

Kai asmens tapatybė panaudojama be sutikimo: civilinė atsakomybė už veido, balso ir judesių pavertimą „deepfake“ turiniu

Andrius Viljamas Gontier, Aurėja Sodytė

Vilniaus universiteto Teisės fakulteto

4 kurso studentai

Saulėtekio al. 9, I rūmai, 10222, Vilnius

El. paštas: andrius.gontier@tf.stud.vu.lt, aureja.sodyte@tf.stud.vu.lt

Mokslinio straipsnio akademinis kuratorius asist. dr. Tadas Varapnickas

El. paštas: tadas.varapnickas@tf.vu.lt

Mokslinio straipsnio praktinė kuratorė asist. dr. Neringa Gaubienė

El. paštas: neringa.gaubiene@tf.vu.lt

Anotacija. *Skaitmeninių technologijų amžiuje asmens tapatybė gali būti pasisavinta pasitelkiant šiuolaikines dirbtinio intelekto technologijas, leidžiančias kurti itin tikroviškas sintetines vaizdo ir garso klastotes (toliau – „deepfake“), kuriose atkuriami bei vaizduojami asmens veido bruožai, balsas ar judesiai be jo sutikimo. Šiame darbe nagrinėjamas civilinės atsakomybės taikymas tais atvejais, kai asmens tapatybės elementai be asmens sutikimo panaudojami kuriant ir platinant „deepfake“ turinį. Darbe analizuojama asmens tapatybės ir biometrinių duomenų samprata, galiojančių civilinės teisės ir Europos Sąjungos duomenų apsaugos normų taikymas bei Lietuvos ir užsienio teismų praktika.*

Pagrindiniai žodžiai: *biometriniai duomenys, duomenų apsauga, dirbtinis intelektas, asmens neturtinės teisės, civilinė atsakomybė.*

Keywords: *biometric data, data protection, artificial intelligence, personal moral rights, civil liability.*

Įvadas

Tyrimo aktualumas. Skaitmeninėje erdvėje vis dažniau pasitaiko situacijų, kai riba tarp realaus asmens ir dirbtinai atkuriamo jo atvaizdo tampa beveik nepastebima. Dirbtinio intelekto technologijos lėmė, kad tai, kas anksčiau atrodė neįmanoma, tampa lengvai įgyvendinama net ir neturint specifinių žinių. Šiandien vis lengviau su-

kurti vaizdo ar garso turinį, kuriame realų asmenį identifikuojantys elementai atkuriami ir vaizduojami taip įtikinamai, kad tampa sunku atskirti tikrovę nuo dirbtinai sukurto vaizdo. Tai kelia rimtų iššūkių asmens tapatybės apsaugai, ypač tais atvejais, kai ji panaudojama be asmens sutikimo. Šią problemą išryškina ir viešai aptariamai pavyzdžiai, tokie kaip žymaus turinio kūrėjo bei boksininko Jake'o Paulo atvejis, kai dirbtinio intelekto pagalba buvo kuriami vaizdo įrašai su jo atvaizdu, vaizduojant jį netikėtose, realybėje neįvykusiose situacijose.¹ Panašaus pobūdžio pavyzdys fiksuotas ir Lietuvoje, kai socialinėje erdvėje išplito vaizdo įrašas, kuriame Ministrė Pirmininkė Inga Ruginienė vaizduojama šokanti. Tai sukėlė diskusijas dėl tokio turinio teisėtumo ir asmens tapatybės apsaugos.² Nors tokie pavyzdžiai gali atrodyti kaip pramoga ar eksperimentas, jie parodo, kaip lengvai asmens tapatybė skaitmeninėje erdvėje gali būti perimta, pakeista ar panaudota. Atsižvelgiant į tai, minėtų aplinkybių kontekste tyrimo aktualumą lemia ir civilinės atsakomybės taikymo problematika neteisėto asmens tapatybės elementų panaudojimo „deepfake“ turinyje atvejais.

Tyrimo tikslas. Išanalizuoti civilinės atsakomybės taikymą, kai asmens tapatybės elementai – veidas, balsas ar judesiai – be asmens sutikimo panaudojami kuriant ir platinant „deepfake“ turinį.

Tyrimo objektas. Asmens tapatybės elementų panaudojimas „deepfake“ technologijų kontekste. Asmens tapatybę sudaro įvairūs identifikavimo elementai, įskaitant dokumentinius duomenis (vardą, pavardę, gimimo datą), biometrinius požymius (veido atvaizdą, balsą, judesius), taip pat skaitmeninės, fiziologinės ar socialinės tapatybės aspektus. Šiame darbe apsiribojama veido, balso ir judesių kaip biometrinių asmens tapatybės elementų analize, todėl kiti asmens tapatybės elementai sąmoningai nenagrinėjami.

Tyrimo uždaviniai

- Atskleisti asmens tapatybės ir biometrinių duomenų, kaip teisiškai saugomų tapatybės elementų, reikšmę civilinėje teisėje bei jų panaudojimo vertinimą „deepfake“ technologijų kontekste, siekiant nustatyti civilinės atsakomybės taikymo prielaidas neteisėto veido, balso ir judesių panaudojimo atvejais.
- Išnagrinėti „deepfake“ technologijų sampratą, jų kategorijas ir teisinę reikšmę asmens tapatybės panaudojimo požiūriu.
- Įvertinti asmens neturtinių teisių – teisės į atvaizdą, privataus gyvenimo bei garbės ir orumo – apsaugos taikymą civilinėje teisėje „deepfake“ turinio kūrimo ir platinimo atvejais.

¹ CARMAUX, Jules (2025). *Jake Paul's AI Gambit: Investments and Deepfake* [interaktyvus]. <https://www.clickanalytic.com/jake-pauls-ai-gambit-investments-deepfake/>

² Delfi (2026-01-12). *Dirbtiniu intelektu sukurtas Ingos Ruginienės šokis papiktino lietuvius: paduočiau į teismą* [interaktyvus]. <https://www.delfi.lt/veidai/zmones/ingos-ruginienes-sokis-papiktino-lietuvius-paduociau-i-teisma-120197097>.

Tyrimo metodai. Doktrininis (analizės) metodas pasitelktas giluminei teisės normų analizei atlikti. Taip pat taikytas sisteminis metodas, leidžiantis analizuoti civilinės teisės normas, atsižvelgiant į asmens duomenų apsaugos reglamentavimą, vertinant asmens tapatybės apsaugą skaitmeninėje erdvėje. Teleologinis (tikslų) aiškinimo metodas naudojamas įvertinti nagrinėjamų normų paskirtį. Taip pat tyrime remtasi loginės analizės ir sintezės metodais formuluojant išvadas.

Problemos ištirimo laipsnis. Asmens tapatybės elementų panaudojimo „deepfake“ technologijose problematika Lietuvos teisės doktrinoje nagrinėta ribotai. Daugiausia dėmesio skiriama asmens duomenų ir privatumo apsaugai, o civilinės atsakomybės taikymas už neteisėtą veido, balso ar judesių panaudojimą išsamiai neanalizuotas.

Tyrimo originalumas. Darbo originalumą lemia tai, kad asmens tapatybės elementų panaudojimas „deepfake“ manipuluotame turinyje analizuojamas civilinės atsakomybės instituto kontekste, vertinant civilinės teisės normų taikymą, kartu atsižvelgiant į asmens duomenų apsaugos reglamentavimą ir dirbtinio intelekto technologijų ypatumus. Tyrime asmens tapatybės elementai – veidas, balsas ir judesiai – analizuojami per konkrečių asmens neturtinių teisių, tokių kaip teisė į atvaizdą, privataus gyvenimo neliečiamumą ir garbės bei orumo apsauga, pažeidimo prizmę. Darbe integruojama nacionalinė ir užsienio teismų praktika, leidžianti nuosekliai įvertinti civilinės atsakomybės taikymo prielaidas asmens neturtinių teisių pažeidimų atvejais, kai jie padaromi pasitelkiant dirbtinio intelekto technologijas.

Tyrimo panaudotų šaltinių ir literatūros apžvalga. Tyrimas grindžiamas tikslingai atrinkta šaltinių baze, apimančia teisės aktus, teismų praktiką ir mokslinę literatūrą, leidžiančią nuosekliai atskleisti nagrinėjamos problemos teisinį reguliavimą ir jo taikymą praktikoje. Analizės pagrindą sudaro Lietuvos Respublikos civilinis kodeksas, ypatingą dėmesį skiriant CK 2.22–2.24 str., taip pat Bendrojo duomenų apsaugos reglamento nuostatos dėl biometrinių duomenų tvarkymo ir Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos 8 str. Ši norminė pagrindą papildė aktualūs Europos Sąjungos teisėkūros dokumentai, susiję su dirbtinio intelekto ir sintetinio turinio reguliavimu. Teismų praktikos analizė apima nacionalinių ir tarptautinių lygmenis, įskaitant Lietuvos Aukščiausiojo Teismo, Europos Žmogaus Teisių Teismo ir Jungtinių Amerikos Valstijų teismų jurisprudenciją asmens tapatybės ir biometrinių duomenų apsaugos srityje. Mokslinė literatūra, apimanti Lietuvos ir užsienio autorių darbus, sudaro teorinį ir praktinį pagrindą nagrinėjamai temai.

