis sukūrimas per API (Variantas VA);
- Funkcinė dalis VI: naudotojas gali pranešti, apie įtartą puslapį.

Vystymo galimybių aprašymas:

- Funkcinė dalis II gali būti papildyta šiais variantais:
 - Variantas IIA-3: visiškai neautomatizuotas būdas, pildant legalių šaltinių sąrašus pagal konkrečius kūrinius, paremtas autorinių teisių turėtojų ir jiems atstovaujančių organizacijų, įsitraukimu;
 - Variantas IIA-4: pusiau automatizuotas būdas, paremtas pačio įrankio nustatytų įtartinų šaltinių sąrašų tikrinimu, pildant sąrašus šaltinių, dėl kurių kilę įtarimai pasiteisino (reikalauja Varianto IIB bent dalinio diegimo kartu su Variantu IIA).
- Funkcinė dalis V gali būti papildyta šiais variantais:
 - Variantas VB: nuosavos duomenų bazės sukūrimas;
 - Variantas VC: DI pasitelkimas legalių šaltinių paieškai.

Įgyvendinus šią alternatyvą, būtų sukurtas alternatyvų A2 ir B hibridas. Iš vienos pusės tai reikštų, kad technologinis sprendimas būtų patogesnis naudotojui, siūlytų didesnį spektrą funkcijų. Iš kitos pusės, technologinio sprendimo įgyvendinimo ir palaikymo sąnaudos būtų didesnės.

Įgyvendinus šią alternatyvą būtų sukurta didžiulius kiekius asmeninių duomenų renkanti programa, todėl kyla rimtų abejonių dėl naudotojų pasiryžimo įsidiesti tokį sprendimą.

Toliau pateiktame skyriuje šios alternatyvos yra palyginamos, suformuluojamas pasiūlymas dėl optimalios alternatyvos. Pažymėtina, kad galutinį sprendimą dėl pasirinktos alternatyvos priima Užsakovas.

2.5. Optimalaus technologinio sprendimo Lietuvos atvejui pasirinkimas

Šiame skyriuje yra analizuojamos 2.4.4. skyriuje išskirtos alternatyvos. Aprašomos alternatyvų stipriosios ir silpnosios pusės, jos palyginamos remiantis 2.1. skyriuje nurodyta metodika.

ALTERNATYVA A1 „PAGALBININKAS NAUDOTOJUI ĮSKIEPIO FORMA“. Pirmajame etape būtų alternatyva realizuojama kaip įskiepis, kurį sąmoningi naudotojai galėtų įsidiegti į savo naršyklės. Įskiepis stebėtų svetaines, kuriuose lankosi naudotojas ir lygintų šių svetainių informaciją su prieinamomis duomenų bazėmis, kurių pagrindą sudarytų LRTK duomenų bazės, nekomercinės nelegalaus turinio duomenų bazės (pavyzdžiui – Lumen) bei kiti patikimi informacijos šaltiniai. Įskiepio pranašumas – įspėjimas naudotojui galėtų būti pradėtas rodyti greičiau, negu LRTK atlieka blokavimo procedūras. Įskiepis taip pat leistų sąmoningiems naudotojams patogesne forma pateikti pranešimą LRTK dėl galimai nelegalų turinį skleidžiančios internetinės svetainės, paspaudę tam skirtą mygtuką. Būtina realizuoti vidinę reputacijos ir išorinę naudotojo skatinimo sistemą. Turėtų būti sekama konkretaus vartotojo pranešimų kokybė (ar pranešimas pasitvirtina), aukštos reputacijos pranešimai turėtų būti vertinami prioriteto tvarka. Vartotojui turėtų būti pranešama apie tai, kad jo skundas padėjo užblokuoti puslapį – tokiu būdu būtų skatinama toliau teikti pranešimus. Tam, kad būtų galima realizuoti šią sistemą, būtina sukurti naudotojų paskyrų sistemą. Atsižvelgiant į renkamos informacijos jautrumą, būtina sukurti galimybę laikinai išjungti įskiepi, o jam veikiant – užtikrinti j serverį perduodamų duomenų saugumą ir konfidencialumą.

Vėliau alternatyvą būtų galima plėsti įdiegiant algoritmus, kurie automatiškai vertintų, ar internetinėse svetainėse, kuriuos lanko naudotojas, gali būti nelegalaus turinio. Tokios internetinės svetainės turėtų būti automatiškai perduodami papildomam tikrinimui. Šių funkcijų realizavimui būtų tikslinga taikyti DI algoritmus (arba realizuoti sąsają su egzistuojančiomis DI platformomis).

Papildomai būtų galima plėsti autorinių teisių turėtojų arba jų atstovų teises ir įsitraukimą, leidžiant deklaruoti ribotą sąrašą internetinių svetainių, kur jų turinys galėtų būti peržiūrimas legaliai. Jeigu sistema nustatytų, kad tokį turinį naudotojas bando peržiūrėti kitur – būtų siunčiamas pranešimas apie galimai neteisėtą turinio platinimą.

ALTERNATYVA A2 „PAGALBININKAS NAUDOTOJUI PROGRAMOS FORMA“. Ši alternatyva skirtųsi tik savo forma – būtų realizuota operacinės sistemos lygmeniu veikiančios programos forma. Tai turi vieną rimtą pranašumą – galima stebėti ne tik veiklą naršyklėje, bet ir kitose programose. Iš kitos pusės ši alternatyva pasižymi labai rimta problema – naudotojas turėtų suteikti prieigą prie visos veiklos savo įrenginyje. Kyla rimtų abejonių, ar pakankamai didelis skaičius naudotojų sutiktų tai padaryti. Iš tokios sistemos kūrėjų pusės, kyla rimtų rizikų užtikrinant j serverį siunčiamų duomenų saugumą ir konfidencialumą. Galiausiai, tokios sistemos sukūrimas būtų ženkliai brangesnis, nei kitų alternatyvų. Dabartiniame Studijos kūrimo etape kainą yra sudėtinga nustatyti, tačiau kaina galėtų viršyti 1 mln. Eur.

ALTERNATYVA B „LEGALIAUS TURINIO ŠALTINIŲ PAIEŠKOS SVETAINĖ“. Ši alternatyva iš esmės plėstų Naudoklegaliai.lt svetainės funkcionalumą. Įgyvendinus šią alternatyvą turėtų būti pasiektas JustWatch naudotojo patirties lygis – sistema turėtų leisti ieškoti konkretaus kūrinio peržiūros legalių šaltinių, rodytų ne tik šaltinius, bet ir naudojimosi jomis sąlygas, kainas. Tokia svetainė pradiniuose etapuose galėtų veikti per sąsajas su egzistuojančiomis svetainėmis (pavyzdžiui, JustWatch) arba lietuviško legalaus turinio pagrindinėmis platformomis – Go3 ir kiti.

Ši alternatyva nepadėtų naudotojui atskirti legalų ir nelegalų turinį, tačiau suteiktų galimybę ieškoti tik tarp legalių šaltinių.

Vystant šią alternatyvą reikėtų sukurti galimybę legalių mažiau žinomų platformų savininkams prijungti savo platformas prie sistemos. Siekiant aktyviai plėsti sąrašą svetainių, kur legalus turinys yra prieinamas, gali tekti pradėti vystyti savo duomenų bazes, tam panaudojant interneto skanavimo sprendimus.

ALTERNATYVA C1 „INTEGRUOTA PLATFORMA NELEGALIAUS TURINIO VENGIMUI IR LEGALIAUS TURINIO PAIEŠKAI“. Alternatyva sujungia A1 ir B alternatyvų funkcijas, naudojamas technologijas. Būtų realizuotas tiek įskiepis, tiek svetainė. Įskiepis savyje integruotų svetainės funkcijas, leistų naudojant įskiepi atlikti legalių šaltinių arba norimo kūrinio legalaus šaltinio paiešką. Tokia alternatyva pasižymėtų abiejų alternatyvų stipriosiomis pusėmis, tačiau iš esmės dviejų alternatyvų vystymas reikalautų didesnių pradinių investicijų.

ALTERNATYVA C2 „INTEGRUOTA PLATFORMA NELEGALAUS TURINIO VENĖIMUI IR LEGALIAUS TURINIO PAIEŠKAI“. Alternatyva sujungia A2 ir B alternatyvų funkcijas, naudojamas technologijas. Pagrindinis trūkumas susidarytų dėl A2 alternatyvos trūkumų.

5 lentelė. Technologinio sprendimo alternatyvų vertinimas ir palyginimas

| Vertinimo kriterijai | Alternatyva A1 „Pagalbininkas naudotojui įskiepio forma“ | Alternatyva A2 „Pagalbininkas naudotojui programos forma“ | Alternatyva B „Legalaus turinio šaltinių paieškos svetainė“ | Alternatyva C1 „Integruota platforma nelegalaus turinio vengimui ir legalaus turinio paieškai (įskiepis)“ | Alternatyva C2 „Integruota platforma nelegalaus turinio vengimui ir legalaus turinio paieškai (programa)“ |
|--|--|--|--|--|--|
| Sudėtingumas, rizikos dėl negebėjimo technologškai išpildyti | Nesudėtingas pirminiuose etapuose, tačiau vystant sprendimą bus pasiektas sudėtingas lygis (dėl DI integracijos) | Sudėtingas | Nesudėtingas pirminiuose etapuose, tačiau vystant sprendimą bus pasiektas sudėtingas lygis (dėl DI integracijos) | Nesudėtingas pirminiuose etapuose, tačiau vystant sprendimą bus pasiektas sudėtingas lygis (dėl DI integracijos) | Sudėtingas |
| Pradinės investicijos | Teigiamai (investicijos 70–120 tūkst. Eur), tačiau reikalingos investicijos didėtų vystant sprendimą | Neigiamai (reikalingos investicijos gali viršyti 1 mln. Eur) | Teigiamai (investicijos iki 300 tūkst. Eur), tačiau reikalingos investicijos didėtų vystant sprendimą | Vidutiniškai (investicijos iki 500 tūkst. Eur), tačiau reikalingos investicijos didėtų vystant sprendimą | Neigiamai (reikalingos investicijos gali viršyti 1 mln. Eur) |
| Palaikymo sudėtingumas, palaikymo išlaidos | Pradžioje žemos , tačiau plečiant funkcijas palaikymo sąnaudos didėtų | Didesnės palaikymo sąnaudos dėl didesnio apdorojamo srauto | Pradžioje žemos , tačiau plečiant funkcijas palaikymo sąnaudos didėtų | Vidutinės , laikui bėgant didėjančios | Didesnės palaikymo sąnaudos dėl didesnio apdorojamo srauto |
| Ar padeda naudotojui atskirti nelegalų turinį? | Taip | Taip | Ne | Taip | Taip |
| Ar padeda naudotojui rasti legalius šaltinius? | Ne | Ne | Taip | Taip | Taip |
| Vartotojo patirtis | Vertinama teigiamai , tačiau daliai naudotojų gali būti nepriimtina dalintis naršymo istorija | Vertinama neigiamai , nes naudotojui reikės pasidalinti dideliu kiekiu konfidencialių duomenų su administruojančia organizacija | Vertinama teigiamai , tačiau priklauso nuo išpildymo | Vertinama teigiamai , tačiau priklauso nuo išpildymo | Vertinama neigiamai , nes naudotojui reikės pasidalinti dideliu kiekiu konfidencialių duomenų su administruojančia organizacija |

Šaltinis: parengta Konsultanto

Atsižvelgiant į prieš tai pateiktą vertinimą, siūloma atsisakyti alternatyvų A2 ir C1. Šios alternatyvos pasižymi didžiausiomis rizikomis (bandoma sukurti ypač sudėtingą sistemą, kurios koncepcija gali būti nepriimtina didelei daliai naudotojų) ir didžiausiomis pradinėmis sąnaudomis.

Užsakovui siūloma rinktis vystyti vieną iš trijų alternatyvų – A1, B, C1.

Rekomenduojama tarp trijų alternatyvų pasirinkti vieną priklausomai nuo Užsakovo prioritetų šiose srityse:

- **Projekto biudžetas** – visos trys alternatyvos gali būti veiksmingas būdas skatinti bent dalį visuomenės vengti nelegalaus turinio, tačiau biudžetas gali priversti pasirinkti pigesnę alternatyvą. Bendrai, siūloma pradžioje prioretizuoti pasirinktos alternatyvos išpildymo kokybę ir investuoti į viešinimą, o ne stengtis išpildyti kuo didesnį skaičių funkcijų;

- **Teisinės rizikos** – apie nelegalų turinį perspėjantis įskiepis (alternatyvos A1 ir iš dalies C1) gali būti susijęs su teisinėmis rizikomis, nes per klaidą įtraukus svetainę į nelegalių svetainių sąrašą gali būti susidurta su tokios svetainės savininkų ieškiniais. Papildomai, aktyvesnė kova su nelegaliomis svetainėmis gali lemti, kad tokių svetainių savininkai gali pradėti aktyviai veikti prieš sukurtą sprendimą, taip pat ir išnaudojant teisinius įrankius. Jeigu Užsakovas yra jautrus teisinėms rizikoms, rekomenduojama pasirinkti alternatyvą B.
- **Sprendžiamų problemų prioretizavimas** – jeigu dėl biudžeto ar kitų apribojimų nebus pasirinkta Alternatyva C1, pasirinkimą tarp A1 ir B gali lemti pirmenybės suteikimas sprendžiamai problemai. Alternatyva A1 pirmiausiai sprendžia problemą, kai dalis naudotojų negeba atskirti legalaus ir nelegalaus turinio. Alternatyva B dalinai sprendžia tą pačią problemą, bet labiau sprendžia legalių šaltinių fragmentacijos (yra daug legalių šaltinių, tačiau konkretūs norimas turinys gali būti tik viename iš jų) problemą. Pasirinkimą gali lemti Užsakovo noras prioretizuoti pirmą arba antrą problemą.

Antrame Studijos kūrimo etape pasirinkta alternatyva būtų detaliau nagrinėjama iš techninės, naudotojų patirties, rinkos galimybių išpildyti alternatyvą, pusės. Papildomai būtų nagrinėjami teisiniai niuansai, administravimo klausimai. Galiausiai būtų atlikta sąnaudų–naudos analizė, galutiniam sprendimui dėl kuriamo technologinio sprendimui priimti.

3. Atrinktos alternatyvos konkretizavimas

Užsakovo sprendimu buvo pasirinkta A1 alternatyva „Pagalbininkas naudotojui įskiepio forma“, todėl toliau bus pateikiama šios alternatyvos detalesnė analizė.

Skyriuje pirmiausia nagrinėjamas jautriausias klausimas – asmens duomenų rinkimas ir apsauga. Atsižvelgiant į analizės rezultatus toliau skyriuje konkretizuojami Technologinio sprendimo techniniai aspektai, plėtos galimybės ir atliekama Technologinio sprendimo SNA.

Tuomet skyriuje atliekamos papildomos analizės – nustatomas Technologinio sprendimo administravimo modelis ir atliekama Lietuvos IT sprendimų kūrėjų rinkos analizė.

Skyriaus analizė leido paruošti Studijos priedą – Technologinio sprendimo sukūrimo techninę specifikaciją.