Asmens tapatybės samprata ir „deepfake“ technologijos teisiniai aspektai

Šiame skyriuje nagrinėjami asmens tapatybės ir „deepfake“ technologijų teisiniai aspektai, reikšmingi tolesnei civilinės atsakomybės analizei. Pirmiausia aptariama asmens tapatybės samprata ir biometrinių duomenų reguliavimas, toliau pristatoma

„deepfake“ technologijų samprata, jų veikimo kategorijos ir teisinė reikšmė, galiausiai apžvelgiamas asmens neturtinių teisių apsaugos institutas Lietuvos civilinėje ir Europos Sąjungos (toliau – ES) teisėje.

Asmens tapatybės sąvoka in genere ir ją identifikuojantys elementai

Tapatumas yra siejamas su asmens gebėjimu suvokti save, o lietuviškas terminas „tapatumas“ atitinka tarptautinį terminą „identitetas“, kilusį iš lotyniško idem, reiškiančio vienodumą ir tęstinumą.^{3, 4} Asmens tapatybė apima identifikavimo požymių visumą, kurios turinys kinta priklausomai nuo erdvės: fizinėje aplinkoje vyrauja dokumentiniai identifikatoriai, o skaitmeninėje – loginiai ir biometriniai požymiai.⁵

Atsižvelgiant į tai, kad tapatybę sudaro įvairūs duomenys ir požymiai, leidžiantys vienareikšmiškai identifikuoti asmenį tiek fizinėje, tiek elektroninėje erdvėje, Lietuvos civilinė teisė asmens tapatybės elementus įvardija kaip specifines fizinių asmenų teises ir suteikia joms teisinę apsaugą. Civilinio kodekso (toliau – CK) reguliavimas parodo, kad teisiškai reikšmingais tapatybės komponentais laikomi tie identifikavimo požymiai, kurie leidžia atpažinti konkretų asmenį ir kurių panaudojimas be sutikimo gali sukelti jo teisių pažeidimą. Šiuo požiūriu civilinė teisė išskiria tris esmines tapatybės apsaugos sritis: (i) teisę į atvaizdą (CK 2.22 str.), (ii) teisę į privatų gyvenimą (CK 2.23 str.), (iii) teisę į garbę ir orumą (CK 2.24 str.).⁶

Pavyzdžiui, Lietuvos Aukščiausiasis Teismas (toliau – LAT) yra konstatavęs, kad asmens atvaizdas atskleidžia unikalius požymius ir yra sudėtinė individualumo dalis, todėl jo fiksavimas ar panaudojimas galimas tik gavus aiškų sutikimą, o vien asmens sutikimas nusifotografuoti nesuteikia teisės atvaizdą naudoti bet kokių tikslų ar forma. Šioje byloje teismas, remdamasis Europos Žmogaus Teisių Teismo (toliau – EŽTT) praktika, pabrėžė, kad atvaizdo panaudojimas be sutikimo sudaro privataus gyvenimo pažeidimą, o tai patvirtina, jog veidas kaip biometrinis požymis yra teisiškai saugomas tapatybės elementas, kurio neteisėtas atkūrimas, modifikavimas ar platinimas vertintinas kaip pagrindas civilinei atsakomybei kilti.⁷

Apibendrinami galime teigti, kad asmens tapatybę sudaro įvairių duomenų ir požymių visuma, kurių sąrašas nėra baigtinis, ir kurie, veikdami kartu, leidžia pagrįstai identifikuoti konkretų asmenį tiek fizinėje, tiek elektroninėje erdvėje. Tarp

³ ANTINIENĖ, Dalia (2002). *Asmens tautinio tapatumo tapsmas. Sociopsichologinės šio proceso interpretacijos*. Sociologija. Mintis ir veiksmas, 10, p. 100–102.

⁴ ANTINIENĖ, Dalia (2002). *Asmens tautinio tapatumo tapsmas. Sociopsichologinės šio proceso interpretacijos*. Sociologija. Mintis ir veiksmas, 10, p. 102–107.

⁵ ŠTITILIS, Darius ir LAURINAITIS, Marius (2009). *Tapatybės vagystė elektroninėje erdvėje*. Information & Media, 50, p. 240–247.

⁶ Lietuvos Respublikos civilinis kodeksas. 2000 m. liepos 18 d. VIII-1864. *Valstybės žinios*, 2000, 74–2262.

⁷ Lietuvos Aukščiausiojo Teismo 2012 m. vasario 13 d. nutartis civilinėje byloje Nr. 3K-3-22/2012.

šių tapatybę identifikuojančių elementų ypatingą vietą užima biometriniai požymiai, kurie leidžia nustatyti asmens tapatybę remiantis jo fizinėmis ar elgsenos savybėmis.

Biometrinių duomenų samprata ir jų rūšys

Biometrinių duomenų sampratą galime išvėlgti Valstybinės duomenų apsaugos inspekcijos rekomendacijoje, kuri grindžiama tarptautiniu ISO/IEC 2382:2015 (tarptautinis informacinių technologijų terminų žodynas) standartu⁸. Joje nurodoma, kad biometriniai duomenys yra konkretūs asmens požymiai, leidžiantys identifiukuoti unikalias žmogaus savybes, tokias kaip piršto atspaudas, akies rainelė ar balsas, ir yra naudojami tapatybės patvirtinimui. Šie duomenys pasižymi unikalumu ir nekintamumu, todėl laikomi vienais patikimiausių identifikavimo elementų. Biometrinius duomenis sudaro specialiais įrenginiais fiksuojami požymiai – piršto atspaudas, veido vaizdas, akies rainelė, balsas ar kiti asmens fiziniai bruožai, kurie gali būti užfiksuoti naudojant fotografavimo ar garso įrašymo įrangą.⁹

Knygoje „Introduction to Biometrics“ yra išskiriamos dvi pagrindinės kategorijos: (i) fiziologiniai požymiai, tokie kaip pirštų atspaudai, veidas, akies rainelė, tinklainės ir delno ar plaštakos geometrija, (ii) elgsenos požymiai, tarp kurių nurodomi balsas, parašo dinamika ar klaviatūros paspaudimų ritmas ar eiseną.¹⁰

Be kita ko, Europos duomenų apsaugos priežiūros pareigūno (angl. European Data Protection Supervisor) (toliau – EDPS) darbo dokumente „Biometrics in the Identity Management Context“ nurodoma, kad biometrika naudojama dviems tikslams: (i) identifikavimui, kai siekiama nustatyti, kas asmuo yra, (ii) autentifikavimui, kai patvirtinama, kad asmuo yra tas, kuo teigia esąs.

EDPS pabrėžia, jog šių duomenų tvarkymas laikomas itin jautriu ir keliančiu aukštesnę riziką nei tradicinės identifikavimo priemonės: (i) biometriniai duomenys gali būti renkami be asmens žinios, nes jie yra vieši, ypač veidas ar balsas, (ii) biometriniai duomenys yra pažeidžiami technologinių klastočių, (iii) biometriniai duomenys gali būti panaudoti ne tik toje sistemoje, kurioje jie buvo surinkti, (iv) biometrinių požymių analizė gali sudaryti prielaidas platesniam asmens profiliavimui: iš tam tikrų asmens fiziologinių požymių gali būti nustatoma kita papildoma jautri informacija.¹¹

⁸ Nors ši rekomendacija nėra norminis teisės aktas, joje vartojamos sąvokos grindžiamos tarptautiniu informacinių technologijų terminų žodynu ISO/IEC 2382:2015, kuris laikomas tarptautiniu mastu pripažintu terminų apibrėžimų standartu.

⁹ Valstybinė duomenų apsaugos inspekcija (2017). *Biometrinių duomenų tvarkymas elektroninėje erdvėje*. Rekomendacija [interaktyvus]. https://vdai.lrv.lt/uploads/vdai/documents/files/Rekomend_Biometriniai_2017.pdf.

¹⁰ JAIN, Anil K.; ROSS, Arun A. ir NANDAKUMAR, Karthik (2011). *Introduction to Biometrics*. New York: Springer, p. 1–15.

¹¹ EUROPEAN DATA PROTECTION SUPERVISOR (2012). *Opinion 3/2012 on developments in biometric technologies (WP193)* [interaktyvus]. Brussels: European Data Protection Supervisor. https://edps.europa.eu/system/files/2019-10/wp193_en.pdf.

Taigi biometriniai duomenys sudaro esminę asmens tapatybės dalį, o Bendrojo duomenų apsaugos reglamento (toliau – BDAR), ISO standartai ir mokslinė literatūra pabrėžia jų identifikacinę vertę ir padidintą tvarkymo riziką. Šios ypatybės lemia tai, jog biometriniai požymiai tampa itin pažeidžiami „deepfake“ technologijoms, kurios sintetiniu būdu atkuria realius veido ar balso bruožus ir kelia grėsmę asmens tapatybės vientisumui bei jos teisei apsaugai.

„Deepfake“ technologijos samprata, veikimo kategorijos ir teisinė reikšmė

„Deepfake“ technologijos samprata

Technologija, apibūdinama kaip išmanusis vaizdo klastojimas ar sintetinis turinys, šiame darbe vadinamas terminu „deepfake“, o šio termino sąvoka gali būti apibūdinama remiantis įvairiais tarptautiniais ir nacionaliniais šaltiniais. Nors tarptautinėje praktikoje vartojamas terminas „deepfake“, ES dirbtinio intelekto akte (toliau – DI aktas) ši technologija lietuviškai įvardijama kaip „sintetinis turinys“, kuriuo laikomas dirbtinio intelekto (toliau – DI) generuojamas arba atlikus manipuliacijas gaunamas judamo ar nejudamo vaizdo ar garso turinys, labai panašus į realius asmenis, objektus, vietas, subjektus ar įvykius ir galintis klaidinti asmenį, jog jis yra autentiškas ar tikras.¹² Oxford žodyne „deepfake“ sąvoka apibūdinama kaip bet kokio pobūdžio medija, ypač vaizdo įrašas, kuris buvo skaitmeniškai manipuluotas taip, kad vieno asmens atvaizdas būtų įtikinamai pakeistas kito asmens atvaizdu; dažnai naudojama piktavališkai siekiant parodyti asmenį darant veiksmus, kurių jis iš tikrųjų neatliko.¹³ Valstybinė lietuvių kalbos komisija pateikia lietuviškus atitikmenis: išmanusis ar sintetinis vaizdo klastojimas (veiksmas) ir vaizdo klastotė (rezultatas).¹⁴

Darytina išvada, jog nepaisant terminų įvairovės, visi apibūdinimai nusako tą patį reiškinį – medijos turinį, kuriame pakeičiami ar atkuriami realaus asmens tapatybės požymiai taip, jog jis gali būti klaidingai palaikytas tikru. Siekiant suprasti, kaip šie požymiai yra techniškai atkuriami, toliau nagrinėjamos pagrindinės „deepfake“ technologijų veikimo kategorijos.

¹² Europos Parlamento ir Tarybos 2024 m. birželio 13 d. reglamentas (ES) Nr. 2024/1689 kuriuo nustatomos suderintos dirbtinio intelekto taisyklės ir iš dalies keičiami reglamentai (EB) Nr. 300/2008, (ES) Nr. 167/2013, (ES) Nr. 168/2013, (ES) 2018/858, (ES) 2018/1139 ir (ES) 2019/2144 ir direktyvos 2014/90/ES, (ES) 2016/797 ir (ES) 2020/1828 (Dirbtinio intelekto aktas). OL L 1689 2024.7.12, p. 1–190.

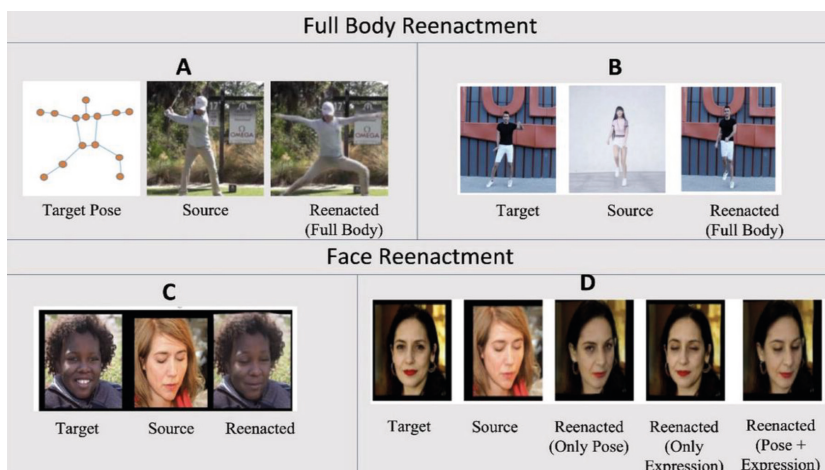
¹³ Oxford University Press. (n.d.). *Deepfake*. Iš: Oxford English Dictionary. [interaktyvus]. <https://doi.org/10.1093/OED/9547101155>.

¹⁴ Valstybinės lietuvių kalbos komisijos konsultacijų bankas. (n.d.). *Koks angl. „deepfake“ lietuviškas atitikmuo?* Iš: Valstybinė lietuvių kalbos komisija. [interaktyvus]. <https://vlkk.lt/konsultacijos/13729-2019-06-18-06-30-56>.

„Deepfake“ technologijos veikimo kategorijos

Technologijos skirstomos į keturias kategorijas: (i) perkūrimą (angl. reenactment), (ii) pakeitimą (angl. replacement), (iii) redagavimą (angl. editing) ir (iv) sintezę (angl. synthesis). Toliau šiame skyriuje: šaltinio asmuo – tas, kurio požymiai naudojami; tikslinis asmuo – tas, kurio vaizdas modifikuojamas.

(i) Perkūrimo kategorijai priskiriamos „deepfake“ technologijos apima metodus, kuriais vieno asmens veido išraiška, galvos poza bei lūpų judesiai yra valdomi kito asmens veiksmiais. Ši kategorija yra labiausiai paplitusi, nes suteikia platų lankstumo spektrą, jai taip pat priskiriami burnos judesių, žvilgsnio, galvos padėties ir kūno pozos perkūrimo metodai, kuriais šaltinio asmens judesiai perkeliama tikslinio asmens atvaizdui valdyti. Šios technologijos taikomos įvairiose srityse – nuo kino industrijos ir vaizdo žaidimų iki balso dubliavimo bei veido atpažinimo sistemų tobulinimo.



1 paveikslas. „Deepfake“ perkūrimo pavyzdžiai: (A), (B) – viso kūno perkūrimo pavyzdžiai; (C) ir (D) – veido perkūrimo pavyzdžiai; Šaltinis: Sudaryta RAMAMURTHY, Dhanyalakshmi; POPIRLAN, Claudiu-Ionuț ir HEMANTH, Duraisamy Jude (2025).

A survey on deep learning based reenactment methods for deepfake applications [interaktyvus]. <https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/ipr2.13201>.

(ii) Pakeitimo kategorijai priskiriamas „deepfake“ turinys yra tuomet, kai vieno asmens tapatybę identifikuojantys požymiai yra pakeičiami kito asmens požymiais, kartu išsaugant pastarojo tapatybę. Ši kategorija apima du metodus: (i) perkėlimą, kai esamas turinys pakeičiamas šaltinio asmens turiniu (pavyzdžiui, mados industrijoje

vizualizuojant, kaip asmuo atrodytų dėvėdamas skirtingus drabužius), ir (ii) apsikeitimą, kai kito asmens turinys integruojamas į esamą vaizdinį kontekstą. Pastarasis metodas dažniausiai taikomas veidų apsikeitimui: memų bei satyrinio turinio kūrimui arba asmens tapatybės anonimizavimui viešai skelbiamame turinyje.

(iii) Redagavimo kategorija apima atvejus, kai asmens ypatybės yra modifikuojamos: keičiant esamas, jas pašalinant ar pridėdant naujų požymių, pavyzdžiui, pakeičiant drabužius, amžių ar svorį. Nors tokios priemonės gali būti naudojamos pramogai, tas pats procesas gali būti panaudojamas kuriant melagingą tapatybę ar modifikuojant aukos atvaizdą kenksmingais tikslais.

(iv) Sintezės kategorijos „deepfake“ turinys yra sukuriamas, kai turinys generuojamas neturint realaus asmens kaip pagrindo. Vienas iš pavyzdžių – personažo generavimas filmui ar žaidimui, tačiau, taip pat, kaip ir redagavimo „deepfake“ turinio atveju, ši technologija gali būti naudojama ir melagingoms tapatybėms internete kurti.¹⁵



2 paveikslas. Redagavimo būdu sukurtas Popiežiaus Pranciškaus „deepfake“ kairėje; tikra Popiežiaus Pranciškaus nuotrauka dešinėje; Šaltinis: BENNET, Drake (2023). AI Deep Fake of the Pope's Puffy Coat Shows the Power of the Human Mind [interaktyvus]. <https://www.bloomberg.com/news/newsletters/2023-04-06/pope-francis-white-puffer-coat-ai-image-sparks-deep-fake-concerns>.

¹⁵ MIRSKY, Yisroel ir LEE, Wenke (2020). *The creation and detection of deepfakes: A survey*. arXiv, p. 3–4 [interaktyvus]. <https://arxiv.org/abs/2004.11138>.