3.1. Asmens duomenų rinkimas ir apsauga

Šiuolaikinėje skaitmeninėje erdvėje vis aktyviau diegiami įvairūs technologiniai įrankiai, veikiantys virtualioje aplinkoje. Sprendžiantys įvairias problemas ir teikiantys paslaugas įrankiai yra neatsiejami nuo sąveikos su naudotojo duomenimis. Tokie sprendimai dažnai reikalauja analizuoti individualius asmenų elgsenos, veiklos ar turinio sąveikos duomenis, o tai neišvengiamai įpareigoja kūrėjus laikytis duomenų saugos teisinių nuostatų ir gerųjų technologijų taikymo praktikų.

Kalbant apie teises nuostatas, ypač svarbus vaidmuo čia tenka 2016 m. Europos Parlamento ir Tarybos reglamentui (ES) 2016/679 – visoje ES taikomam Bendrojo duomenų apsaugos reglamentui (toliau – BDAR), kuris nustato asmens duomenų apsaugos principus.

Kalbant apie technologijų taikymo gerąsias praktikas, būtina užtikrinti, kad Technologinis sprendimas būtų kuriamas teikiant prioritetą duomenų saugumui visuose lygmenyse – neapsiribojant šifravimo algoritmų taikymu, pati sistemos architektūra turi būti kuriama siekiant minimizuoti duomenų saugumo rizikas.

BDAR

Kuriant bet kokios formos skaitmeninėje erdvėje veikiantį įrankį, kurio tikslas analizuoti su individualiais asmenimis susijusius duomenis, būtina remtis 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (ES) 2016/679 nuostatomis.⁷⁵

Pirmiausia tam, jog duomenų tvarkymas būtų laikomas teisėtu, turi būti taikoma bent viena iš BDAR reglamente 6 straipsnyje nurodytų sąlygų. Duomenų tvarkymo procesas negali peržengti duomenų apdorojimo masto, kuris yra nurodomas BDAR reglamente. Dažniausiai šiuo atveju tai yra naudotojo sutikimas arba valdytojo teisėtas interesas. Kadangi, įskiepis yra savanoriška, ne privaloma funkcija, šiuo atveju pakaktų duomenų subjekto duoto sutikimo, kad jo asmens duomenys būtų tvarkomi vienu ar keliais konkrečiais tikslais. Asmens duomenų subjektai turi būti skaidriai informuojami apie duomenų tvarkymo tikslus, teisinį pagrindą, saugojimo laikotarpį, galimus duomenų gavėjus ir savo teises. Informacija turi būti pateikiama aiškiai, išskiriant esmę. Naudotojo sutikimas leisti apdoroti duomenis galėtų būti pateikiamas tokiu būdu – įskiepio diegimo metu – pateikti elektroninę nuorodą į privatumo politiką ar sutikimo formą, kurioje naudotojas galėtų pažymėti savo sutikimą/nesutikimą duomenų apdorojimui. Be to, turėtų būti užtikrinama naudotojo teisė į prieigą prie duomenų, jų taisymą, ištrynimą („teisė būti pamirštam“) ir duomenų tvarkymo apribojimą.

Remiantis 5 straipsniu, įskiepio funkcionalumas turi būti paremtas duomenų kiekio mažinimo principu, t. y. turi būti renkama tik tiek duomenų, kiek yra būtina – pavyzdžiui, IP adresus, svetainės URL ar atitinkamas turinio

⁷⁵ Europos Parlamento ir Tarybos reglamentas (ES) 2016/679, 2016 m. balandžio 27 d. dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas). Prieiga internetu: <https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:32016R0679>

žymos, vengiant perteklinės informacijos apie naudotojo elgseną ar tapatybę. Patariama, jog asmeniniai duomenys, neturėtų būti renkami, o taip pat nėra matomas tų duomenų poreikis paskyrų kūrimo procesui, bent jau pradinėse įskiepio stadijose. Duomenų saugumo požiūriu, 32 straipsnis įpareigoja diegti tinkamas technines ir organizacines priemones – duomenų šifravimą, prieigos valdymą, audito įrašus ir reakcijas į saugumo pažeidimus procedūras, atitinkančias šiuolaikinius informacijos saugos standartus. Tuo atveju, jei būtų įvykęs asmens duomenų saugumo pažeidimas, 33 straipsnis numato pareigą per 72 valandas pranešti priežiūros institucijai, o 34 straipsnis – ir pačiam duomenų subjektui, jei rizika jo teisėms yra didelė. Todėl geriausia laikytis minimalaus duomenų kaupimo, apdorojimo principo.

Atsižvelgiant į tai, kad įskiepis automatiškai gali apdoroti naudotojo veiklos, potencialiai susijusios su jautriomis temomis (politinėmis, religinėmis pažiūromis, seksualine orientacija), informaciją, būtina įvertinti galimą specialių kategorijų duomenų apdorojimą. Pagal 9 straipsnį, tokių duomenų tvarkymas yra griežtai draudžiamas, nebent yra aiškus, informuotas ir išreikštas sutikimas arba kita reglamento numatyta išimtis. Šiuo atveju rekomenduojama iš anksto techninėmis priemonėmis taikyti anonimizaciją. Taigi, BDAR taikymas siekia užtikrinti duomenų subjekto atžvilgiu tvarkomus duomenis teisėtu, sąžiningu ir skaidriu būdu (teisėtumo, sąžiningumo ir skaidrumo principas). Kadangi įskiepis apima daugiasluoksnią atitikties sistemą: nuo teisinio pagrindo ir duomenų rinkimo ribojimo iki naudotojų informavimo, duomenų saugos priemonių diegimo, šių principų laikymasis yra ne tik būtinas norint išvengti sankcijų ar grėsmės reputacijai, bet ir kritiškai svarbus siekiant užtikrinti technologijų etišką taikymą, naudotojų pasitikėjimą ir pagarbą jų fundamentalioms teisėms į privatumą.

TECHNOLOGINIAI ASPEKTAI

Vertinant technologinius aspektus svarbiausia laikytis principo, kad asmeniniai duomenys yra siunčiami į serverį tik tais atvejais, kai to negalima išvengti. Prie tokių duomenų galima priskirti asmens duomenis, naršymo internete istoriją.

Jeigu nėra galimybės to išvengti, reikėtų naudoti skirtingus maišos algoritmus, kurie apsunkina siunčiamos informacijos dekodavimą neautorizuotiems naudotojams, o autorizuotieji naudotojai galėtų neįsankcionuoti tokius veiksmus atlikti tik įdėję nemenką darbą.

Galiausiai, visi asmeniniai duomenys serveryje neturėtų būti saugomi ilgiau, nei yra būtina. Pavyzdžiui, net taikant maišos algoritmus užkoduoti duomenys neturėtų būti saugomi neribotą laiką, jeigu jie nebėra reikalingi. Būtina užtikrinti algoritmų, kurie automatiškai pašalina tokius nebereikalingus duomenis, darbą.

Pasirinktos A1 alternatyvos kontekste tai reiškia 2 galimus išpildymo būdus:

- Nesiųsti naudotojo naršymo istorijos į serverį patikrai, o atvirkščiai, lokaliai naudotojo aplinkoje saugoti nelegalių ir legalių svetainių sąrašų kopijas. Tokiu atveju iš naudotojo įskiepio į serverį būtų kreipiamasi tik tikrinant, ar atsirado atnaujinta sąrašo versija ir norint pateikti pranešimą dėl pastebėto galimai nelegalaus turinio;
- Siųsti užklausos dėl atidarytos svetainės duomenis tik pritaikius maišos algoritmus. Serverio pusėje, duomenų bazėje saugoti nelegalių ir legalių svetainių sąrašus taip pat pritaikius maišos algoritmus ir tikrinti maišos reikšmes.

Pirmas variantas (lokalus nelegalių ir legalių svetainių sąrašų kopijų saugojimas) yra pranašesnis duomenų apsaugos prasme, tačiau turi apribojimų:

- Negalima saugoti ypač didelių duomenų bazių lokaliai – didelės duomenų bazės dydis gali siekti gigabaitus arba net terabaitus. Net vienkartinis tokių bazių parsisiuntimas būtų per daug nepatogus naudotojui, ne visos sistemos galėtų sutalpinti tokio dydžio duomenų bases. Todėl toks variantas būtų tinkamas tik jeigu nelegalių ir legalių svetainių sąrašai nebūtų didesni nei keletas megabaitų;
- Negalima per dažnai atnaujinti tokių sąrašų (nebent duomenų bazės dydis ypač mažas) – per dažnas net santykinai nedidelių duomenų bazių atnaujinimas lemtų sulėtėjusią naršymo patirtį. Nors vienkartiniai sulėtėjimai nesukeltų didelių problemų ir greičiausiai nebūtų pastebėti naudotojo, tačiau nuolatinis atnaujinimas būtų pastebimas. Todėl toks variantas būtų tinkamas, jeigu sąrašai nebūtų atnaujinami dažniau nei kelis kartus per dieną.

Dėl pirmojo varianto pranašumo duomenų apsaugos srityje toliau 3 skyriuje pristatomas Technologinio sprendimo aprašymas remiasi pirmuoju variantu – naršyklės įskiepis nesiųstų naršymo istorijos į serverio pusę, o serveris siųstų nelegalių ir legalių šaltinių sąrašus naudotojui lokaliai saugojimui. Šis variantas tinkamai veiktų tol, kol Technologinis sprendimas nesiektų padengti viso pasaulio nelegalias svetaines, o tik tas, kurios yra aktualios Lietuvai (t.y. nebūtų siekiama į sąrašus įtraukti svetainių, kuriose nesilanko Lietuvos naudotojai). Priešingu atveju tikėtina, kad nelegalių ir legalių svetainių sąrašai būtų per dideli. Jeigu dėl šios ar kitokios priežasties sąrašai taptų per dideli, tekstų pilnai arba dalinai keisti Technologinio sprendimo išpildymą realizuojant antrą variantą (maišos algoritmų taikymas).

Papildomai verta paminėti, kad svarbi yra ne tik objektyvi duomenų saugumo ir apsaugos situacija, bet ir subjektyvus naudotojo vertinimas. Dėl šios priežasties reikėtų užtikrinti, kad duomenų apsaugai jautresni naudotojai turėtų galimybę pasinaudoti toliau išdėstytais funkcionalumais:

- Turėtų galimybę patogiai ir greitai išjungti naršyklės įskiepi;
- Turėtų galimybę naudotis Technologiniu sprendimu be naudotojo paskyros.

Bendrai nagrinėjant Technologinio sprendimo funkcionalumą kyla abejonių dėl paskyrų poreikio. Paskyrų sistema nėra būtina nei vienam iš funkcionalumų išpildyti (nors pranešimų srauto valdymas galėtų būti pažangesnis su paskyrų sistema, tačiau turint omenyje nedidelį naudotojų skaičių pirmose versijose, paskyrų sistemos sukūrimas nėra tikslingas). Norint užtikrinti didesnę subjektyvų anonimiškumą ir supaprastinti naudotojų prisijungimą prie sistemos, siūloma pradžioje nerealizuoti paskyrų sistemos paprastiems naudotojams.

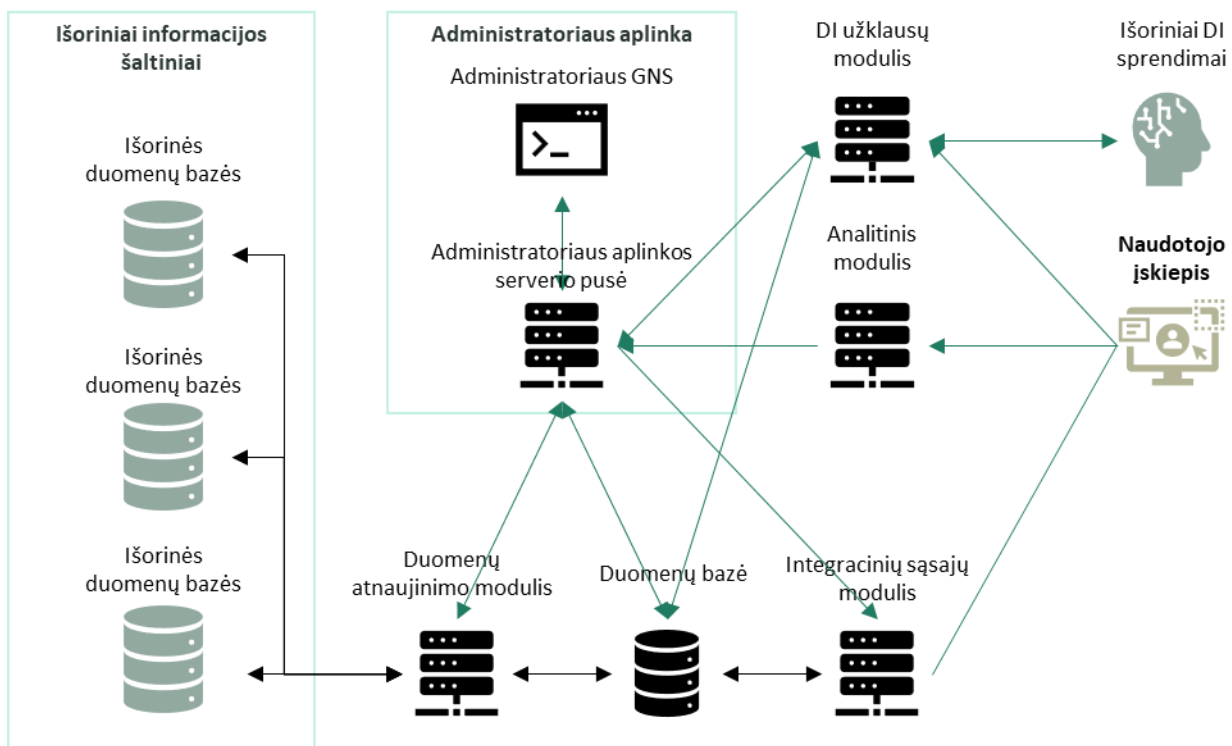
3.2. Technologinio sprendimo aprašymas ir plėtros galimybės

Šiame skyriuje aprašomas Technologinis sprendimas. Šis skyrius suskirstytas į šiuos poskyrius:

- Technologinio sprendimo aprašymas;
- Technologinio sprendimo plėtros ir atnaujinimo galimybių aprašymas;
- Technologinio sprendimo įgyvendinimo sąnaudų–naudos analizė.

3.2.1. Technologinio sprendimo aprašymas

Šiame poskyryje aprašomos pasirinktos alternatyvos funkcinės architektūros dalys.



16 paveikslas. Principinė Technologinio sprendimo schema
Šaltinis: sudaryta Konsultanto

Technologinį sprendimą sudaro 6 principinės dalys, per serverį jos sąveikauja su išorinėmis duomenų bazėmis ir DI sprendimais (žr. prieš tai pateiktą paveikslą). Pažymėtina, kad išorinės duomenų bazės yra abstrakti sąvoka apibūdinti išorinius informacijos šaltinius. Šios dalys:

1. Naudotojo įskiepis. Įskiepis, kuris veikia naudotojo įrenginyje. Įskiepyje vyks nelegalų turinį plintančių svetainių paieška;
2. Administratoriaus aplinka (administratoriaus aplinkos grafinė dalis (toliau – GNS) ir administratoriaus aplinkos serverio pusė);
3. Integracinių sąsajų modulis (atsakingas už informacijos pateikimą naudotojų įskiepiams ir užklausų iš naudotojų įskiepių gavimą);
4. Duomenų bazė (saugomi duomenys, atnaujinami iš išorinių duomenų šaltinių arba rankiniu būdu);
5. Duomenų atnaujinimo modulis, skirtas užtikrinti sąsajas tarp kuriamos sistemos ir išorinių informacijos šaltinių;
6. DI užklausų modulis, skirtas užtikrinti integraciją su išorinėmis DI sistemomis bei bendrai užtikrinti su DI susijusių funkcionalumų tinkamą veikimą.