Atsižvelgiant į tai, perkūrimo ir pakeitimo kategorijos yra tiesiogiai susijusios su realių asmens biometrinių požymių atkūrimu ar pakeitimu, todėl sudaro didžiausią riziką asmens tapatybei, o šis skirtumas turi ir teisinę reikšmę, nes nuo jo priklauso, ar „deepfake“ turinio kūrimas patenka į asmens duomenų ir tapatybės elementų apsaugos reguliavimo sritį.

„Deepfake“ technologijos teisinė reikšmė

„Deepfake“ technologijoje naudojami asmens veido, balso ir judesių požymiai priskiriami biometriniais duomenimis pagal BDAR 4 str. 14 p., todėl jų tvarkymui taikomi BDAR reikalavimai.

Pagal BDAR 6 str. 1 d., asmens duomenų tvarkymas laikomas teisėtu tik tenkinus bent vieną iš straipsnyje nustatytų sąlygų: (i) kai duomenų subjektas yra davęs sutikimą, (ii) kai tvarkymas būtinas sutarties vykdymui, (iii) teisinės prievolės vykdymui, (iv) gyvybiškai svarbiems interesams apsaugoti, (v) viešojo intereso tikslams ar (vi) duomenų valdytojo teisėtiems interesams, jei duomenų subjekto teisės nėra viršesnės. Kadangi biometriniai duomenys, tvarkomi identifikavimo tikslais, priskiriami specialių kategorijų duomenimis, jiems papildomai taikomos ir BDAR 9 str. nustatytos tvarkymo sąlygos.

Pagal BDAR 9 str. 2 d., specialių kategorijų duomenų tvarkymas leidžiamas, jei yra taikoma bent viena straipsnyje numatyta sąlyga: (i) kai duomenų subjektas aiškiai sutiko, kad tokie asmens duomenys būtų tvarkomi vienu ar keliais nurodytais tikslais, taip pat, jei (ii) yra tvarkomi akivaizdžiai viešai duomenų subjekto paskelbti duomenys arba, jei (iii) tai būtina siekiant pareikšti, vykdyti arba apginti teisinius reikalavimus, arba (iv) dėl svarbaus viešojo intereso priežasčių, nustatytų ES ar valstybės narės teisėje ir užtikrinant tinkamas ir konkrečias duomenų subjekto pagrindinių teisių ir interesų apsaugos priemones.¹⁶

Atsižvelgiant į tai, darytina išvada, kad veido, balso ar judesių požymiai gali būti naudojami „deepfake“ turinio generavimui tik tada, kai egzistuoja BDAR 6 str. numatytas teisėtas tvarkymo pagrindas, o identifikavimo tikslais tvarkomiems biometriniais duomenimis – dar bent viena BDAR 9 str. 2 d. numatyta specialių kategorijų duomenų tvarkymo išimtis. Kartu pažymėtina, kad „deepfake“ technologijų vaizdo ir garso turinio naudojimo vertinimas neapsiriboja asmens duomenų apsaugos reikalavimais ir yra reikšmingas civilinės teisės normų požiūriu.

¹⁶ Europos Parlamento ir Tarybos 2016 m. balandžio 27 d. reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas). OL L 119, 2016, p. 1–116.

Asmens teisės į atvaizdą, teisės į privatų gyvenimą ir teisės į garbę ir orumą apsaugos institutas Lietuvos civilinėje ir Europos Sąjungos teisėje

Asmens tapatybės elementai yra saugomi plačiau nei vien tik per atvaizdo ar privataus gyvenimo apsaugos prizmę – Lietuvos CK įtvirtina visą asmens neturtinių teisių sistemą, apimančią teisę į vardą (2.20, 2.21 str.), atvaizdą (2.22 str.), privatų gyvenimą (2.23 str.), garbės ir orumo gynimą (2.24 str.) ir kitas neturtines teises (2.25–2.27 str.).¹⁷

Teisė į atvaizdą saugo asmens identifikuojamą vizualinį pavidalą ir jo kontrolę. CK komentare (toliau – Komentaras) atvaizdas apibrėžiamas kaip bet koks užfiksuotas žmogaus pavidalas, leidžiantis jį atpažinti, o pagrindinė taisyklė yra sutikimo reikalavimas: bet koks atvaizdo fiksavimas ar panaudojimas galimas tik gavus aiškų asmens sutikimą, susietą su konkrečiu naudojimo tikslu, ir pažeidimu laikomas bet koks panaudojimas be sutikimo, jeigu asmuo išlieka atpažįstamas.¹⁸

CK 2.23 str. įtvirtina privataus gyvenimo neliečiamumą – informacija apie asmens privatų gyvenimą gali būti skelbiama tik turint jo sutikimą, o apsauga taikoma tiek pačiam turiniui, tiek ir jo rinkimo, perdavimo ar skleidimo faktui.

Pažeidimas egzistuoja net tada, kai asmuo nėra tiesiogiai identifikuotas, bet duomenų visuma leidžia jį nustatyti, tačiau privatumo teisė nėra absoliuti: remiantis Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos (toliau – EŽTK) 8 str., jos ribojimas galimas tik įstatyme numatytais atvejais, kai tai būtina demokratinėje visuomenėje ir proporcinga teisėtiems tikslams.¹⁹ Publikacijos be sutikimo gali pažeisti tiek teisę į privatų gyvenimą, tiek ir teisę į atvaizdą, o neteisėtas informacijos rinkimas yra savarankiškas pažeidimas net tada, kai informacija vėliau nėra skelbiama. Už privatumo pažeidimą galima reikšti reikalavimus pagal CK 6.250 str. (neturtinė žala), o esminė šios teisės paskirtis – suteikti asmeniui kontrolę nuspręsti, kokia informacija apie jį gali tapti vieša.²⁰

CK 2.24 str. gina asmens garbę, orumą ir reputaciją tais atvejais, kai paskleidžiami tikrovės neatitinkantys ir žeminantys duomenys. Komentare pabrėžiama, kad duomenų neatitiktis tikrovei preziumuojama tol, kol ją paneigia pats skleidėjas, o paskleidimu laikomas perdavimas bent vienam trečiajam asmeniui bet kokia forma,

¹⁷ Lietuvos Respublikos civilinis kodeksas. 2000 m. liepos 18 d. VIII-1864. *Valstybės žinios*, 2000, 74–2262.

¹⁸ BAKANSKAS, Algimantas; BARTKUS, Gintautas; DOMINAS, Giedrius ir kt. (2002). *Civilinio kodekso komentaras. Antroji knyga: Asmenys*. Vilnius: Justitia, p. 53–56.

¹⁹ Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija (1950). *Valstybės žinios*, 1995, 40–987.

²⁰ BAKANSKAS, Algimantas; BARTKUS, Gintautas; DOMINAS, Giedrius ir kt. (2002). *Civilinio kodekso komentaras. Antroji knyga: Asmenys*. Vilnius: Justitia, p. 56–59.

įskaitant ir sklaidą internete. Civilinė atsakomybė kyla tiek už neteisingos informacijos paskleidimą, tiek už atsisakymą ją paneigti, o CK 2.24 str. aiškinimas derinamas su Lietuvos Respublikos Konstitucijos 25 str.²¹ ir EŽTT praktika, kuri reikalauja tarpusavio sąveikos tarp reputacijos apsaugos ir saviraiškos laisvės.²²

LAT 2024 m. gegužės 16 d. nutartis civilinėje byloje Nr. e3K-3-73-421/2024 patvirtina pagrindinius CK 2.22–2.24 str. taikymo principus. Teismas pažymi, kad teisė į atvaizdą yra teisės į privatų gyvenimą dalis, o CK 2.22 str. įtvirtina aiškią taisyklę: asmens atvaizdas gali būti fiksuojamas ir naudojamas tik su jo sutikimu, išskyrus įstatyme nurodytas išimtis, tačiau net ir tais atvejais atvaizdas negali būti naudojamas taip, kad žemintų asmens garbę ar reputaciją.

Dėl CK 2.23 str. teismas pabrėžia, kad asmuo pats sprendžia, kokią informaciją apie savo privatų gyvenimą atskleisti, o bet koks jos rinkimas ar skleidimas be sutikimo gali būti neteisėtas, nes net tikrovę atitinkanti informacija, paskelbta pažeidžiant įstatymo nustatytą tvarką, gali būti pagrindas reikalauti žalos atlyginimo.

Aiškindamas CK 2.24 str., teismas primena, kad garbė ir orumas ginami nustačius keturis faktus: (i) žinių paskleidimą, (ii) jų susiejimą su ieškovu, (iii) neatitiktį tikrovei ir (iv) žeminantį pobūdį.²³

F. Romero Moreno pažymi, kad „deepfake“ technologijos tiesiogiai kelia grėsmę neturtinėms asmens teisėms, nes jų veikimas grindžiamas biometrinį požymių – veido ir balso – apdorojimu, leidžiančiu manipuluoti žmogaus tapatybės elementais taip, kad netikras turinys turėtų realių pasekmių jo socialiniam vertinimui ir privatumui. Autorius taip pat atskleidžia, kad „deepfake“ kelia pavojų informacijos vienišumui ir viešojo diskurso patikimumui, todėl būtina taikyti skaidrumo priemonės, tokias kaip dirbtinio turinio žymėjimas, kurios vėliau buvo įtvirtintos ir ES teisėkūroje.²⁴

Vienas reikšmingiausių EŽTT sprendimų dėl teisės į privatų gyvenimą ir atvaizdo apsaugą yra Von Hannover prieš Vokietiją, kuriame teismas konstatavo, kad asmens kasdienio gyvenimo nuotraukos, publikuojamos be jo sutikimo, patenka į EŽTK 8 str. taikymo sritį, o jų viešinimas gali būti pateisinamas tik tada, kai publikacija prisideda prie visuomenei reikšmingos diskusijos. Teismas pripažino, kad visuomenė neturi teisėto intereso į viešųjų funkcijų neatliekančio asmens asmeninę kasdienybę,

²¹ Lietuvos Respublikos Konstitucija. Lietuvos Respublikos piliečių priimta 1992 m. spalio 25 d. referendumu. *Valstybės žinios*, 1992, 33–1014.

²² BAKANSKAS, Algimantas; BARTKUS, Gintautas; DOMINAS, Giedrius ir kt. (2002). *Civilinio kodekso komentaras. Antroji knyga: Asmenys*. Vilnius: Justitia, p. 59–65.

²³ Lietuvos Aukščiausiojo Teismo Civilinių bylų skyriaus 2024 m. gegužės 16 d. nutartis civilinėje byloje Nr. e3K-3-73-421/2024.

²⁴ ROMERO MORENO, F. (2024). *Generative AI and deepfakes: a human rights approach to tackling harmful content*. *International Review of Law, Computers & Technology*, 38(3), p. 297–326. <https://doi.org/10.1080/13600869.2024.2324540>.

ir konstatavo, jog Vokietijos teismai neužtikrino pakankamos pareiškėjos privataus gyvenimo apsaugos.²⁵

Darytina išvada, jog nacionalinė teisė ir EŽTT praktika asmens tapatybės apsaugą grindžia neturtinių teisių sistema, kuri faktiškai persidengia su BDAR reglamentuojama duomenų apsauga, kai tvarkomi asmens tapatybę identifikuojantys duomenys. Atsižvelgiant į tai, toliau nagrinėjamos civilinės atsakomybės taikymo sąlygos neteisėto asmens tapatybės elementų panaudojimo atvejais.

Civilinės atsakomybės taikymas neteisėtai sukūrus ir išplatinus „deepfake“ turinį

Šiame skyriuje analizuojamas civilinės atsakomybės taikymas, kai be asmens sutikimo sukuriamas ir (ar) išplatinamas „deepfake“ turinys. Pirmiausia aptariamos neteisėto panaudojimo formos ir teismų praktikos pavyzdžiai, toliau nagrinėjama neturtinė ir turtinė žala, priežastinis ryšys bei kaltė ir atsakingi subjektai, galiausiai apibrėžiama riba tarp teisėto ir neteisėto „deepfake“ turinio panaudojimo.

Neteisėtas asmens tapatybės elementų panaudojimas

Sparčiai tobulėjanti „deepfake“ technologija iš esmės pakeitė dezinformacijos pobūdį, nes generatyvinis DI leidžia kurti itin tikrovišką sintetinį turinį. Nors biometrinė autentifikacija plačiai naudojama tapatybei patvirtinti, „deepfake“ technologijos paverčia ją vienu pagrindinių taikinių, sukurdamos riziką asmens privatumui.²⁶ Atsižvelgiant į šių technologijų keliamas rizikas, teismų praktikoje vis dažniau kyla ginčų dėl neteisėto asmens tapatybės elementų – veido, balso ar judesių – panaudojimo.

Lietuvos ir ES teismų praktika šioje srityje dar tik formuojasi, todėl šiame darbe analizei pasitelkiami Jungtinių Amerikos Valstijų (toliau – JAV) teismų procesai ir sprendimai, kurie jau apima konkrečius DI ir „deepfake“ panaudojimo atvejus. Byloje *In re Clearview AI, Inc.* (toliau – Bendrovė) prieš *Consumer Privacy Litigation* nustatyta, kad bendrovė sistemingai rinko (angl. *scraping*) asmenų nuotraukas iš viešai prieinamų interneto svetainių ir, išgaudama veido geometrijos duomenis, sudarė didelio masto biometrinę duomenų bazę, pasiekusią apytiksliai dešimt milijardų atvaizdų. Šia baze naudojosi teisėsaugos institucijos ir privatūs subjektai asmens tapatybei nustatyti. 2025 m. teismas patvirtino taikos sutartį, kuria bendrovė įsipareigojo nutraukti biometrinį identifikatorių atskleidimą trečiosioms šalims. Teismas pažy-

²⁵ *Von Hannover prieš Vokietiją* [EŽTT], Nr. 59320/00, [2004-06-24]. ECLI:CE:ECHR:2004-0624JUD005932000.

²⁶ HE, Shijing; LEI, Yaxiong; ZHANG, Zihan ir kt. (2025). *Identity Deepfake Threats to Biometric Authentication Systems: Public and Expert Perspectives*. arXiv [interaktyvus]. <https://arxiv.org/abs/2506.06825>.

mėjo, kad veido geometrijos duomenys yra itin galinga ir kartu ypač pažeidžiama netinkamam panaudojimui identifikavimo priemonė.²⁷

Analogiška problema kyla balso atkartojimo srityje. Byloje Lehrman et al. (toliau – Ieškovai) prieš Lovo, Inc. (toliau – Atsakovė) Ieškovai, būdami profesionalūs įgarsintojai, pateikė balso įrašus Atsakovei, kuri patikino, jog jie bus naudojami tik vidiniams tyrimų ir akademiniams tikslams. Tačiau Atsakovė, teikianti DI pagrįstą teksto į kalbą konvertavimo (angl. text-to-speech) paslaugą, panaudojo šiuos įrašus DI balso klonams kurti, o Ieškovai atpažino sukurtus balsus kaip praktiškai identiškus Ieškovams. Teismas nustatė, kad Ieškovai pagrįstai pareiškė reikalavimus dėl balso pasisavinimo pagal Niujorko Civilinių teisių įstatymą, draudžiantį naudoti asmens balsą komerciniais tikslais be rašytinio sutikimo. Ši byla šiuo metu dar nėra išnagrinėta iš esmės – teismas 2025 m. liepos 10 d. pateikė tik sprendimą dėl Atsakovės prašymo atmesti ieškinį, todėl bylos nagrinėjimas tęsiasi toliau.²⁸

Taip pat verta pažymėti, jog „deepfake“ technologijų keliamos rizikos gali pasireikšti ir teismo procese, pateikiant vaizdo ar garso įrašus kaip įrodymus. Byloje Ariel Mendones et al. (toliau – Ieškovai) prieš Cushman & Wakefield, Inc. (toliau – Atsakovai) teismui kilo įtarimų, kad dalis Ieškovų pateiktų vaizdo įrašų gali būti sukurti naudojant generatyvinę DI, nes jie pasižymėjo DI būdingais požymiais, tokiais kaip veido išraiškų stoka, neįprasti žodžių junginiai ir su tariamais žodžiais nesuderinti lūpų judesiai. Įvertinęs pateiktus duomenis, teismas nustatė, kad bent du įrašai iš tiesų yra generatyvinio DI sukurti „deepfake“, ir taikė griežčiausią procesinę sankciją – bylos nutraukimą, pažymėdamas, kad ši sankcija siunčia aiškų perspėjimą visiems proceso dalyviams, jog teismas netoleruoja bandymų pateikti DI sukurtus vaizdo įrašus kaip tikrus įrodymus.²⁹

Atsižvelgiant į šiuos teismų praktikoje nagrinėtus pavyzdžius, galime teigti, kad neteisėtas asmens tapatybės elementų panaudojimas DI priemonėmis gali pasireikšti įvairiomis formomis: nuo masinio biometrinių duomenų rinkimo iki balso klonavimo ir dirbtinai sugeneruotų įrašų pateikimo kaip tikrų įrodymų teismo procese. Šių iššūkių kontekste toliau nagrinėjama „deepfake“ technologijų sukeliamą neturtinę ir turtinę žalą.

Neturtinė ir turtinė žala

Mokslinėje literatūroje „deepfake“ keliami žala apibrėžiama kaip daugiasluoksnė, apimanti tiek individualius, tiek sisteminius padarinius. B. Chesney ir D. Citron nurodo, kad „deepfake“ technologijos sukuria daugiasluoksnią žalą, darančią poveikį

²⁷ Ilinojaus šiaurinės apygardos teismo 2025 m. kovo 20 d. nutartis byloje Nr. 21-cv-00135.