Atsižvelgiant į 3.1. skyriuje pateikiamą informaciją, naudotojo naršymo patirties sulginimas su nelegalų ir legalų turinį plintančių svetainių sąrašu įvyksta lokaliai, naudotojo įskiepyje. Įskiepis sulgina atidaryto puslapio mazgo

pavadinimą (angl. *hostname*) su lokaliai saugomu sąrašu. Jeigu nustatomas sutapimas, atvaizduojamas grafinis rezultatas (grafinis pranešimas naudotojui) ir pateikiamas į analitinį modulį (pateikiama informacija apie svetainę, kurioje apsilankyta, naudotojo įskiepio unikalus kodas, kita administratoriaus aplinkoje nustatyta informacija). Jeigu nelegalių ir legalių svetainių sąrašas nėra įrašo apie tokią svetainę, naudotojui paaiškinama, kad atsakymo nėra ir pasiūloma pateikti pranešimą apie įtartinį puslapį arba kreiptis į DI (žr. detalesnį paaiškinimą toliau).

Nelegalių ir legalių svetainių sąrašas (kur saugomas puslapio mazgo pavadinimas, angl. *hostname*) sudaromas remiantis šiais šaltiniais:

- Nelegalios svetainės – remiantis LRTK teikiamais duomenimis (LRTK duomenų bazė, išorinis informacijos šaltinis). Kaip papildomas informacijos šaltinis galėtų būti naudojama Lumen duomenų bazė, tačiau šios duomenų bazės informacija turėtų būti filtruojama, nes joje taip pat yra puslapių, kurie nėra aktualūs Lietuvai;
- Legalios svetainės – turėtų būti sudaromas Technologinio sprendimo administratorių, remiantis Naudoklegaliai.lt platformos informacija.

Siekiant užtikrinti, kad naudotojo įskiepis turėtų naujausią informaciją pasikeitus nelegalių ir legalių svetainių sąrašui, administratoriaus aplinkoje nustatyti dažniu įskiepis siunčia užklausas į integracinių sąsajų modulį naujai sąrašo versijai gauti. Dažnis turėtų būti nustatomas atsižvelgiant į faktinį nelegalių ir legalių svetainių sąrašo atnaujinimą, rekomenduojamas dažnis – 1 kartą per parą.

Įskiepis pateikia tokius rezultatus priklausomai nuo nelegalių ir legalių svetainių sąrašo ir lankomo puslapio suliginimo rezultato:

- Jeigu puslapio mazgo pavadinimas (angl. *hostname*) pilnai sutampa su įrašu nelegalių ir legalių svetainių sąrašas, kuris pažymėtas kaip „nelegalaus turinio šaltinis“ naudotojui grąžinamas scenarijus „Aptiktas nelegalus šaltinis“. Pavyzdžiui, į nelegalių svetainių sąrašą įtrauktas „filmai.org“ ir naudotojas lankosi svetainėje, kurio mazgo pavadinimas „filmai.org“ (pilnas adresas „<https://filmai.org/>“);
- Jeigu puslapio mazgo pavadinimas (angl. *hostname*) pilnai sutampa įrašu nelegalių ir legalių svetainių sąrašas, kuris pažymėtas kaip „legalus turinio šaltinis“ naudotojui grąžinamas scenarijus „Aptiktas legalus šaltinis“. Pavyzdžiui, į nelegalių svetainių sąrašą įtrauktas „epika.lrt.lt“ ir naudotojas lankosi puslapyje, kurio mazgo pavadinimas „epika.lrt.lt“ (pilnas adresas „<https://epika.lrt.lt/>“);
- Jeigu lankomo puslapio adresas nėra įtrauktas į nelegalių ir legalių svetainių sąrašą, naudotojui grąžinamas scenarijus „Puslapis nėra įtrauktas į sąrašus“. Pavyzdžiui, naudotojas lankosi svetainėje, kurios mazgo pavadinimas „france24.fr“ (pilnas adresas „<https://france24.fr/>“).

Visi 3 scenarijai atvaizduojami toliau pateiktame 17 paveiksle.

Esant scenarijui „Aptiktas nelegalus šaltinis“, naudotojas informuojamas pasikeičiančiu įskiepio logotipu arba pranešimu ir iššokančiu įskiepio langu (jeigu tokią galimybę palaiko platforma). Naudotojui paaiškinama, kad, remiantis LRTK arba kitu naudojamu informacijos šaltiniu, svetainė, kurioje jis lankosi, yra naudojama nelegalaus turinio sklaidai.

Esant scenarijui „Aptiktas legalus šaltinis“, naudotojas informuojamas pasikeičiančiu įskiepio logotipu. Pranešimai ir iššokantys langai šiame scenarijuje nėra naudojami, nes tokie dažni pranešimai blogintų naudotojo patirtį (angl. *UX*).

Esant scenarijui „Puslapis nėra įtrauktas į sąrašus“, naudotojas informuojamas pasikeičiančiu įskiepio logotipu. Pranešimai ir iššokantys langai šiame scenarijuje nėra naudojami, nes tokie dažni pranešimai blogintų naudotojo patirtį (angl. *UX*). Langą naudotojas turėtų atidaryti pats, paspausdamas ant įskiepio logotipo. Lange naudotojui paaiškinama, kad jo lankomas puslapis nėra įtrauktas į legalių arba nelegalių svetainių sąrašą. Naudotojas kviečiamas pateikti pranešimą apie galimai nelegalų turinį skleidžiančią svetainę, jeigu svetainė jam atrodo nepatinkama. Naudotojui taip pat pasiūloma pasinaudoti galimybe suformuoti užklausą DI platformai. Pateikus tokią užklausą, grąžinamas rezultatas skalėje nuo 0 iki 10 – įvertinimas, kiek konkreti svetainė DI platformai pasirodė įtartina arba rezultatas „DI platforma negalėjo pateikti atsakymo“.

Automatizuotos užklauskos DI funkcija realizuojama sukuriant DI užklauskų modulį serverio pusėje. Modulio paskirtis – gavus naudotojo užklausą dėl kreipimosi į DI suformuoti užklausą duomenų basei, kurioje yra saugoma informacija apie ankstesnes visų naudotojų užklauskas DI funkcijai ir DI atsakymus į atliktas užklauskas. Jeigu

praityje jau buvo atlikta užklausa DI platformai dėl svetainės, naudotojui yra grąžinamas rezultatas iš duomenų bazės, pakartotina užklausa nėra atliekama. Pažymėtina, kad atsižvelgiant į DI raidą, seniau atliktos užklauskos gali būti nebeaktualios. Dėl šios priežasties siūloma įvesti senaties terminą, po kurio pakartotina užklausa DI, gavus naudotojo užklausa, būtų atliekama nepaisant to, kad duomenų bazėje yra saugomas DI atsakymas. Papildomai, DI atsakymų sąrašas turėtų būti prieinamas sistemos administratoriui, tam, kad būtų galima rankiniu būdu tikrinti puslapius, dėl kurių DI pateikė neigiamą atsakymą. Pasitvirtinus įtarimui, informacija apie aptiktą galimai nelegalų turinį turėtų būti perduodama nagrinėti atsakingoms institucijoms (pirmiausiai – LRTK).

Formuojant užklausa DI, svarbiausias aspektas siekiant užtikrinti atsakymo kokybę – tinkamai suformuotas DI užklauskos tekstas (angl. *AI prompt*). Administratoriaus aplinkoje turėtų būti sukurta galimybė keisti DI užklauskos teksto šablonus, nes vystantis DI technologijoms šios Studijos rengimo metu sudarytas užklauskos tekstas gali pasenti. Toliau pateikiama sudaryta DI užklausa anglų kalba.

At the bottom of my prompt, I provide website source code. Analyse its contents. Evaluate how likely it is that this website contains illegal content on a scale from 1 (likely) to 10 (unlikely). If you cannot present a definitive answer, return "Impossible to assess". Use the list of domains of confirmed illegal websites (<https://www.rtk.lt/lt/atviri-duomenys/interneto-svetaines-kuriose-pazeidziamos-autoriu-teises>). If you find similarities with illegal websites, give a rating lower than 4. If you find other suspicious attributes in the given website, provide a rating around 5. On the last line of your answer, only provide the evaluation.

Dabartinėje versijoje DI pateikiama ne nuoroda (ne visais atvejais DI gali atidaryti nuorodą), o puslapio pirminis kodas. Pažymėtina, kad kartais pirminis kodas yra per ilgas paprastai užklauskai, jį gali reikėti pateikti kaip failą arba skaidyti į dalis. Kuriant Technologinį sprendimą į tai turės būti atsižvelgta.

Toliau pateikiamas pagrindinių svetainių, su kuriomis buvo testuojama ši DI užklausa, sąrašas. Naudota ChatGPT-4o versija. Atsakymų tikslumas gali skirtis kitose DI platformose arba naudojant kitokius modelius.

- **Lietuviška nelegalaus turinio svetainė** (<https://45.87.153.175/846578-saskaitininkas-2-online.html>). DI vertinimas – 2 (tikriausiai nelegalus šaltinis). DI argumentai: nemokama peržiūra ir parsisiuntimai; nustatytos sąsajos su grupėmis ir „prekės ženklais“, kurie žinomi kaip piratiniai; nėra nurodoma informacija apie autorines teises;
- **Tarptautinė nelegalaus turinio svetainė** (<https://piratebayproxy.info/>). DI vertinimas – 3 (tikriausiai nelegalus šaltinis). DI argumentai: nemokama peržiūra ir parsisiuntimai; nustatytos sąsajos su grupėmis ir „prekės ženklais“, kurie žinomi kaip piratiniai;
- **Rusiška nelegalaus turinio svetainė** (<https://severance-hdrezka.net/>). DI vertinimas – 3 (tikriausiai nelegalus šaltinis). DI argumentai – svetainė siūlomas nemokamas turinio peržiūrėjimas; yra minimos grupės ir „prekės ženklai“, kurie žinomi kaip piratiniai; LRTK bazėje yra minimi panašių svetainių pavadinimai;
- **LRT Epika** (<https://epika.lrt.lt>). DI vertinimas – 10 (legalus šaltinis). DI argumentas – puslapis priklauso Lietuvos visuomeniniam transliuotojui; skaidrių ir patikimų technologijų naudojimas;
- **E-kinas** (<https://e-kinas.lt>). DI vertinimas – 10 (legalus šaltinis). DI argumentas – puslapis priklauso Lietuvos valstybinei institucijai.

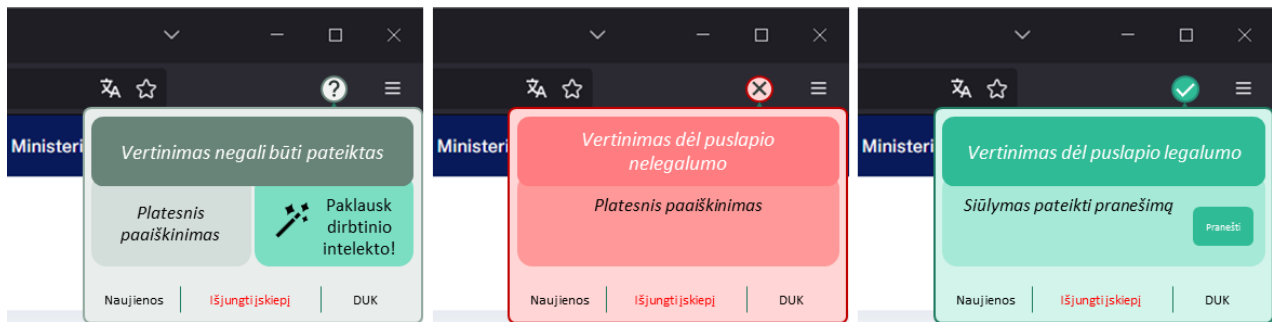
DI grąžinamas rezultatas turės būti apdorotas tokiu būdu, kad naudotojui naršyklės įskiepyje būtų pavaizduotas korektiškas rezultatas. Kuriant Technologinį sprendimą pagal galimybes turėtų būti integruotos kelios DI platformos, siekiant suteikti naudotojams galimybę pasirinkti iš siūlomų platformų ar modelių.

Pagrindinis praktinis iššūkis – DI užklauskos gali kainuoti santykinai brangiai (plačiau žr. 3.2.3. skyriuje). Vienas iš būdu mažinti išlaidas – saugoti DI atsakymus, neteikti atsakymų dėl svetainių, apie kurias jau buvo užduotas klausimas ir gautas atsakymas. Kitas būdas – dienos kvotos naudotojams. Dienos kvotos leistų išvengti piktnaudžiavimo. Siūloma pradėti nuo 5 užklauskų per dieną ir priklausomai nuo naudotojų reakcijos ir faktinių sąnaudų – keisti kvotą. Kvotą turėtų būti galima pakoreguoti administratoriaus aplinkoje.

Naudotojo įskiepis administratoriaus aplinkoje nustatytu dažniu taip pat pateikia analitinę informaciją analitiniam moduliui pagal administratoriaus aplinkoje nustatytą analitinių rodiklių sąrašą. Ši informacija leidžia įvertinti aktyvių naudotojų skaičių.

Toks požiūris leidžia užtikrinti, kad yra minimizuojamas krūvis serverio pusei (kiekvieno naudotojo veiksmas naršyklėje nereikalauja apdoroti naujos užklauso), naudotojo naršymo patirčiai (mažėja siunčiamos informacijos kiekis), o svarbiausia – išlaikomas naršymo istorijos anonimiškumas.

Toliau pateikiamos koncepcinės įskiepio vizualizacijos.



17 paveikslas. Įskiepio skirtingų scenarijų koncepcinės vizualizacijos. Pirmas paveikslas – atvejis, kai įskiepis negali pateikti vertinimo, antras paveikslas – įskiepis nustatė, kad puslapis įtrauktas į nelegalių svetainių sąrašą, trečias paveikslas – įskiepis nustatė, kad puslapis įtrauktas į legalių svetainių sąrašą

Šaltinis: sudaryta Konsultanto

Valdymo aplinkoje yra nustatomos sąsajos su išorinėmis sistemomis – tiek duomenų gavimo dažnis ir principas, tiek informacijos pateikimas (pavyzdžiui, patvirtintas pranešimas dėl galimai nelegalaus puslapio).

KITOS TECHNOLOGINIO SPRENDIMO SAVYBĖS

Užtikrinant Technologinio sprendimo tinkamą įgyvendinimą, būtina užtikrinti ir kitų toliau aprašytų savybių įgyvendinimą.

Technologinis sprendimas, jeigu tai techniškai įmanoma, turi būti suderintas su toliau išvardintomis platformomis:

- turi būti užtikrintas veikimas „Chrome“ (taip pat naršyklėse, kurios naudoja „Chrome“ naršyklės pagrindą ir kurios palaiko tokio pobūdžio įskiepius) ir „Firefox“ naršyklių versijose Windows ir Linux platformose;
- turi būti užtikrintas veikimas „Safari“ naršyklių versijose MacOS, iOS, iPadOS platformose;
- turi būti užtikrintas veikimas „Firefox for Android“ naršyklių versijose Android platformose.

Šios naršyklės yra pasirenkamos dėl jų populiarumo tarp naudotojų. Remiantis „StatCounter Global Stats“ duomenimis⁷⁶ 2024–2025 m. periode, Lietuvos regione populiariausios ir dažniausiai naudojamos naršyklės yra šios: „Chrome“ (vid. 65 proc. visų naudotojų), „Safari“ (vid. 26 proc. visų naudotojų), „Firefox“ (vid. 3,5 proc. visų naudotojų). Šios trys naršyklės apima daugiau nei 90 proc. Lietuvos interneto naudotojų bazės, todėl jos leidžia sukurti technologinį sprendimą, kuris būtų prieinamas platesnei auditorijai.

Pažymėtina, kad Technologinio sprendimo išpildymas gali skirtis dėl išsiskiriančių apribojimų skirtingose platformose. Pavyzdžiui, „Safari“ naršyklė iOS negalės atvaizduoti informacijos iššokančiame lange. Prie tokių sistemos apribojimų reikės prisitaikyti kuriant Technologinį sprendimą.

Atsižvelgiant į galimybes ateityje plėsti ir tobulinti Technologinį sprendimą (žr. 3.2.2. skyrių), Technologinis sprendimas turi būti įgyvendinamas plačiai taikant modulinio IRT sprendimų kūrimo principą.

Planuojant Technologinio sprendimo našumą, būtina nustatyti tikėtiną naudotojų skaičių. Nors potencialus naudotojų skaičius galiausiai priklausys nuo šiuo metu sunkiai išmatuojamų veiksnių, dabartiniame etape būtina nustatyti orientacinį naudotojų skaičių, kurį pirminė Technologinio sprendimo versija būtų pajėgi aptarnauti.

Reikalavimai greitaveikai nustatomi atsižvelgiant į orientacinį vidutinį naudotojų skaičių per dieną. 3.2.3. skyriuje nustatoma, kad orientacinis vidutinis unikalių naudotojų skaičius per dieną neturėtų viršyti 10 tūkst. žmonių.

⁷⁶ „StatCounter GlobalStats“, Browser Market Share, Lithuania May 2024 - May 2025. Prieiga internetu: <https://gs.statcounter.com/browser-market-share/all/lithuania>

Siūloma reikalavimus greitaveikai formuoti taip, kad Technologinis sprendimas nepatirtų trikdžių esant tokiam tuo pačiu metu prisijungusių naudotojų skaičiui. Jeigu esant optimistiniam scenarijui visi potencialūs naudotojai būtų pritraukti naudotis technologiniu sprendimu, reikalavimai greitaveikai padidėtų iki 100 tūkst. naudotojų tuo pačiu metu. Siūloma kuriant jau pirmą Technologinio sprendimo versiją numatyti galimybę išplėsti Technologinio sprendimo našumą iki tokio lygio.

Siekiant išvengti duomenų praradimo, visa informacija turi būti kartą per mėnesį išsaugoma rezerviniuose atsarginių kopijų saugyklose, nepriklausančiose nuo Technologinio sprendimo pagrindinių sistemų.

Remiantis skyriuje pateikta informacija, parengtas Studijos priedas – Technologinio sprendimo techninė specifikacija. Priede papildomai detalizuojama skyriaus informacija (žr. 1 priedą).

3.2.2. Technologinio sprendimo plėtros ir atnaujinimo galimybės

Tolimesniuose etapuose rekomenduojama plėtoti Technologinį sprendimą jį pildant toliau išvardintais funkcionalumais:

- **Patikimų organizacijų įtraukimas į sąrašų sudarymo procesą.** Visiškai neautomatizuotas būdas, pildant legalių šaltinių sąrašus pagal konkrečius kūrinius, paremtas autorių teisių turėtojų ir jiems atstovaujančių organizacijų, įsitraukimu. Plačiau 2.4.3. skyriuje šis variantas aprašytas kaip variantas IIA-3;
- **Naršyklės įskiepio funkcionalumo plėtra nustatant įtartinus puslapius.** Pusiau automatizuotas būdas, paremtas pačio įrankio nustatytų įtartinų šaltinių sąrašų tikrinimu, pildant sąrašus šaltinių, dėl kurių kilę įtarimai pasiteisino. Plačiau 2.4.3. skyriuje šis variantas aprašytas kaip variantas IIA-4.

Patikimų organizacijų įtraukimas turėtų būti realizuojamas sukuriant aplinką autorizuotų institucijų atstovų prisijungimui prie sistemos ir sukuriant susijusius funkcionalumus sąrašų redagavimui.

Patikimų organizacijų atstovai galėtų pildyti konkrečių kūrinių legalių šaltinių sąrašus. Naršyklės įskiepio funkcionalumas turėtų būti išplėstas tokiu būdu, kad jis galėtų nustatyti, kokį konkrečiai kūrinių naudotojas bando peržiūrėti atidarytoje svetainėje. Jeigu ši svetainė nėra įtraukta į patikimos organizacijos atstovų užpildytą sąrašą, naršyklės įskiepis praneštų apie galimai nelegalų šaltinį.

Naršyklės įskiepio funkcionalumo plėtra nustatant įtartinus puslapius susidarytų iš algoritmų, kurie nustato puslapius, panašius į nelegalias svetaines. Tokie algoritmai susidarytų iš puslapio išvaizdos, teksto, puslapio kodo analizės. Jeigu algoritmai nustatytų, kad puslapis primena nelegalų turinį skleidžiantį šaltinį, automatiškai būtų pateiktas pranešimas į valdymo aplinką. Pranešimas būtų perduotas atsakingoms institucijoms (LRTK ir kitoms) nagrinėjimui.

Tokia plėtra reikalautų rimto įskiepio funkcionalumo papildymo, tačiau galėtų palengvinti atsakingų institucijų darbą, ypač jeigu įskiepis būtų plačiai naudojamas.

3.2.1. Technologinio sprendimo sukūrimo ir palaikymo proceso aprašymas

Siekiant užtikrinti, kad Technologinis sprendimas bus tinkamai įgyvendinamas šiame skyriuje pateikiamas sukūrimo ir palaikymo proceso aprašymas bei reikalavimai Technologiniam sprendimui.

Technologinio sprendimo sukūrimas ir palaikymas sudarytas iš šių etapų:

- I etapas. Technologinio sprendimo kūrėjai (toliau – Paslaugų teikėjas) privalės suderinti prototipo kūrimo sąlygas su Perkančiąja organizacija, atsižvelgiant į Technologinio sprendimo techninę specifikaciją (žr. 1 priedą);
- II etapas. Paslaugų teikėjas parengia Technologinio sprendimo prototipą ir atlieka jo testavimą (žr. 1 priedą);
- III etapas. Paslaugų teikėjas pakoreguoja Technologinio sprendimo prototipą, parengia praktiniam veikimui parengtą versiją ir Technologinis sprendimas pradeda veikti (žr. 1 priedą);

- IV etapas. Technologinis sprendimas yra stebimas, pagal poreikį atliekami sistemos atnaujinimai.

I etape Paslaugų teikėjas su Perkančiąja organizacija privalo suderinti šiuos aspektus:

- Technologinio sprendimo dizainas (iš trijų teikėjo pasiūlytų variantų);
- Analitinių rodiklių rinkimo, atvaizdavimo administratoriaus aplinkoje ir parsisiuntimo būdai ir dažniai;
- Atviro kodo principo įgyvendinimo būdai;
- DI integracijos būdai;
- Prototipo ir paruošto Technologinio sprendimo automatizuoti ir rankinio testavimo būdai, procedūros.

II etape Paslaugų teikėjas parengia Technologinio sprendimo prototipą. Prototipas turėtų išpildyti visus funkcinis ir nefunkcinis reikalavimus tokia apimtimi, kurios pakaktų atlikti automatizuotas ir rankines testavimo procedūras. Kartu su prototipu Paslaugų teikėjas turės paruošti testavimo aplinką.

Funkcinių ir nefunkcinių techninės specifikacijos reikalavimų testavimas. Testavimo metu tikrinami šie scenarijai ir situacijos:

- Nelegalių ir legalių šaltinių sąrašo atnaujinimas;
- Klaidų nelegalių ir legalių šaltinių sąrašė nustatymas;
- Didelės apkrovos (jei tuo pačiu metu Technologiniu sprendimu naudojasi 10 000 žmonių) atsiradimas;
- Nustatymų keitimas sistemos veikimo metu;
- Kiekvieno iš sistemos elemento funkcionalumo praradimas;
- Skirtingų svetainių vertinimas;
- Veikimas skirtingose platformose (naršyklėse, operacinėse sistemose).

Atliekant testavimą turi būti užtikrinami šie kriterijai:

- Visais atvejais yra išpildomi funkciniai techninės specifikacijos reikalavimai, nėra nustatomas kitoks sistemos veikimas, išskyrus tuos atvejus, jeigu yra testuojamas sistemos veikimas praradus vieno iš sistemos elemento funkcionavimą. Tokiu atveju sėkmės kriterijus – tinkamas sistemos administratoriaus ir naudotojų informavimas apie susiklosčiusią situaciją;
- DI atsakymų tikslumas viršija 95 proc.;
- Išpildomi nefunkciniai reikalavimai.

Papildomai atliekamas testavimas su žmonėmis, tikrinamas ne tik tinkamas veikimas, tačiau ir bendra naudotojo patirtis. Nustatoma galimybė tobulinti naudotojo patirtį techninės specifikacijos reikalavimų ribose.

III etape Paslaugų teikėjas perkančiajai organizacijai turės įrodyti, kad bet kokie nustatyti Technologinio sprendimo prototipo netobulumai yra ištaisyti ir Technologinio sprendimo pirminis kodas ir susijusi medžiaga yra paruošti naudojimui. Papildomai, Paslaugų teikėjas privalo paruošti aplinką, įrankius, funkcionalumus, skirtus problemų nustatymui veikiančiame Technologiniame sprendime. Kartu su III etapo medžiaga Paslaugų teikėjas privalo pateikti techninį aprašymą ir aprašymą naudotojui.

Veikiančio (IV etapas) Technologinio sprendimo problemų fiksavimo aplinka, įrankiai ir funkcionalumas yra skirti užtikrinti, kad nebūtų pažeistas paslaugų lygio susitarimas (arba PLS (angl. SLA)).

Detalus paslaugų lygio susitarimas turėtų būti parengtas III etape, toliau pateikiamas apibendrintas PLS.

PLS sudaro šie komponentai:

- Atsakymo laiko ir reakcijos į nenumatytas aplinkybes reikalavimai: įsipareigojama pranešti vartotojams apie sistemos veikimo sutrikdymus per 24 val. ir atstatyti sistemos veikimą per 5 d. d.;
- Sistemos prieinamumo (veikimo užtikrinimo) reikalavimai: įsipareigojama, kad sistema veiks 95 proc. laiko;
- Pranešimų apie sistemos veikimo laikino nutraukimo reikalavimai: pranešimai apie tokio pobūdžio trikdžius yra pateikiami naudotojams prieš 5 d. d.;
- Pagalbos prieinamumo reikalavimai: naudotojams pagalba teikiama el. paštu darbo dienomis tarp 9 val. ir 15 val. Į užklausas atsakoma per 1 d. d.

Atitinkamai, siekiant užtikrinti atitikimą PLS III etapo funkcionalumams, Paslaugų teikėjas užtikrina, kad IV etape veiks šie funkcionalumai:

- Sistemos veiklą stebinčių žurnalų sistema, kur yra saugoma informacija apie sistemos komponentų būseną, sąveiką, klaidų atsiradimą. Žurnalų informacija pasiekama per administratoriaus aplinką. Žurnalų sistema turi užtikrinti PLS įgyvendinimą. Žurnalai turėtų būti saugomi metus laiko. Žurnalų šalinimo laikotarpių nustatymas turėtų būti reguliuojamas administratoriaus aplinkoje;
- Pagrindinių sistemos elementų tinkamo veikimo stebėseną (atskirų sistemos elementų veikimo statusas ir integracijų patikra) turėtų būti užtikrinama administratoriaus aplinkoje.

Atsižvelgiant į 3.3. skyriuje nurodytą informaciją, Technologinis sprendimas veiks atviro kodo principu. Paslaugų teikėjas turi pasirūpinti, kad Technologinio sprendimo kodas būtų prieinamas viešose kodo saugyklose (pavyzdžiui, GitHub arba Gitlab). Kodo talpinimas yra atliekamas siekiant užtikrinti naudotojų pasitikėjimą Technologinio sprendimo kodu. Nėra siekiama aktyvaus naudotojų įsitraukimo į Technologinio sprendimo plėtrą, todėl kodo saugyklų nustatymai turi būti parengti tokiu būdu, kad neautorizuoti naudotojai negalėtų siūlyti savo korekcijų.

Siekiant užtikrinti galimybę naudotojams, pastebėjusiems saugumo spragas ar kitokias kodo problemas, pranešti apie sistemos pažeidžiamumą, turi būti aprašytas atsakingo atskleidimo procesas. Atsakingo atskleidimo procesas numato, koku būdu ir apie kokio pobūdžio pažeidžiamumą naudotojas gali pranešti sistemos administruojančiam subjektui. Atsakingo atskleidimo procesas Technologinio sprendimo atveju turėtų būti realizuojamas aiškiai nurodant:

- El. pašto adresą, kurį tikrina administruojantis subjektas, į kurį bet kas gali pateikti pranešimą apie pastebėtą pažeidžiamumą;
- Trumpą ir aiškų aprašymą, kas ir kokiais atvejais gali teikti pranešimus.

Technologinis sprendimas turėtų veikti naudojant Elastic License v2 arba panašią licenciją, kuri užtikrina, kad kodas yra viešai prieinamas, tačiau negali būti platinamas, tik naudojamas ir modifikuojamas asmeniniais tikslais.

3.2.2. Technologinio sprendimo sąnaudų–naudos analizė

Šį skyrių sudaro dvi dalys:

- **Naudos komponento nustatymas** – naudos komponentas pilna apimtimi sudarytas iš socioekonominės naudos, atsirandančios dėl patiriamų nuostolių, susijusių su piratavimu, sumažėjimo;
- **Sąnaudų komponento nustatymas** – sąnaudų komponentas sudarytas iš finansinių sąnaudų, nes neigiamo socioekonominio poveikio nenumatoma.

Naudos komponento nustatymui būtina įvertinti, kiek žmonių naudos Technologinį sprendimą. Turint omenyje, kad šio Technologinio sprendimo tikslinė auditorija – asmenys, kurie nežino, jog vartoja nelegalų turinį – laikoma, kad Technologinio sprendimo naudojimas lemtų, jog tokie asmenys nustotų vartoti nelegalų turinį, t.y. sumažėtų piratavimo mastas.

Orientacinio naudotojų skaičiaus nustatymas turėtų būti pradedamas nuo didžiausio galimo naudotojų skaičiaus. Remiantis 1 skyriuje pateikiama analize, Technologinis sprendimas potencialiai gali sudominti tuos Lietuvos suaugusius gyventojus, kurie sunkiai geba atskirti legalius ir nelegalius audiovizualinio turinio šaltinius. Nors, priklausomai nuo 1 skyriuje pateiktos apklausos rezultatų interpretavimo metodikos, tokių žmonių skaičius gali būti iki 25 proc., siūloma skaičiavimams naudoti labiau apribotus vertinimus.