²⁸ Pietų Niujorko apygardos teismo 2025 m. liepos 10 d. nutartis byloje Nr. 1:24-cv-03770.

²⁹ Kalifornijos valstijos Aukštesniojo teismo 2025 m. liepos 11 d. nutartis byloje Nr. 23CV028772.

privatumui, reputacijai, psichologinei gerovei ir viešosios informacijos patikimumui. Autoriai taip pat pabrėžia vadinamąjį „melagio dividendą“ (angl. liar's dividend), kai net tikri įrašai gali būti neigiami vien dėl to, kad egzistuoja technologinė galimybė juos suklastoti.³⁰ „Data & Society“ tyrimas papildo šią išvalgą, pažymėdamas, kad žalos mastą lemia ne klastotės sudėtingumas, bet apgaulingas kontekstas, kuriame turinys pateikiamas.³¹ Literatūroje taip pat išskiriama, kad žala gali būti tiek individuali (emocinis stresas, tapatybės destabilizavimas, socialinė stigmatizacija), tiek kolektyvinė, nes sintetiniai vaizdai silpnina informacinės erdvės patikimumą ir kelia grėsmę demokratijai.³²

Moksliniai tyrimai rodo, kad „deepfake“ technologijos daro itin plataus masto neturtinę žalą. Europos Parlamento tyrime pabrėžiama, kad seksualinio pobūdžio „deepfake“ įrašai sukelia ilgalaikius psichologinius padarinius, įskaitant nerimą, socialinę izoliaciją ir tarpusavio santykių praradimą, o toks turinys sukelia pasikartojančią žalą, nes kiekvienas klastotės perdavimas naujai auditorijai vėl sukelia emocinę įtampą nukentėjusiajam. Vaikų ir paauglių atžvilgiu ši neturtinė žala yra dar ryškesnė, nes „deepfake“ naudojimas patyčių kontekste siejamas su savivertės praradimu ir padidėjusiu nerimu.³³ Galiausiai, C. Vaccari ir A. Chadwick tyrimas taip pat parodė, kad nukentėjusieji gali patirti vadinamąją „paneigimo našta“ (angl. denial burden) – nuolatinę pareigą įrodinėti, jog klastotėje vaizduojamas asmuo nėra iš tikrųjų jįs.³⁴

Be reputacinių ir psichologinių pasekmių, moksliniai tyrimai identifikuoja ir turtinę žalą. M. Westerlund pažymi, kad „deepfake“ yra viena sparčiausiai plintančių kibernetinių grėsmių formų, galinčių būti panaudotų finansinėms apgaulėms, impersonacijai ir verslo procesų sutrikdymui, nes ši technologija leidžia sukurti autentiškai skambančius įrašus, kuriais apsimetama vadovais ar įmonių atstovais.³⁵ B. Chesney ir D. Citron pabrėžia, kad ekonominiai padariniai gali būti tiek tiesioginiai (finansiniai nuostoliai, pajamų ar profesinės karjeros galimybių praradimas), tiek netiesioginiai

³⁰ CHESNEY, Bobby ir CITRON, Danielle. *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*. California Law Review, 2019, p. 1754–1760.

³¹ PARIS, Britt ir DONOVAN, Joan (2019). *Deepfakes and Cheap Fakes*. Data & Society Research Institute, p. 3.

³² VACCARI, Cristian ir CHADWICK, Andrew (2020). *Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News*. Social Media + Society, p. 2–4.

³³ NEGREIRO, Mar (2025). *Children and Deepfakes*. European Parliamentary Research Service, PE 775.855, 1–8 [interaktyvus]. [https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/775855/EPRS_BRI\(2025\)775855_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/775855/EPRS_BRI(2025)775855_EN.pdf).

³⁴ VACCARI, Cristian ir CHADWICK, Andrew (2020). *Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News*. Social Media + Society, p. 3–4.

³⁵ WESTERLUND, Mika (2019). *The Emergence of Deepfake Technology: A Review*. TIM Review, p. 40–42.

(išlaidos sugadintos reputacijos atkūrimui ir informacijos tikrinimo procedūroms), o dėl „melagio dividendo“ įmonės ir institucijos nebegali pasitikėti viešu vaizdo ar garso turiniu.^{36, 37} „Data & Society“ tyrimo autoriai taip pat pastebi, kad net paprasčia manipuluota vaizdinė medžiaga gali lemti neigiamas rinkos reakcijas ir prekinio ženklo nuvertėjimą.³⁸

Taigi „deepfake“ technologijos sukuria žalą, kuri vienu metu pažeidžia kelis asmens teisinius gėrius: reputacinę, psichologinę ir socialinę žalą atsiranda dėl sintetinės medžiagos gebėjimo paveikti asmens tapatybę ir socialinį statusą, o ekonominė žala apima finansinius nuostolius ir verslo patikimumo sumažėjimą. Nustačius šios žalos pobūdį, tolesnė analizė orientuojama į priežastinio ryšio tarp žalos ir ją lėmusių veiksmų nustatymą.

Priežastinis ryšys

Nors „deepfake“ technologija yra nauja, tačiau kenksminga veikla, kuriai tokia technologija yra naudojama, teisiniu požiūriu nėra nauja – pasikeitė tik veikimo dinamika ir operacijų mastas, o žalingo elgesio esmė nuo Romos teisės laikų nėra pasikeitusi.³⁹ Lietuvos civilinėje teisėje priežastinis ryšys suprantamas kaip būtina civilinės atsakomybės sąlyga, o jo turinį apibrėžia CK 6.247 str. LAT ne kartą yra pažymėjęs, jog atlyginami yra tik tie nuostoliai, kurie pagal jų ir civilinės atsakomybės prigimtį gali būti laikomi skolininko veiksmų (veikimo, neveikimo) rezultatu.

Kasacinis teismas yra išaiškinęs, kad priežastinio ryšio nustatymas vyksta dviem etapais: pirmiausia *conditio sine qua non* testu nustatomas faktinis priežastinis ryšys, t. y. ar žalingi padariniai būtų atsiradę be neteisėto veiksmo, o antrame etape vertinama, ar padariniai teisine prasme nėra pernelyg nutolę nuo neteisėto veiksmo, atsižvelgiant į protingo asmens galimybę numatyti žalos atsiradimą ir pažeisto intereso prigimtį.⁴⁰

Kabėdami apie sintetinę mediją, priežastinio ryšio nustatymas tampa sudėtingesnis, nes pati technologija apima skirtingus asmenis, nevienodai prisidedančius prie rezultato: DI sistemos kūrėją, programinės įrangos diegėją, naudotoją ir platformas, kuriose žalingas turinys platinamas. Esant daugeliui subjektų, teisei sistemai sudė-

³⁶ CHESNEY, Bobby ir CITRON, Danielle (2019). *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, p. 1750–1753.

³⁷ CHESNEY, Bobby ir CITRON, Danielle (2019). *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, p. 1754–1755.

³⁸ PARIS, Britt ir DONOVAN, Joan (2019). *Deepfakes and Cheap Fakes*. Data & Society Research Institute, p. 3–5.

³⁹ HRISTOV, Georgi (2025). *Genuine harms behind artificial content: How EU regulation can combat malicious use of deep fake technology*. Social Science Research Network, p. 15–16 [interaktyvus]. <https://ssrn.com/abstract=5634715>.

⁴⁰ Lietuvos Aukščiausiojo Teismo 2024 m. spalio 8 d. nutartis civilinėje byloje Nr. e3K-3-173-378/2024.

tinga tinkamai paskirstyti atsakomybę, be to, „deepfake“ turinį galima modifikuoti turint bent minimalias technines žinias ir lengvai pašalinti metaduomenis, todėl nukentėję asmenys dažnai negali susieti žalingo turinio su jo tikruoju kūrėju. DI sugeneruoto turinio aukoms bus sunku įrodyti kiekvieną atsakomybės elementą: (i) kaltininką, (ii) neteisėtą veikimą ar neveikimą, (iii) tyčią, kuri (iv) sukelia (v) žalingą rezultatą.

Europos Komisija (toliau – EK) 2022 m. pateikė atsakomybės už DI direktyvos pasiūlymą (toliau – Direktyva), kuriuo siekta sukurti reguliavimo pagrindą deliktinei atsakomybei už DI sukeltą žalą. Vienas esminių pasiūlytų elementų – įrodinėjimo pareigos supaprastinimas: jei DI sistemos kūrėjas atsisakytų pateikti ieškovui informaciją, būtų taikoma nugrinčijama prezumpcija, kad egzistuoja priežastinis ryšys tarp jo kaltės ir DI sistemos išvesties. Tokiu atveju ieškovui pakaktų pagrįsti kaltę, tikėtiną jos poveikį DI veikimui ir faktinės žalos atsiradimą.