Remiantis 1 skyriuje pristatytos apklausos duomenimis 4 proc. respondentų buvo įsitikinę, kad Filmai.in ir Linkomanija yra legalūs audiovizualinio turinio šaltiniai. Būtent ši procentinė dalis bus toliau naudojama potencialių naudotojų skaičiui nustatyti (nuo suaugusiųjų populiacijos Lietuvoje 2025 m. pradžioje). Atlikus skaičiavimus tokių potencialių naudotojų būtų apie 98 tūkst. Pažymėtina, kad šis skaičius apibrėžia Technologinio sprendimo naudotojų skaičiaus lubas, t. y. daugiau nei 98 tūkst. naudotojų nebus, o greičiausiai jų bus ir daug mažiau.

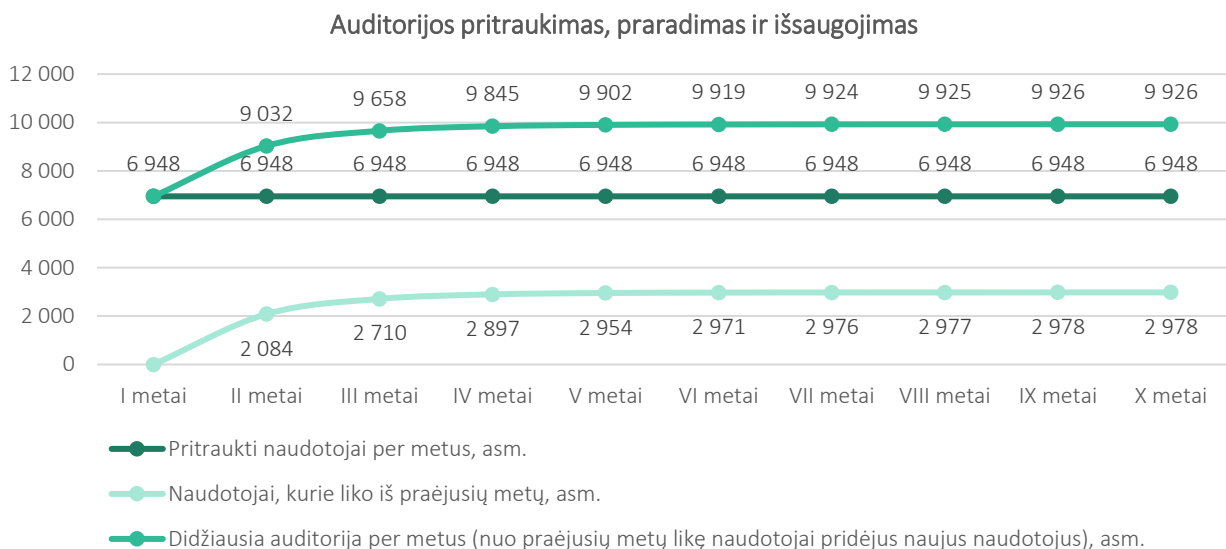
Technologinio sprendimo naudotojų skaičius ir jų kaita bėgant laikui priklausys nuo:

- Tikslinės auditorijos masto nustatymo tikslumo (ar šiuose ir kituose tyrimuose nustatytas potencialių naudotojų skaičius pakankamai artimas tikrovei);
- Viešinimo ir rinkodaros veiksmų veiksmingumo (ar viešinimo, rinkodaros kompanijos ir veiksmai bus veiksmingi);
- Technologinio sprendimo išpildymo kokybės;
- Administracinių veiksmų taikymo (ar bus nuspręsta privalomai instaliuoti Technologinį sprendimą į viešųjų įstaigų kompiuterius, ar ne ir pan.).

Šių veiksmų negalima įvertinti dabartiniame etape, ypač vykstant jų kaitai. Dėl šios priežasties visi tolimesni veiksmai bus vertinami kaip tikėtinas unikalių naudotojų vidurkis. Jis nustatomas tokiu būdu:

1. Tikėtina, kad Technologinio sprendimo viešinimo veiksmai pasieks visus tikslinės auditorijos atstovus, todėl 100 proc. auditorijos potencialiai susidomės Technologiniu sprendimu;
2. Remiantis paspaudimo ant reklaminių pranešimų tikimybės tyrimais, iki 13,1 proc.⁷⁷ reklaminių pranešimą pamačiusių asmenų pereina į reklamuojamą puslapį meno ir pramogų srityje. Todėl vertinama, kad tokių žmonių bus 12,8 tūkst.;
3. Remiantis konversijos tyrimais, analizuojančiais, kiek susidomėjusių žmonių tampa naudotojais, laikoma, jog apie 5 proc.⁷⁸ susidomėjusių lankytojų taptų naudotojais. Tokiu atveju viena reklaminė kompanija galėtų pritraukti 579 naudotojus – tačiau planuojama tokias kompanijas vykdyti nuolat. Atsižvelgiant į tai, toliau pateikiamas paprastas auditorijos priaugio modelis.

Modelis remiasi prielaidomis, kad 12 kartų per metus bus paleidžiamos reklaminės kompanijos, kurios lemtų 13,1 proc. paspaudimų ant reklaminių pranešimų (nuo tikslinės auditorijos unikalių naudotojų), iš šių lankytojų 5 proc. taptų naudotojais. Po metų, 30 proc. naudotojų būtų išlaikyta⁷⁹, nes įvyktų natūralus naudotojų praradimas. Po metų situacija pasikartotų.



3 paveikslas. Auditorijos pritraukimo, praradimo ir išsaugojimo modelis 10 metų į priekį

Šaltinis: sudaryta Konsultanto

Po maždaug 5 metų situacija stabilizuotųsi, nes pritraukiamų naudotojų skaičius pradėtų kompensuoti prarandamų naudotojų skaičių. Didžiausias metų naudotojų skaičius (kuris susidaro, kai dar nebuvo prarasta

⁷⁷ WordStream. Google Ads Benchmarks 2025: Competitive Data & Insights for Every Industry. Prieiga internetu: <https://www.wordstream.com/blog/2025-google-ads-benchmarks>

⁷⁸ WordStream. Conversion Rate Benchmarks: Find Out How YOUR Conversion Rate Compares. Prieiga internetu: <https://www.wordstream.com/blog/ws/2019/08/19/conversion-rate-benchmarks>

⁷⁹ WordStream. 13 Customer Retention Strategies to Earn Loyalty (& Save Money). Prieiga internetu: <https://www.wordstream.com/blog/ws/2022/03/09/customer-retention-strategies>

auditorija iš praėjusių metų ir jau pritraukta nauja auditorija) sudarytų apie 9,5 tūkst. asmenų (ne daugiau nei 9,9 tūkst. asm.). Dėl šios priežasties toliau laikomasi prielaidos, kad didžiausias galimas tuo pačiu metu prisijungusių naudotojų skaičius sudarytų iki 10 tūkst. asmenų.

Atsižvelgiant į tai, kad TS nurodoma, jog Lietuvoje dėl nelegalaus turinio vartojimo patiriama 15 mln. Eur nuostolių, o šis skaičius, apskritai, yra mažesnis nei kiti vertinimai, siekiant saugiai įvertinti nuostolių mastą, laikoma, kad Technologinis sprendimas sumažins nuostolius 4 proc., t. y. 600 tūkst. Eur./metus kiekvienais metais nuo veikimo pradžios. Toliau pristatomas sąnaudų komponentas.

Sąnaudų komponentas susidaro iš:

- **Sukūrimo sąnaudų** – jos įvertinamos remiantis Inovacijų agentūros atlikta rinkos konsultacija dėl panašaus technologinio sprendimo. Kaina priklausys nuo viešojo pirkimo konkurso rezultato, tačiau tokio sprendimo sukūrimo kaina neturėtų viršyti 50 tūkst. Eur.;
- **Viešinimo sąnaudų** – jos priklauso nuo viešinimo kompanijų masto, tačiau daroma prielaida, kad išlaidos nebus didesnės nei įprastos rinkodaros kompanijos, kuriomis kviečiama priimti atsakingus sprendimus (pavyzdžiui, Lietuvos universitetų kvietimo studijuoti rinkodaros kampanijos – „Studijuok Kaune“, kuri buvo paskelbta CPV IS sistemoje 2024 m. birželio 17 d.). Šių viešinimo kompanijų išlaidos paimtos iš Lietuvos viešųjų pirkimų sistemos. Vertinama, kad Technologinis sprendimas turės būti nuolat viešinamas, todėl išlaidos bus patiriamos kiekvienais metais. Išlaidos – 6 tūkst. Eur./metus, kiekvienais metais nuo veikimo pradžios;
- **Serverio pusės darbo palaikymo sąnaudų** – jos priklauso nuo faktinių duomenų srautų, tačiau didžiausios galimos išlaidos, turint omenyje dabartines prielaidas dėl naudotojų ir duomenų kiekio, nebus didesnės nei 50 Eur./mėnesį arba 600 Eur./metus, kiekvienais metais nuo veikimo pradžios;
- **Išlaidos DI paslaugoms** – priklausomai nuo išpildymo faktinės sąnaudos gali ženkliai skirtis. Įprastai DI paslaugas teikiančios įmonės apmokestina užklausų skaičių ir sudėtingumą. Atitinkamai, svarbiausi kintamieji, darantys įtaką galutinėms išlaidoms DI paslaugoms, yra užklausų kiekis ir įprastos užklauskos sudėtingumas. Įprastos užklauskos sudėtingumas įvertintas pateikiant DI kainų skaičiuoklei⁸⁰ įprastas suformuotas užklauskas (žr. 3.2.1. skyrių). Atmetus pačius pažangiausius ir brangiausius modelius, vienos naudotojo užklauskos kaina sudaro 0,02246 Eur. Su 3.2.1. skyriuje siūlomais apribojimais (5 užklauskos per dieną) didžiausios galimos metinės išlaidos – 4,1 mln. Eur. Iš kitos pusės, atsižvelgiant į užklausų saugojimą (ne kiekviena naudotojo užklausa bus perduodama DI) ir naudotojų elgseną, tikėtina, jog išlaidos bus ženkliai mažesnės. Atsižvelgiant į Lietuvos gyventojų nelegalaus turinio vartojimo lygio nustatymo tyrimo duomenis, tik trečdalis naudotojų ieško populiariausio turinio formato – serialų ir filmų – kasdien. Todėl realus naudotojų, kuriems gali kilti poreikis nustatyti turinio legalumą, skaičius yra apie 5 188. Atsižvelgiant į tai, kad DI yra planuojamas kaip papildanti, o ne pagrindinė priemonė, vertinama, kad vidutiniškai tokie naudotojai atliktų 1 užklausą per dieną. Remiantis tokiais prielaidomis DI paslaugų sąnaudos sudarytų apie 42 538 Eur./metus;
- **Aptarnaujančio personalo atlyginimai** – vertinama, kad šios sistemos darbo priežiūrai bendrai nereikėtų pilno etato dėl priežiūros darbų trūkumo. Skaičiavimams daroma prielaida, kad sistemos aptarnaujančio personalo atlyginimai kartu sudarytų 1 etatą Kultūros ministerijos, arba bet kurios kitos Technologinį sprendimą administruojančios institucijos vyr. specialisto atlyginimo – 2 325 Eur./mėn. arba 27 900 Eur./metus.

Sudėjus prieš tai pateiktas išlaidų eilutes gaunamos bendros metinės sąnaudos apie 77 tūkst. Eur./metus.

Atliekama įprasta sąnaudų-naudos analizė taikant 4 proc. finansinę diskonto normą ir 5 proc. socialinę diskonto normą. Analizės laikotarpis – 15 metų. Pagrindiniai SNA rodikliai apskaičiuojami tokiu būdu (dėl detalesnio paaiškinimo žr. CPVA Investicijų projektų rengimo metodiką⁸¹):

- Ekonominė grynoji dabartinė vertė (EGDV) – tai projekto investicijų ekonominių išlaidų, sumažintų likutine verte, ir veiklos bei priežiūros ekonominių išlaidų ir socialinės-ekonominės naudos diskontuotų pinigų srautų, įvertintų per visą projekto ataskaitinį laikotarpį, dabartinė vertė. Ji parodo, kokia grynoji socialinė-ekonominė nauda, įvertinant visas pinigine išraiška pamatuojamas naudas ir išlaidas, būtų sukurta įgyvendinus projektą, kartu atsižvelgiant ir į alternatyvius ekonominius kaštus, t. y. į ekonominę grąžą, kurią visuomenė tikisi gauti iš pokyčiai įgyvendinti skiriamų lėšų;

⁸⁰ Token calculator. Prieiga internetu: <https://token-calculator.net/>

⁸¹ CPVA. Investicijų projektų rengimo metodika. https://cpva.lt/wp-content/uploads/2025/01/IP-metodika_2025.pdf

- Ekonominės naudos ir išlaidų santykis (ENIS) – atskleidžia, kiek kartų projekto sukuriama socialinė-ekonominė nauda viršija jam įgyvendinti reikalingas išlaidas. ENIS apskaičiuojamas, padalinant projekto kuriamą socialinę-ekonominę naudą iš ekonominių išlaidų.

Atlikus SNA analizę 15 metų laikotarpiui gaunami toliau nurodyti rezultatai:

- Ekonominė grynoji dabartinė vertė (EGDV) – 5 585 359 Eur.;
- Ekonominės naudos ir išlaidų santykis (ENIS) – 8,6. Pastaba – rezultatas, didesnis nei vienetas, laikomas geru. Šis rezultatas laikomas ypač geru.

Apibendrinant atliktą SNA analizę galima teigti, kad Technologinio sprendimo įgyvendinimas yra naudingas ir efektyvus.

3.3. Technologinio sprendinio administravimo modelis

Administravimo modelis – administravimo sistema, kuri padeda apibrėžti konkrečios technologijos valdymo, palaikymo, priežiūros ir tobulinimo procesus. Jis padeda administruojančiai organizacijai efektyviai optimizuoti bei valdyti įrankį. Tai užtikrina sklandesnį veikimą bei efektyvų išteklių panaudojimą.

Yra išskiriami du būdai, kaip galima administruoti technologinius sprendimus – tai yra atviro kodo ir uždaro kodo reguliacijos modeliai.

ATVIRO KODO PROJEKTŲ VALDYMO MODELIS

Valdymas suprantamas kaip formalių ar neformalių taisyklių, normų bei procedūrų visuma, kuri apibrėžia, kas organizacijoje ar iniciatyvoje turi teisę vykdyti tam tikras funkcijas, kaip jos turėtų būti atliekamos bei kokiomis aplinkybėmis ar terminais. Svarbus tokių modelių aspektas – jis orientuotas į platesnės bendruomenės įtraukimą į technologinio sprendimo valdymą ir plėtrą (dažniausiai savanoriškais pagrindais). Modelis užtikrina:

- skaidrius dokumentacijos ir darbo indėlio srautus;
- kodų kokybės standartus;
- konfliktų sprendimo procedūras;
- intelektinės nuosavybės ir licencijavimo atitiktį;
- projekto kryptį;
- priežiūros pareigas.

Atvirojo kodo projektų valdymas – tai vis labiau įsitvirtinanti praktika, kuri suteikia galimybę skirtingiems veikėjams (tiek kūrėjams, tiek naudotojams) bendrai kurti, palaikyti ir tobulinti programinę įrangą. Šis modelis reikalauja, kad esminiai projekto vystymo aspektai – sprendimų priėmimas, problemų sprendimo tvarka, etikos bei elgesio gairės – būtų grindžiami atvirumo ir skaidrumo principais.

Be to, atvirojo kodo modelis padeda projektui tapti lankstesniu, efektyvesniu bei labiau prisitaikančiu prie sparčiai kintančio technologinio konteksto. Galiausiai, naudojamos skaitmeninės bendradarbiavimo platformos, atvirojo kodo bendruomenės gali užtikrinti nuolatinį informacijos prieinamumą, sprendimų viešumą bei operatyvų pokyčių įgyvendinimą, taip stiprindamos pasitikėjimą tarp visų dalyvaujančių subjektų.⁸²

Galimi skirtingi modelio išpildymo variantai:

1. „Do-Ocracy“ – atvirojo kodo projektai, veikiantys pagal „do-ocracy“ valdymo modelį, ypatingai pabrėžia nuosekliai prisidedančių narių įdirbį. Todėl sprendimai priimami remiantis tuo, kurio indėlis buvo vertingiausias.
2. „Founder-Leader“ – įkūrėjo–lyderio modelis dažniausiai pasitaiko naujuose projektuose arba projektuose, kuriuose dalyvauja tik nedidelis skaičius prisidedančiųjų. Šio valdymo būdo privalumas yra tas, jog asmuo ar komanda, kuri kuria projektą, taip pat prisiima atsakomybę už administravimą, viziją, leidimų integruoti kodą suteikimą ir oficialios nuomonės viešą pateikimą.
3. „Self-Appointing Council Or Board“ – įkūrėjo–lyderio valdymo modelis ne visada yra idealus atvirojo kodo projektams. Savarankiškai paskirta taryba ar valdyba yra vienas iš būdų įvesti atskiras pareigas, kuriomis valdomos skirtingos sritys. Šis metodas leidžia efektyviau perduoti vadovavimą, užtikrinant nuolatinę paramą. Be to, galima sudaryti įvairius komitetus, įskaitant iniciatyvinius komitetus, komitetų tarybas, techninių operacijų komandas, architektūros tarybas ir direktorių valdybas, siekiant nustatyti jų darbo tvarkos taisykles ir hierarchiją struktūros viduje.
4. „Electoral“ – rinkiminė demokratija suteikia atvirojo kodo projektams galimybę sukurti valdymo struktūras ir procesus, kuriuos gerbs jų nariai. Šis požiūris dažnai pasitaiko decentralizuotose ekosistemose, kurias sudaro prisidedantys kūrėjai iš viso pasaulio. Jis leidžia nariams balsuoti dėl to, kas turėtų juos atstovauti ir vadovauti jų projektui, taip pat dėl su pačiu projektu susijusių klausimų ar būtinų pakeitimų.

⁸² Scantist, „A Guide to the 6 Open Source Governance Models“, 2023 m. Peržiūra internete: <https://scantist.com/resources/blogs/a-guide-to-the-6-open-source-governance-models>

5. „Single-Vendor“ – vieno tiekėjo valdymo modelis dažnai pasitaiko projektuose, kuriuose visa projekto veikla kontroliuojama vienos įmonės ar organizacijos. Šis metodas apima nuolatinę komandą, kurios užduotis yra kurti ir prižiūrėti programinę įrangą, taip pat užtikrinti, kad būtų sprendžiami visi iškilę klausimai. Už projekto valdymą atsakingas tiekėjas paprastai turi galutinį žodį visais su projekto valdymu ir naudojimu susijusiais klausimais.
6. „Foundation-Backed“ – šiuo atveju fondo remiamas valdymas yra panašus į vieno tiekėjo modelį, tačiau už projekto valdymą atsakinga nepriklausoma ne pelno siekianti organizacija. Ši organizacija paprastai turi savo valdybą ir darbuotojus, prižiūrinčius atviro kodo projekto kūrimą ir naudojimą. Ji taip pat teikia finansavimą, kad užtikrintų projekto tęstinumą. Fondo modelis užtikrina didesnę skaidrumą, nes sprendimus priima visos bendruomenės atstovai, o ne vienas tiekėjas.

UŽDARO KODO PROJEKTŲ VALDYMO MODELIS

Taikant uždaro kodo modelį, technologinį sprendimą valdanti organizacija išlaiko visišką nuosavybės teisę į kodą, įskaitant jo platinimą ir naudojimą. Naudotojai gali naudoti sukurtą programinę įrangą tik taip, kaip jį sukūrusi organizacija nurodo, paprastai įsigydami licenciją. Nustatant aiškias sąlygas, galima užkirsti kelią naudotojams neteisėtai kopijuoti, platinti ar atkurti kodą.

Galima išskirti keletą paplitusių licencijų tipų:

- **Proprietarinė licencija** užtikrina, kad niekas negalės naudotis sukurta programine įranga, nebent atsakinga organizacija aiškiai nurodytų kitaip. Tai optimaliausias sprendimas įmonėms ar kūrėjams, kurie nori apsaugoti savo kodą ir tuo pačiu uždirbti iš jo;
- Jei dirbama su debesų kompiuterijos programine įranga, geriausias sprendimas yra **SaaS** (angl. *Software as a Service*) sutartis. Ši sutartis išlaiko visą programinės įrangos kontrolę, o naudotojai moka už prieigą (jei produktas yra mokomas);
- **Komerčinė licencija** leidžia naudotojams įsigyti (jei produktas yra mokomas) programinę įrangą pagal nustatytas sąlygas, dažnai ribojančias programinės įrangos platinimo, keitimo ar kopijavimo galimybes. Ji sukurta tam, kad kūrėjui, būtų suteikta pinigine kompensacija. Ši licencija leidžia nustatyti sąlygas individualiam arba korporatyviniam naudojimui ir rinkti pajamas pagal sutartį;
- Taip pat panašaus pobūdžio į komerčinę licenciją yra **EULA** licencija. EULA yra sutartis tarp programinės įrangos kūrėjo ir galutinio naudotojo. Joje išsamiai aprašoma, kaip naudotojas gali naudoti programinę įrangą, kas yra draudžiama (atvirkštinė inžinerija, kopijų dalijimasis) ir kokios yra sąlygų pažeidimo pasekmės.⁸³

Apibendrinant, uždaro kodo projektų valdymo modelyje visą arba beveik visą kontrolę išlaiko administruojanti organizacija.

ADMINISTRAVIMO MODELIO PASIRINKIMAS

Apibendrinant skyriaus informaciją, pateikiamas atviro ir uždaro kodų administravimo modelių apibendrinimas lentelės forma.

6 lentelė. Atviro ir uždaro administravimo modelio apibendrinimas

| Administravimo funkcijos | Atviras modelis | Uždaras modelis |
|---|------------------|-----------------|
| Valdymas | Decentralizuotas | Centralizuotas |
| Bendruomenės įtraukimas | + | – |
| Ilgalaikė plėtra paremta savanoriavimu | + | – |
| Projekto valdymo struktūros konkretumas | – | + |
| Kontrolė | – | + |

⁸³ Jeferson F Silva, „A Handy Guide to Closed Source Licenses: Protecting Your Code Like a Pro“, 2024 m. Prieiga internetu: <https://dev.to/jeferson0993/a-handy-guide-to-closed-source-licenses-protecting-your-code-like-a-pro-10b3>

| | | |
|---|---|---|
| Aiški nuosavybės teisė | – | + |
| Aiškūs už įrankio kūrybinį procesą atsakingi veikėjai | – | + |

Šaltinis: sudaryta Konsultanto

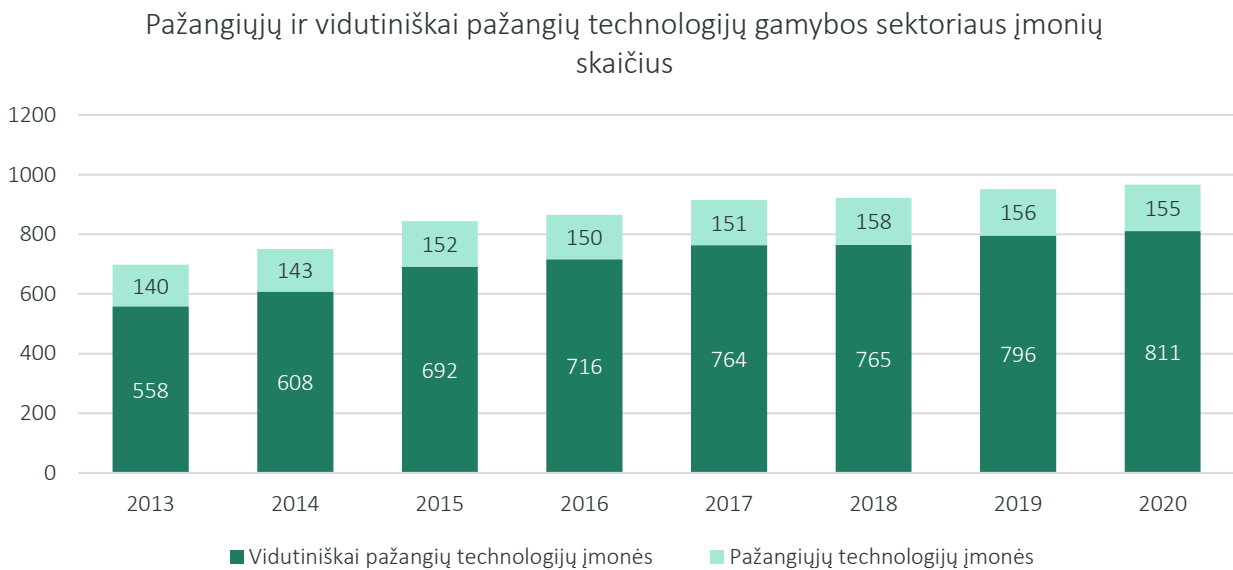
Atviro kodo sistemos pasižymi atvirumu, patikimumu. Uždaro kodo sistemos pasižymi kontrole ir intelektinės nuosavybės užtikrinimu.

Atsižvelgiant į tai, kad būtina užtikrinti naudotojų pasitikėjimą, siūloma programos kodą turėti viešai – versijų valdymo sistemose tokiose kaip Git. Kultūros ministerija vis tiek išlaikytų kontrolę, t. y. pašaliniai asmenys negalėtų savavališkai redaguoti programos kodo, tačiau galėtų su juo susipažinti, pasiūlyti pokyčius. Kontrolę turėtų išlaikyti Kultūros ministerija arba pavaldžiai įstaigai.

4. Lietuvos IT sprendimų kūrėjų rinkos analizė

Šiame skyriuje pateikiama Lietuvos IRT sektoriaus apžvalga ir nustatoma, ar Lietuvos įmonės būtų pajėgios sukurti Technologinį sprendimą.

Siekiant detaliau apžvelgti IRT sektoriaus rodiklius Lietuvoje bei šio sektoriaus raidą, toliau pateikiama išsamesnė statistinė analizė. Lietuvoje ryškėja tendencija, jog pažangiųjų ir vidutiniškai pažangių technologijų gamybos sektoriaus įmonių skaičius auga. 2013 m. buvo 558 vidutiniškai pažangių technologijų įmonių ir 140 pažangiųjų technologijų įmonių, o 2020 m. 881 įmonių buvo priskiriamos prie vidutiniškai pažangių technologijų srities ir 155 įmonės – prie pažangiųjų technologijų srities.⁸⁴ Todėl vidutiniškai per 7-rius metus vidutiniškai pažangių technologijų įmonių skaičius padidėjo – 45,34 proc., pažangiųjų technologijų įmonių – 10,71 proc.⁸⁵



18 paveikslas. Pažangiųjų ir vidutiniškai pažangių technologijų gamybos sektoriaus įmonių skaičius

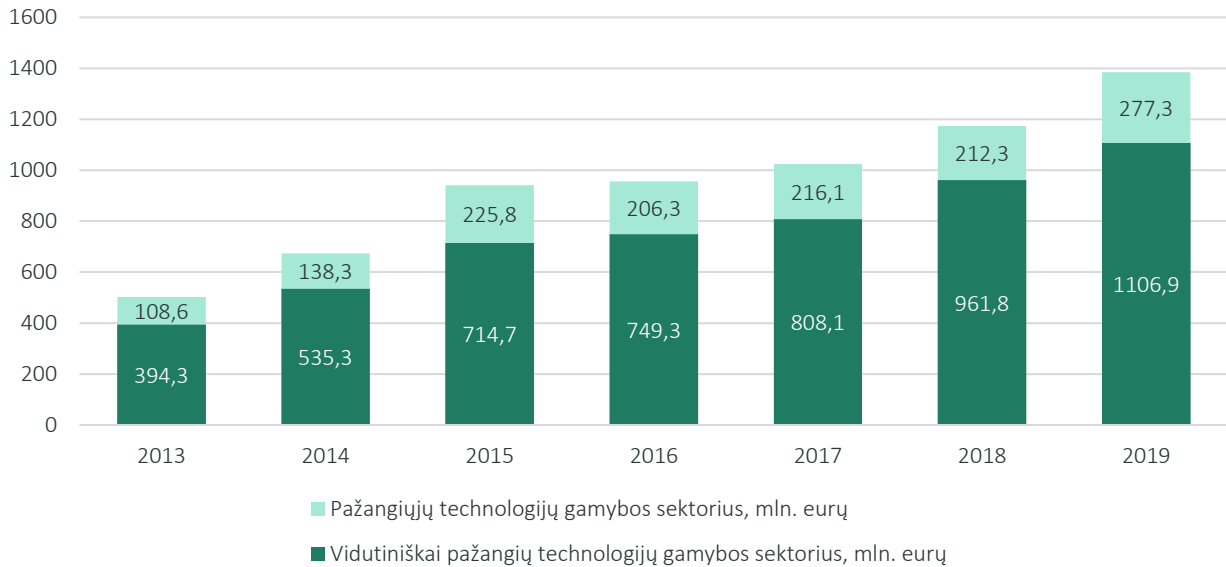
Šaltinis: STRATA, Lietuvos inovacijų ekosistemos apžvalga, sudaryta Konsultanto

Taip pat kartu proporcingai auga ir šių sektorių gamybos pridėtinė vertė. 2019 m. duomenimis, pažangiųjų ir vidutiniškai pažangių technologijų gamybos sektoriaus pridėtinė vertė sudarė 2,8 proc. BVP. Tai geriausias 2013 – 2019 m. laikotarpio rezultatas.