Nors Direktyvos pasiūlymas buvo išbrauktas iš 2025 m. EK darbo programos, jame suformuluotos taisyklės vis dar gali būti reikšmingos vertinant „deepfake“ žalos atlyginimą. Verta pabrėžti, jog pasiūlyme buvo ypač kritikuojama konstatuojamoji dalis Nr. 15, eliminuojanti iš Direktyvos taikymo srities sistemas, kuriose sprendimų grandinėje dalyvauja žmogus, nes praktikoje „deepfake“ kūrimas ir platinimas beveik visada apima žmogaus įsikišimą, todėl tokia išimtis sudarytų sąlygas išvengti atsakomybės. Nepaisant to, tokio pobūdžio taisyklės leistų suformuoti nuoseklią atsakomybės sistemą, tačiau ar šios nuostatos ateityje bus įtrauktos į ES teisės aktus, lieka neaišku.⁴¹

Galima daryti išvadą, jog „deepfake“ technologijų kontekste priežastinio ryšio nustatymas tampa sudėtingesnis dėl kelių subjektų dalyvavimo ir objektyvių įrodinėjimo sunkumų, ypač kai žalingi padariniai kyla ne dėl vieno veiksmo, o dėl visos veiksmų sekos, apimančios technologijos kūrimą, naudojimą ir turinio platinimą. Todėl toliau tikslinga analizuoti kaltę ir atsakingus subjektus.

Kaltė ir atsakingi subjektai

Kaltė civilinėje teisėje siejama su asmens nesąžiningumu, kuris pasireiškia tuo, kad jis nebuvo tiek rūpestingas ir apdairus, kiek konkrečiomis sąlygomis buvo būtina. Laikoma, kad kaltė traktuojama kaip subjektyvusis nesąžiningumas, o neteisėti veiksmai – kaip objektyvusis nesąžiningumas, todėl šios dvi kategorijos sudaro du asmens elgesio vertinimo aspektus. Neteisėti veiksmai reiškia teisinės pareigos nevykdymą, o kaltė parodo, kad asmuo nepadarė visko, ką konkrečioje situacijoje ga-

⁴¹ HRISTOV, Georgi (2025). *Genuine harms behind artificial content: How EU regulation can combat malicious use of deep fake technology*. Social Science Research Network, p. 37–39 [interaktyvus]. <https://ssrn.com/abstract=5634715>.

lėjo padaryti, siekdamas išvengti žalos. Civilinėje teisėje galioja sąžiningumo, kitaip tariant, nekaltumo prezumpcija, tačiau įrodžius neteisėtus veiksmus preziumuojama ir kaltė, kol asmuo nepaneigia, jog jo elgesys buvo pakankamai rūpestingas ir atidus.⁴²

Taigi šie kriterijai yra itin aktualūs vertinant asmens ir skaitmeninių platformų atsakomybę dėl tapatybės elementų panaudojimo „deepfake“ turinyje, nes svarbu suprasti, ar subjektai ėmėsi visų protingų priemonių išvengti žalos atsiradimui. Atsižvelgiant į tai, pirmiausia tikslinga analizuoti individualaus asmens veiksmus ir jų teisinį vertinimą, nustatant, kada tapatybės elementų panaudojimas sudaro pagrindą deliktinei asmens atsakomybei.

Deliktinė asmens atsakomybė

Asmens civilinė atsakomybė už tapatybės elementų panaudojimą „deepfake“ turinyje kyla dėl to, kad pažeidžiama asmens teisė kontroliuoti savo atvaizdą, balsą ar judesius. H. Peng ir P. W. Lee pažymi, kad „deepfake“ sukeliama žala dažniausiai yra reputacinė, emocinė arba profesinė, o autoriaus veikla dažnai pasižymi tyčiniu manipuliavimu asmens įvaizdžiu, kas leidžia ją kvalifikuoti kaip deliktą (angl. tort). Nors tradiciniai deliktai ne visada tinkamai aprėpia šios technologijos sukeltus padarinius, pati žala patenka į deliktinės atsakomybės sritį.⁴³

M. D. Murray analizė papildomai pagrindžia, kad neteisėtas asmens identiteto – veido, balso ar judesių – panaudojimas yra suprantamas kaip civilinis pažeidimas, sukuriantis deliktinę atsakomybę net ir tais atvejais, kai turinys nėra komercinis. „Teisė į viešumą“ (angl. right of publicity) šaltinyje aiškinama kaip asmens galimybė kontroliuoti savo tapatybės panaudojimą, todėl „deepfake“ kūrėjui gali kilti pareiga atlyginti tiek neturtinę, tiek turtinę žalą, o tyčinis asmens identiteto iškraipymas gali lemti dar didesnę atsakomybės dydį.⁴⁴

Praktinis šių principų taikymo pavyzdys pateiktas byloje Midler prieš Ford Motor Co. JAV Apeliacinis teismas pripažino, kad net ir netiesioginė asmens tapatybės imitacija – garsios dainininkės Bette Midler balso stilistinė imitacija reklamoje – gali sudaryti civilinį pažeidimą pagal teisės į viešumą principus, o balso imitacija laikytina neteisėtu tapatybės pasisavinimu. Grąžinus bylą nagrinėti iš naujo, prisiekusieji (angl. jury) B. Midler priteisė 400 000 JAV dolerių žalos atlyginimą.⁴⁵ Šis precedentas yra

⁴² NORKŪNAS, Algis (2002). *Kaltė kaip civilinės atsakomybės pagrindas*. Jurisprudencija, 28(20), p. 112–118.

⁴³ PENG, Huijuan ir LEE, Pey W. (2025). *Reimagining U.S. tort law for deepfake harms: Comparative insights from China and Singapore*. Singapore Management University, p. 3.

⁴⁴ MURRAY, Michael D. (2024). *Deceptive exploitation: Deepfakes, the rights of publicity and privacy, and trademark law* (SSRN Working Paper No. 4981531). SSRN. <https://doi.org/10.2139/ssrn.498153>, p. 2–3.

⁴⁵ 9-ojo Apeliacinio teismo 1988 m. birželio 22 d. nutartis byloje Nr. 849 F.2d 460.

svarbus „deepfake“ kontekste, kadangi parodo, jog sintetinė asmens tapatybės dalis gali būti pripažinta civiliniu deliktu, už kurį priteisiama žalos kompensacija.

Apibendrinami galime teigti, kad asmens deliktinė atsakomybė „deepfake“ kontekste kyla, kai be sutikimo atkuriami ar imituojami tapatybės elementai ir dėl to padaroma reputacinė, emocinė ar ekonominė žala, o doktrina ir praktika įrodo, jog net netiesioginis identiteto atkūrimas sudaro pakankamą pagrindą atsakomybei kilti. Tačiau „deepfake“ turinio padariniai dažnai atsiranda ir dėl tolesnio platinimo, todėl civilinės atsakomybės vertinimas negali apsiriboti vien turinio kūrėjo veiksmiais.

Deliktinė skaitmeninių platformų atsakomybė

Skaitmeninių platformų civilinė atsakomybė „deepfake“ kontekste siejama ne su pačiu turinio sukūrimu, o su jo platinimu, amplifikacija ir nepakankamu turinio moderavimu. E. Douek pabrėžia, kad platformos veikia ne kaip neutralūs tarpininkai, bet kaip struktūriniai sprendimų priėmėjai, valdantys taisykles, algoritmus ir reagavimo mechanizmus, todėl jų atsakomybė gali kilti dėl visos moderavimo sistemos trūkumų. Platformos, kurios žino arba turėtų žinoti apie „deepfake“ keliamą grėsmę asmens teisėms, tačiau nesiima proporcingų priemonių, prisideda prie žalos atsiradimo – tokiu atveju deliktinė atsakomybė grindžiama pareigos rūpintis (angl. duty of care) pažeidimu.⁴⁶

K. Nagumotu pabrėžia, kad socialinės medijos platformos ne tik sudaro sąlygas „deepfake“ turiniui egzistuoti, bet ir aktyviai jį platina per algoritminę amplifikaciją, todėl platformų vaidmuo žalos grandinėje tampa esminis – jos kontroliuoja turinio matomumą, pasiekiamumą ir pašalinimo galimybes. Teisiniai imuniteto modeliai kai kuriose jurisdikcijose riboja platformų atsakomybę, tačiau tai nekeičia fakto, jog platformos faktiškai dalyvauja žalos sklaidoje, todėl jų atsakomybė turėtų būti vertinama per faktinį indėlį į žalos atsiradimą, o ne per formalų tarpininko statusą.⁴⁷

Pavyzdžiui, EŽTT byloje Delfi AS prieš Estiją suformavo esminius kriterijus, pagal kuriuos skaitmeninė platforma gali būti pripažinta deliktu atsakinga už trečiųjų asmenų neteisėtą turinį. Teismas konstatavo, kad portalas, integruojantis komentarų funkciją į savo veiklą, nustatantis jos taisykles ir gaunantis ekonominę naudą, laikomas aktyviu turinio paslaugų teikėju, o ne pasyviu prieglobos (angl. hosting) tarpininku, todėl negali remtis ribotos atsakomybės išimtimis. Platformos pareigos neapsiriboja vien pranešimo ir pašalinimo (angl. notice-and-take-down) procedūra – „Delfi“, leidusi anoniminių komentarus be pakankamų prevencinių priemonių, prisiėmė padidintą atsakomybę ir šiai platformai buvo priteistas 300 eurų neturtinės

⁴⁶ DOUEK, Evelyn (2022). *Content moderation as systems thinking*. Harvard Law Review, p. 526–592.