⁸⁴ STRATA, Lietuvos inovacijų ekosistemos apžvalga, 2021 m. Prieiga internetu: <https://strata.gov.lt/wp-content/uploads/2024/01/20210324-inovaciju-apzvalga-2021.pdf>

⁸⁵ Ten pat

Pažangiųjų ir vidutiniškai pažangiųjų technologijų gamybos sektoriaus pridėtinė vertė



19 paveikslas. Pažangiųjų ir vidutiniškai pažangiųjų technologijų gamybos sektoriaus pridėtinė vertė
Šaltinis: STRATA, Lietuvos inovacijų ekosistemos apžvalga, sudaryta Konsultanto

Skaitmeninių technologijų naudojimas versle yra viena iš inovatyvaus verslo sektoriaus plėtros priedaidų. Pagal 2020 m. Skaitmeninės ekonomikos ir visuomenės indeksą (DESI) Lietuvos skaitmeninių technologijų integracijos versle lygis (49,5 balo) yra aukščiausias tarp Baltijos šalių ir viršija ES rezultatą (41,4 balo). Pagal šį rodiklį Lietuva užima 10 vietą ES.⁸⁶

Lietuvoje taip pat didėja skaičius įmonių, kurios stengiasi neatsilikti nuo inovatyvių sprendimų ir įtraukia dirbtinio intelekto įrankius į savo darbotvarkes siekiant optimizuoti įmonės darbo greitį ir efektyvumą. Pavyzdžiui, 2021 m. įmonių, naudojančių dirbtinio intelekto technologijas, procentinė dalis Lietuvoje siekė 4,5 proc., tuo tarpu 2024 m. šis rodmuo padidėjo iki 8,8 proc. – beveik du kartus.⁸⁷ Lentelėje toliau pateikti duomenys reprezentuoja tai, jog didėjanti informacijos ir ryšių sektoriaus juridinių asmenų proporcija prisideda prie efektyvesnio pridėtinės vertės kūrimo. Besiplečiant informacijos ir ryšių sektoriui tolygiai auga ir pridėtinė vertė gamybos sąnaudoms.

⁸⁶ STRATA, Lietuvos inovacijų ekosistemos apžvalga, 2021 m. Prieiga internetu: <https://strata.gov.lt/wp-content/uploads/2024/01/20210324-inovaciju-apzvalga-2021.pdf>

⁸⁷ OSP, „Įmonės naudojančios dirbtinio intelekto technologijas ir naudojimo tikslai“. Prieiga internetu: <https://osp.stat.gov.lt/lt/statistiniu-rodikliu-analize?hash=5d4aaffd-8181-402a-9e89-4fc20ea0d372>

7 lentelė. Pridėtinė vertė gamybos sąnaudoms pagal ekonominės veiklos rūšis (konkrečiai lyginant informacijos ir ryšių veiklos rūšį ir bendrą ekonominės veiklos rūšių sumą) tūkst. Eur

| | 2019 | 2020 | 2021 | 2022 | 2023 |
|-----------------------|-------------|------------|------------|------------|------------|
| Iš viso | 23 273 337 | 24 777 165 | 29 967 259 | 36 498 142 | 38 420 580 |
| Informacija ir ryšiai | 1 407 041 | 1 560 198 | 1 841 076 | 2 436 450 | 3 062 919 |
| Procentinė dalis | 6,045 proc. | 6,29 proc. | 6,14 proc. | 6,67 proc. | 7,97 proc. |

Šaltinis: Valstybės duomenų agentūra, sudaryta konsultanto

Taip pat Lietuva iš bendros pagamintos produkcijos šalyje eksportuoja 14 proc. (2023 m.) aukštosios technologijos produktų, kurie kuria pridėtinę vertę bei atneša didesnes pajamas.⁸⁸ Aukštųjų technologijų eksportas 2023 m. sudarė apie 3,37 milijardai Eur pajamų. Šis skaičius kiekvienais metais stabiliai auga nuo 2015 m.⁸⁹

Siekiant susidaryti platesnį bei išsamesnį vaizdą apie Lietuvoje veikiančias ir įsikūrusias IT paslaugų sektoriaus įmones, kurios potencialiai galėtų prisidėti prie Kultūros Ministerijos projekto Technologinio sprendinio kūrimo, remiantis viešai prieinamais šaltiniais – Rekvizitai.Lt, buvo atrinkta 10 įmonių pagal jų paslaugų sritį, darbuotojų skaičių, pelningumą bei dalyvavimą/nedalyvavimą viešuosiuose projektuose. Nors šias įmones skiria jų pelningumo lygis, darbuotojų skaičius bei aktyvumas viešuosiuose pirkimuose, atrinktų įmonių įvairovė padeda susidaryti įvairesnį vaizdą apie IT sektoriaus įmonių pajėgumą, skirtumus, verslo modelį. Optimaliausios įmonės Technologinio sprendimo įgyvendinimui, tikėtina, būtų šios:

- Asseco Lietuva, UAB;
- CGI Lithuania, UAB;
- Edrana Baltic, UAB;
- Novian grupė (Novian Systems, UAB, Novian Pro, UAB, Novia Technologies, UAB ir t.t.);
- NRD System, UAB;
- Reiz Tech, UAB;
- SUPER HOW, UAB;
- Telesoftas, UAB;
- The Infotrust, UAB;
- Tieto Lietuva, UAB.

Šios įmonės pasirinktos dėl to, kad jų darbo modelis yra sutelktas paslaugų srityje kuriant naujas kompiuterines programas bei siūlant specifines problemas sprendžiančius technologinius sprendimus verslo bei viešųjų institucijų partneriams. Taip pat jos dalyvauja viešuosiuose pirkimuose ir jau turi darbo patirties teikiant sprendimus viešojo sektoriaus įstaigoms. Minėtos įmonės jau yra bendradarbiavusios viešuosiuose projektuose su tokiomis institucijomis, kaip: Užimtumo tarnyba prie Lietuvos Respublikos socialinės apsaugos ir darbo ministerijos, Lietuvos Statistikos Departamentas, Nacionalinė teismų administracija, Viešoji įstaiga Centrinė projektų valdymo agentūra, Finansinių nusikaltimų tyrimo tarnyba prie Lietuvos Respublikos vidaus reikalų ministerijos ir kitos. Verta peržiūrėti projektus, kurių įvykdymas galėtų reikšmingai reprezentuoti IT įmonės kompetentingumą bei tinkamumą Kultūros Ministerijos Technologinio sprendimo kūrimui.

ASSECO LIETUVA, UAB dalyvauja UAB Vilniaus vandenų projekte, kuriant Finansų apskaitos, valdymo apskaitos ir klientų apskaitos (FAVAKA) sistemą. Įmonė Asseco Lietuva sukūrė, įdiegė ir toliau palaiko bei vysto informacinę sistemą Užimtumo tarnybos prie Lietuvos Respublikos socialinės apsaugos ir darbo ministerijai. Taip pat įmonė dalyvauja Lietuvos kalėjimų tarnybos paskelbtame projekte 2023 m. Lietuvos kalėjimų tarnybos informacinės sistemos (KADIS–2) kūrimo. Ši sistema siekia užtikrinti vidinių paslaugos teikimo procesų skaitmeninimą. Tam taip pat reikalinga dirbtinio intelekto integracija, procesų automatizavimas, veiklos analizės duomenimis pagrįsti sprendimai. Technologinis sprendimas siekia užtikrinti vienkartinio duomenų pateikimo principą, t. y. visus reikiamus dokumentus siekiama pateikti vienoje vietoje, sukurtos integracinės sąsajos su kitomis informacinėmis

⁸⁸ World Bank, High-technology exports (% of manufactured exports) – Lithuania. Prieiga internetu: <https://data.worldbank.org/indicator/TX.VAL.TECH.MF.ZS?view=chart&locations=LT>

⁸⁹ World bank, High-technology exports (current US\$) – Lithuania. Prieiga internetu: <https://data.worldbank.org/indicator/TX.VAL.TECH.CD?end=2023&locations=LT&start=2007>

sistemomis, registrais pakartotinai leis naudoti (keistis) institucijų jau surinktais duomenimis. Šios sistemos prototipas taip pat reprezentuoja inovatyvių sprendimų integraciją moderniuose sprendimuose pasitelkiant IT sistemos automatizavimą bei sklandesnę informacijos sklaidą tarp skirtingų institucijos vienetų.

CGI LITHUANIA, UAB – CGI paslaugos apima verslo ir IT konsultacijas, sistemų integravimą, programų kūrimą ir priežiūrą, infrastruktūros valdymą bei 150 IP paslaugų ir sprendimų. Šios įmonės patirtis byloja, jog įmonė aktyviai teikia paslaugas tokioms institucijoms, kaip Viešojo valdymo agentūra (VSDR IS), VĮ Registrų centras (Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos plėtra), Kauno miesto savivaldybės administracija, prisidedant būtent prie institucijų informacinių sistemų kūrimo. Įmonė taip pat teikia paslaugas įvairioms institucijoms prižiūrint bei modifikuojant pastarųjų informacinius portalus.

UAB EDRA BAL TIC daugiausiai teikia paslaugas sveikatos apsaugos įstaigoms, kaip Antakalnio poliklinika bei Kėdainių ligoninė. Įmonė kuria programinę įrangą, pritaikytą sveikatos apsaugos įstaigų poreikiams užtikrinti. Kadangi sveikatos įstaigų informacinės sistemos dažnai pasižymi nemažu informacijos srautu bei apkrova, tikėtina, jog Edra Baltic sukaupta patirtis galėtų prisidėti prie Technologinio sprendimo kūrimo ieškant geriausio būdo efektyviai apdoroti informaciją bei ją kaupti ir panaudoti informuojant Technologinio sprendimo naudotojus.

NOVIAN GRUPĖ, kurią sudaro UAB Novian pro ir UAB Novian Systems kompanijos, teikė projektą Muitinės Departamentui. Projekto objektas buvo sukurti centralizuotą dirbtiniu intelektu grįstą rentgeno vaizdų analizės sistemą ir sąlygas tolimesniam autonomiškam sistemos mokymui bei užtikrinti nepertraukiamą, stabilų ir efektyvų sistemos veikimą, siekiant pagerinti ir paspartinti muitinės rizikos valdymą ir tikrinimą. Šis projektas pasižymi inovatyvumu, įtraukiant dirbtinio intelekto naudojimą, taip pat yra pritaikytas sistemos analizei – informacijos rinkimui, sisteminimui bei automatiškam sistemos tobulėjimui suteikiant efektyvaus veikimo garantiją.

NRD SYSTEM, UAB – informacinių technologijų įmonė, kuri specializuojasi registrų kūrimo ir plėtros srityje bei teikia informacinių sistemų kūrimo, plėtros, priežiūros, registrų reformų ir IT projektų techninės priežiūros paslaugas tiek Lietuvos, tiek užsienio rinkose. Centrinėje Viešųjų pirkimų informacinėje sistemoje nėra duomenų apie projektus, kuriuose dalyvavo ši įmonė, tačiau atsižvelgiant į šios įmonės specifikaciją bei darbo sritį, galima ją priskirti prie pakankamai kompetentingos Technologinio sprendimo kūrimui Kultūros Ministerijai.

REIZ TECH, UAB – kompiuterinių ir programinių įrangų kūrimo įmonė, teikianti paslaugas IT sektoriaus paslaugas. Reiz Tech dalyvavo Lietuvos Banko paskelbtame projekte – informacinių sistemų kūrimo komandos paslaugų pirkime. Paslaugų teikėjas įsipareigojo teikti informacinių sistemų kūrimo komandos paslaugas, susijusias su Lietuvos banko eksploatuojamos mokėjimų sistemos CENTROLink (toliau – Sistema) plėtra ir priežiūra. Paslaugų tikslas – užtikrinti sistemos veikimą pagal atitiktus reikalavimus ir efektyvų sistemos naudojimą. Sistema yra Lietuvos banko mokėjimų sistema, sudaranti techninę galimybę visiems Europos ekonominėje erdvėje licencijuotiems mokėjimų paslaugų teikėjams prisijungti prie bendros mokėjimų eurais erdvės (SEPA) naudojantis Lietuvos banko infrastruktūra ir vykdyti joje momentinius, kredito ir debeto mokėjimus. CENTROLink sistema pasižymi didele apkrova bei mokėjimų srautu ir tikimasi, jog Reiz Tech patirtis šiame projekte galėtų būti naudinga, kuriant Technologinį sprendimą.

SUPER HOW, UAB – komanda specializuojasi blokų grandinės technologijų taikyme bei dirbtinio intelekto technologijose nuo 2014 m. Turi sukauptos patirties tiek konsultuojant projektus dirbtinio intelekto panaudojimo, semantikos, didžiųjų duomenų analizės klausimais, tiek analizuojant blokų grandinių technologijos panaudojimo versle galimybes. Įmonė taip pat dalyvauja užsakomuosiuose moksliniuose tyrimuose bei kuria inovacijas – sudėtingas paskirstytųjų resursų technologijos infrastruktūras, semantinius modelius, protokolus bei algoritmus.

TELESOFTAS, UAB taip pat dalyvauja viešuose pirkimuose ir dažnai siūlo savo JAVA specialistų paslaugas tokioms institucijoms kaip Vilniaus Miesto savivaldybės administracija bei VĮ Registrų Centras taip suteikdami pagalbą šių institucijų informacinių sistemų vystymui.

THE INFOTRUST, UAB dažnai viešųjų pirkimų metu teikia specialistų mokymų paslaugas, pavyzdžiui, Valstybės sienos apsaugos tarnybai prie Lietuvos Respublikos vidaus reikalų ministerijos bei Kauno miesto savivaldybės administracijai siekiant tobulinti pastarųjų institucijų darbuotojų kompiuterinį raštingumą.

TIETO LIETUVA, UAB įmonė aktyviai teikia informacinių technologinių paslaugas tokioms bendrovėms, kaip Lietuvos Bankas, Registrų centras. Pavyzdžiui, įmonė neseniai pradėjo teikti Lietuvos bankui konsultacines paslaugas

siekiant užtikrinti Lietuvos banko eksploatuojamos mokėjimų sistemos CENTROLink (toliau – CENTROLink) plėtrą ir priežiūrą. CENTROLink yra Lietuvos banko mokėjimų sistema, sudaranti techninę galimybę visiems Europos ekonominėje erdvėje licencijuotiems mokėjimo paslaugų teikėjams prisijungti prie bendros mokėjimų eurais erdvės (SEPA) naudojantis Lietuvos banko infrastruktūra ir vykdyti joje momentinius, kredito ir debeto mokėjimus. Tai yra viena iš svarbiausių mokėjimo sistemų Lietuvoje vien dėl to, nes Lietuvos bankas yra nacionalinis–centrinis Lietuvos bankas ir prižiūri visų likusių Lietuvoje veikiančių bankų veiklą. Tai pagrindžia, jog įmonė turi pakankamai kompetentingų specialistų, gebančių apsiimti konsultacine bei technine veikla vienoms iš svarbiausių Lietuvos institucijų tuo pačiu užtikrinant sistemų efektyvumą suvaldant masyvų informacijos srautą. Kadangi informacinių sistemų specialistai šiame projekte koncentruojasi ties automatizavimo užtikrinimu bei tobulinimu, tikimasi, jog patirties metu sukauptos žinios galėtų pasitarnauti kuriant Technologinio sprendimo sistemą.

Apibendrinant, Lietuvos IT sprendimų kūrėjai yra pajėgus sukurti siūloma Technologinį sprendimą.

Priedai

1 priedas. Kuriamo technologinio sprendimo techninė specifikacija

Atsižvelgiant į 3.2 skyriuje pateiktą informaciją, toliau pateikiama techninė specifikacija Technologiniam sprendimui sukurti.

8 lentelė. Galimybių studijos priedas – Kuriamo Technologinio sprendimo techninė specifikacija

| Nr. | Reikalavimai |
|-------------------------|--|
| Funkciniai reikalavimai | |
| FR-1 | Kuriamo Technologinio sprendimo (toliau – KTS) tikslas – patogiai informuoti naudotoją apie galimai nelegalų turinį. KTS turėtų būti patrauklus tikslinėms grupėms, tam turėtų būti taikomi geriausi vizualiniai ir techniniai sprendimai. |
| FR-2 | KTS turi sudaryti FR-2.1–FR-2.5 punktuose nurodytos funkcinės dalys: |
| FR-2.1 | naršyklės įskiepis, kuri naudotojas gali parsisiųsti ir įdiegti palaikomose sistemose (žr. Nefunkcinius reikalavimus); |
| FR-2.2 | serverio pusė ir duomenų bazė, kurios skirtos KTS duomenų saugojimui ir naršyklės įskiepio (žr. FR-2.1) funkcionalumui užtikrinti; |
| FR-2.3 | integracinės sąsajos (angl. API – <i>Application Programming Interfaces</i>), kurios skirtos gauti ir teikti duomenis į išorinius duomenų šaltinius ir sistemas bei naršyklės įskiepius (duomenų atnaujinimo modulis, integracinių sąsajų modulis, analitinis modulis); |
| FR-2.4 | valdymo aplinka, kuri skirta KTS sistemos administratorių darbui užtikrinti.; |
| FR-2.5 | DI užklausų modulis, kuris užtikrina galimybę naudotojui pateikti užklausas DI platformoms pagal valdymo aplinkoje nustatytas taisykles. |
| FR-3 | Naršyklės įskiepis, aprašytas FR-2.1 punkte, turi atitikti FR-3.1–FR-3.8 punktuose nurodytus funkcinis reikalavimus: |
| FR-3.1 | turi turėti užklausos sudarymo ir pateikimo į serverį (žr. FR-2.2) funkcijas; |
| FR-3.2 | turi turėti naudotojo lankomų internetinių svetainių duomenų surinkimo funkciją; |
| FR-3.3 | turi turėti iš serverio pusės gauto nelegalių internetinių svetainių sąrašo saugojimo funkciją; |
| FR-3.4 | turi turėti aplankytos svetainės duomenų sulginimo su lokaliai saugomu nelegalių svetainių sąrašu funkciją; |
| FR-3.5 | turi turėti pranešimų pateikimo naudotojui funkciją. Naudotojui turi būti rodomas pranešimas apie aptiktą legalų, nelegalų turinį arba galimybės nustatyti, ar turinys (ne)legalus, nebuvimą; |
| FR-3.6 | turi turėti patogaus laikino išjungimo funkciją; |
| FR-3.7 | turi turėti duomenų rinkimo analitiniais tikslais funkciją. Analitiniais tikslais renkamų duomenų sąrašą pasiūlo Paslaugų teikėjas ir suderina su Perkančiąja organizacija; |
| FR-3.8 | turi turėti pasiūlymo palikti atsiliepiamą platinimo platformose ir tiesiogiai administruojančiai institucijai funkciją. |
| FR-4 | Serverio pusė, duomenų bazė ir integracinių sąsajų moduliai, turi atitikti FR-4.1–FR-4.5 punktuose nurodytus funkcinis reikalavimus: |

| Nr. | Reikalavimai |
|---------|---|
| FR-4.1 | turi turėti duomenų apie nelegalų turinį platinančias svetaines saugojimo funkciją; |
| FR-4.2 | turi turėti užklausų gavimo iš naršyklės įskiepio ir apdorojimo (atnaujinto nelegalių svetainių sąrašo pateikimo įskiepiui) funkciją; |
| FR-4.3 | turi turėti užklausų pateikimo į išorinius informacijos šaltinius (duomenų gavimas, pranešimų pateikimas) funkciją; |
| FR-4.4 | turi turėti statistinių duomenų apie naudotojų elgesį ir kitus KTS aspektus rinkimo funkciją (analitinis modulis). Renkamų statistinių parametrų sąrašas suderinamas su Perkančiąja organizacija prototipo kūrimo metu; |
| FR-4.5 | turi turėti rezervinių kopijų formavimo ir duomenų atstatymo pagal rezervines kopijas funkciją. Rezervinių kopijų formavimo dažnis ir taisyklės gali būti keičiami valdymo aplinkoje. |
| FR-5 | Valdymo aplinka turi atitikti FR-5.1– FR-5.12 punktuose nurodytus funkcinius reikalavimus: |
| FR-5.1 | turi turėti autorizuotų naudotojų (sistemos administratorių) prisijungimo prie sistemos ir atsijungimo nuo sistemos funkciją; |
| FR-5.2 | turi turėti autorizuotų naudotojų paskyrų sukūrimo naudojant grafinę naudotojo sąsają (toliau – GNS) funkciją; |
| FR-5.3 | turi turėti įrašų duomenų bazėje redagavimo, šalinimo, pildymo naudojant GNS funkciją. Tai apima nelegalių ir legalių svetainių sąrašo rankinį redagavimą; |
| FR-5.4 | turi turėti duomenų bazėje saugomų duomenų struktūros keitimo naudojant GNS funkciją; |
| FR-5.5 | turi turėti statistinių ataskaitų peržiūros ir parsisiuntimo su Perkančiąja organizacija suderintais formatais (XLSX, CSV, JSON, XML) naudojant GNS funkciją; |
| FR-5.6 | turi turėti darbo su naudotojų sąrašo informacija (naudotojų pagal identifikacinius numerius blokavimas, veiklos tikrinimas) naudojant GNS funkciją; |
| FR-5.7 | turi turėti integracinių sąsajų su išoriniais informacijos šaltiniais nustatymo naudojant GNS funkciją. Tai apima nelegalių ir legalių svetainių sąrašo dalinį arba pilną atnaujinimą remiantis išoriniais informacijos šaltiniais; |
| FR-5.8 | turi turėti naudotojo pranešimų apie nelegalų turinį rankinio apdorojimo ir automatinio apdorojimo algoritmų nustatymo naudojant GNS funkciją; |
| FR-5.9 | turi turėti skirtingus autorizuotų naudotojų (prie valdymo aplinkos prieigą turinčių naudotojų) lygius. Lygiai skiriasi pagal turimą prieigą prie skirtingų valdymo aplinkos funkcijų. Šių lygių nustatymas ir priskyrimas autorizuotiems naudotojams nustatomas naudojant GNS funkciją. Sistemos veikimo pradžioje nustatyti du autorizuotų naudotojų tipai – administratoriaus (prieinamas visas administratoriaus aplinkos funkcionalumas) ir moderatoriaus (turi prieigą prie visų funkcionalumų, tačiau be redagavimo teisės); |
| FR-5.10 | turi būti užtikrinama galimybė keisti rezervinių kopijų formavimo dažnį, taisykles ir susijusius nustatymus. Užtikrinama žurnalų saugojimo termino keitimo funkcija; |
| FR-5.11 | turi būti užtikrinama naudotojų skatinimo palikti atsiliepimą taisyklės (kokioms sąlygoms esant naudotojui įskiepis pasiūlo palikti atsiliepimą); |
| FR-5.12 | turi būti užtikrinamas DI integracinio modulio nustatymas (palaikomos platformos, naudotojo užklausų dienos limitas ir kitos susijusios funkcijos). |
| FR-6 | DI užklausų modulis turi atitikti FR-6.1– FR-5.6 punktuose nurodytus funkcinius reikalavimus: |

| Nr. | Reikalavimai |
|----------------------------------|---|
| FR-6.1 | turi turėti užklausų iš naudotojo įskiepių gavimo funkciją (gaunamas svetainės, kurią reikia patikrinti, pirminis kodas); |
| FR-6.2 | turi užtikrinti didžiausio dienos užklausų skaičiaus limito taikymo naudotojams funkciją; |
| FR-6.3 | turi turėti patikrinimo, ar duomenų bazėje nėra išsaugoto DI atsakymo dėl šios svetainės, funkciją; |
| FR-6.4 | turi turėti DI užklauso teksto suformavimo pagal valdymo aplinkoje nustatytas taisykles funkciją; |
| FR-6.5 | turi turėti užklauso DI pateikimo ir atsakymo gavimo funkciją, įskaitant visas funkcijas, būtinas darbui su DI platformomis. Palaikomų DI platformų sąrašas suderinamas su Perkančiąja organizacija; |
| FR-6.6 | turi turėti DI atsakymo interpretavimo, įrašo duomenų bazėje suformavimo ir atsakymo naudotojo įskiepiui pateikimo funkciją. |
| Nefunkciniai reikalavimai | |
| NR-1 | KTS turi atitikti reikalavimus architektūrai: |
| NR-1.1 | turi įgyvendinti plečiamumo principą (angl. <i>scalability</i>). Programinis kodas neturi riboti KTS našumo (tuo pačiu metu prisijungusių vartotojų skaičiaus); |
| NR-1.2 | turi būti įgyvendinamas atviro kodo principas. Atviro kodo principo įgyvendinimo apimtis ir būdai suderinami su Perkančiąja organizacija prieš pradėdant prototipo kūrimą; |
| NR-1.3 | turi būti sukurtas modulinės informacinės sistemos principu. Esant poreikiui, turi būti galimybė, neperprogramuojant KTS, įdiegti jame papildomus modulius ar funkcionalumus. |
| NR-2 | KTS turi atitikti reikalavimus saugumui: |
| NR-2.1 | Paslaugų teikėjas atlieka Duomenų apsaugos poveikio vertinimą (angl. <i>Data Protection Impact Assessment, DPIA</i> , toliau – DPAV). DPAV suderinama su Perkančiąja organizacija. Turi būti užtikrinta, kad taikomi technologiniai sprendimai užtikrina sistemos apsaugą, nustatytų rizikų valdymą ir atitiktį gerosioms praktikoms; |
| NR-2.2 | visais atvejais, išskyrus tuos, kur kitaip neįmanoma įgyvendinti KTS tikslo, būtina užtikrinti naudotojų duomenų anonimiškumą, nebereikalingų duomenų automatinį šalinimą be galimybės atkurti; |
| NR-2.3 | turi būti užtikrinamas saugumas naršyklės įskiepio lygmeniu, duomenų bazės lygmeniu; |
| NR-2.4 | ryšys tarp serverio pusės ir naršyklės įskiepio turi būti šifruojamas naudojant SSL (angl. <i>Secure Socket Layer</i>) arba kitas lygiavertes šifravimo priemones. |
| NR-3 | KTS turi atitikti reikalavimą greitaveikai – tuo pat metu KTS turėtų gebėti naudotis ne mažiau 10 000 naudotojų. Tiekėjas turės pateikti greitaveikos testavimo rezultatus. Turi būti numatytos galimybės ateityje plėsti įskiepio našumą. |
| NR-4 | KTS turi atitikti suderinamumo reikalavimus: |
| NR-4.1 | turi būti užtikrintas veikimas „Chrome“ (taip pat naršyklėse, kurios naudoja „Chrome“ naršyklės pagrindą ir kurios palaiko tokio pobūdžio įskiepius) ir „Firefox“ naršyklių versijose Windows, MacOS ir Linux platformose, taip pat „Safari“ naršyklių versijose MacOS, iOS, iPadOS platformose ir „Firefox for Android“ naršyklių versijose Android platformose; |
| NR-4.2 | turi būti užtikrintas tinkamas funkcinų reikalavimų išpildymas iOS, iPadOS ir Android platformose, atsižvelgiant į šių platformų apribojimus. |

| Nr. | Reikalavimai |
|----------|---|
| NR-5 | KTS turi atitikti patogumo ir naudotojo patirties reikalavimus: |
| NR-5.1 | turi būti užtikrintas atitikimas naudotojo patirties reikalavimams, numatytiems Žiniatinklio turinio prieinamumo gairėse (angl. Web Content Accessibility Guidelines (WCAG), toliau – ŽTPG). Šios gairės apima, tačiau neapsiriboja toliau pateiktais reikalavimais: |
| NR-5.2 | Paslaugų teikėjas privalo pateikti Perkančiajai organizacijai 3 KTS dizaino sprendimų variantus, kur būti grafiškai pavaizduoti skirtingi KTS scenarijai, detalizuojama atitiktis ŽTPG. Atsižvelgiant į mobilių platformų specifiką, turi būti parengtas atskiras pasiūlymas šioms platformoms. |
| NR-6 | Paslaugų teikėjas privalo įvykdyti šiuos KTS sukūrimo ir paruošimo praktinei veiklai reikalavimus: |
| NR-6.1 | su Perkančiąja organizacija suderinami atviro kodo principo įgyvendinimo būdai. Turi būti naudojama Elastic License v2 licencija, pirminis kodas (po KTS sukūrimo) turi būti viešinamas viešose kodo saugyklose. Paslaugų teikėjas atsakingas už viešos kodo saugyklos tinkamų nustatymų parinkimą su Perkančiąja organizacija suderinta tvarka; |
| NR-6.2 | su Perkančiąja organizacija suderinta tvarka paruošti KTS prototipą, kuris leistų patikrinti visus funkcinis reikalavimus ir su Perkančiąja organizacija suderintus nefunkcinius reikalavimus. Patikrinimas (testavimas) turi būti įgyvendinamas su žmonėmis (testuotojais) ir su automatizuotais testavimo sprendimais, kurias Paslaugų teikėjas privalės paruošti kartu su testavimo aplinka. Atliekant testavimus visais atvejais turi būti tinkamai išpildomi funkciniai ir nefunkciniai reikalavimai. DI atsakymų tikslumas turi viršyti 95 proc. Testuojami šie scenarijai: |
| NR-6.2.1 | nelegalių ir legalių šaltinių sąrašo atnaujinimas; |
| NR-6.2.2 | klaidų nelegalių ir legalių šaltinių sąrašė nustatymas; |
| NR-6.2.3 | didelės apkrovos (tuo pačiu metu Technologiniu sprendimu naudojami 10 000 žmonių) atsiradimas; |
| NR-6.2.4 | nustatymų keitimas sistemos veikimo metu; |
| NR-6.2.5 | kiekvieno iš sistemos išorinio sistemos elemento funkcionalumo praradimas; |
| NR-6.2.6 | skirtingų svetainių vertinimas; |
| NR-6.2.7 | veikimas skirtingose platformose (naršyklėse, operacinėse sistemose); |
| NR-6.2.8 | kiti su Perkančiąja organizacija suderinti scenarijai. |
| NR-6.3 | paruošti ir su Perkančiąja organizacija suderinti paslaugų lygio susitarimą (angl. SLA); |
| NR-6.4 | paruošti ir su Perkančiąja organizacija suderinti atsakingo atkleidimo proceso įgyvendinimą; |
| NR-6.5 | paruošti ir su Perkančiąja organizacija suderinti techninę dokumentaciją ir naudotojo instrukciją. Techninėje dokumentacijoje ir naudotojo instrukcijoje turi būti detalai aprašytas technologinio sprendimo veikimas, darbo su juo galimybės ir apribojimai. Turi apimti, bet neapsiriboti, atsarginių kopijų sukūrimo ir atkūrimo procesas; |
| NR-6.6 | užtikrinti, kad galutinė KTS versija atitiktų platinimo platformų keliamus reikalavimus. Platinimo platformų sąrašas suderinamas su Perkančiąja organizacija; |
| NR-6.7 | galutinė Perkančiajai organizacijai perduodama KTS versija turi atitikti visus techninės specifikacijos reikalavimus, turi būti pilnai paruošta praktiniam veikimui. |

Šaltinis: sudaryta Konsultanto