⁴⁷ NAGUMOTU, Kavyasri (2022). *Deepfakes are taking over social media: Can the law keep up?* IDEA: The Law Review of the Franklin Pierce Center for Intellectual Property 62(2), 113–157 [interaktyvus]. https://law.unh.edu/sites/default/files/media/2022/06/nagumotu_pp113-157.pdf.

žalos atlyginimas.⁴⁸ Pagrindinė bylos reikšmė slypi ne sankcijos dydyje, o teismo suformuluotame principo, kad platformos gali būti atsakingos už akivaizdžiai neteisėto vartotojų sukurto turinio nepašalinimą.

Taigi skaitmeninių platformų deliktinė atsakomybė „deepfake“ kontekste grindžiama ne turinio autoryste, bet faktiniu vaidmeniu platinant ir modoruojant turinį, o EŽTT praktika patvirtina, kad platformos gali būti atsakingos už neveikimą, žinodamos apie žalą asmens teisėms. Atsižvelgiant į tai, toliau nagrinėjama, kada „deepfake“ turinio kūrimas bei platinimas laikytini teisėtais ir kada šios ribos peržengiamos.

Teisėto ir neteisėto panaudojimo ribos „deepfake“ kontekste

„Deepfake“ technologijos gali būti naudojamos ir teisėtais tikslais: balsų atkūrimui po ligos, muziejų interaktyvumui (pvz., Floridos „Dali“ muziejuje), daugiakalbei komunikacijai (2019 m. maliarijos kampanijoje D. Beckhamas atrodė kalbantis keliomis kalbomis), mirusių artimųjų skaitmeniniam „prikėlimui“ per „Deep Nostalgia“ programėlę, Alzheimerio ligonių komunikacijos palengvinimui bei medicinos ir medžiagų mokslo pažangai. Rinkodaros srityje ši technologija leidžia sumažinti kampanijų kaštus ir kurti hiperpersonalizuotą patirtį licencijuojant aktoriaus tapatybę, o žurnalistikoje – apsaugoti šaltinių anonimiškumą represiniuose režimuose.

Tuo tarpu neteisėtas „deepfake“ naudojimas siejamas su asmens teisių, garbės ir orumo, privatumo bei viešosios tvarkos pažeidimais. 2019 m. bendrovė „Deeptrace“ aptiko daugiau kaip penkiolika tūkstančių „deepfake“ įrašų, iš kurių 96 % sudarė pornografija, o 99 % vaizduojamų asmenų buvo moterys – kaip pažymi profesorė D. Citron, ši technologija yra „ginkluojama prieš moteris“. „Deepfake“ taip pat naudojamas bauginimui, šantažui, neapykantos kurtymui ir dezinformacijai – nuo rasistinio mokyklos direktoriaus „deepfake“ iki politiškai jautrių įrašų su B. Obama, N. Pelosi ar T. Perezu.⁴⁹

Kaip jau buvo nustatyta ankstesnėse šio darbo potėmėse, „deepfake“ technologijų panaudojimas savaime nėra nei teisėtas, nei neteisėtas – šią ribą lemia tai, kaip ir kokiomis sąlygomis naudojami asmens tapatybę identifikuojantys elementai, neišvengiamai patenkantys į asmens duomenų bei neturtinių teisių apsaugos reguliavimo sritį. Teisėtas panaudojimas galimas, kai biometrinių požymių naudojimas atitinka BDAR 6 str. numatytą tvarkymo pagrindą ir bent vieną BDAR 9 str. 2 d. išimtį, o teisėtumas siejamas su aiškiu asmens sutikimu konkrečiam tikslui. Kartu vien BDAR laikymasis neužtikrina teisėtumo, nes CK 2.22–2.24 str. įtvirtinta apsaugos sistema taikoma nepriklausomai nuo technologinių priemonių. Neteisėto panaudojimo riba

⁴⁸ *Delfi AS prieš Estiją* [EŽTT], Nr. 64569/09, [2015-06-16]. ECLI:CE:ECHR:2015:0616JUD006456909.

⁴⁹ NNAMDI, Nmesoma; ONIYINDE, Adeyemi O. ir ABEGUNDE, Babalola (2023). *An appraisal of the implications of deep fakes: The need for urgent international legislations*. American Journal of Leadership and Governance, 8(1), 43–52 [interaktyvus]. <https://doi.org/10.47672/ajlg.1540>.

peržengiama, kai tapatybės elementai naudojami be sutikimo arba viršijant jo apimtį, pažeidžiant tiek BDAR 6 ir 9 str., tiek CK 2.22–2.24 str.

Todėl galima daryti išvadą, kad „deepfake“ kontekste teisėto ir neteisėto panaudojimo riba yra nustatoma kompleksiskai – vertinant ne tik technologijos pobūdį, bet ir asmens duomenų tvarkymo teisėtumą pagal BDAR bei asmens tapatybės apsaugą pagal CK nuostatas. Būtent šių elementų visuma leidžia atriboti teisiškai pateisinamus „deepfake“ naudojimo atvejus nuo tokių, kurie laikytini neteisėtais ir sukeliančiais civilinės atsakomybės taikymo pagrindą.

Išvados

Asmens tapatybė civilinėje teisėje nėra apibrėžta kaip savarankiška, vieninga teisinė kategorija, tačiau jos apsauga užtikrinama per tarpusavyje susijusių neturtinių teisių sistemą. Veidas, balsas ir judesiai laikytini reikšmingais tapatybės elementais tiek dėl jų identifikacinės galios, tiek dėl priskyrimo biometriniais duomenimis. „Deepfake“ technologijų kontekste šių elementų panaudojimas be asmens sutikimo kvalifikuojamas kaip neteisėtas civilinės teisės požiūriu, sudarantis prielaidas civilinei atsakomybei taikyti, o vieningos asmens tapatybės sampratos nebuvimas nėra esminė kliūtis tokios atsakomybės taikymui.

„Deepfake“ technologijos apima skirtingus asmens veido, balso ir judesių atkūrimo ar modifikavimo būdus, tačiau civilinės teisės požiūriu lemiamas yra ne technologijos veikimo metodas, o tai, ar jos rezultatas leidžia atpažinti konkretų asmenį. Nors ES teisėje „deepfake“ dažniausiai įvardijamas kaip „sintetinis turinys“, o doktrinoje vartojamos skirtingos sąvokos, teisės taikymo praktikoje nėra susiformavęs konsoliduotas požiūris į šių technologijų sampratą. Dėl to „deepfake“ atvejai civilinėje teisėje vertinami ne kaip atskira teisinė kategorija, bet taikant bendrąsias asmens duomenų apsaugos ir neturtinių teisių gynimo normas, kurios ir formuoja civilinės atsakomybės taikymo ribas.

„Deepfake“ turinio kūrimas ir platinimas be asmens sutikimo paprastai pažeidžia ne vieną, o kelias tarpusavyje susijusias asmens neturtines teises – teisę į atvaizdą, privataus gyvenimo neliečiamumą bei garbę ir orumą. Civilinės atsakomybės taikymas tokiais atvejais grindžiamas sistemišku šių teisių vertinimu, atsižvelgiant į galimybę atpažinti konkretų asmenį, sutikimo ribas ir turinio poveikį. Nors Lietuvos ir užsienio teismų praktika dar nėra vieninga, ji patvirtina tendenciją „deepfake“ atvejus vertinti kaip realius civilinių teisių pažeidimus, už kuriuos gali būti taikomos civilinės teisės gynimo priemonės, įskaitant neturtinės žalos atlyginimą.

Šaltinių sąrašas

Teisės aktai

ES teisės aktai

Europos Parlamento ir Tarybos 2016 m. balandžio 27 d. reglamentas (ES) 2016/679 dėl fizinų asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas). OL L 119, 2016.

Europos Parlamento ir Tarybos 2024 m. birželio 13 d. reglamentas (ES) Nr. 2024/1689 kuriuo nustatomos suderintos dirbtinio intelekto taisyklės ir iš dalies keičiami reglamentai (EB) Nr. 300/2008, (ES) Nr. 167/2013, (ES) Nr. 168/2013, (ES) 2018/858, (ES) 2018/1139 ir (ES) 2019/2144 ir direktyvos 2014/90/ES, (ES) 2016/797 ir (ES) 2020/1828 (Dirbtinio intelekto aktas). OL L 1689 2024.7.12.

Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija (1950). Valstybės žinios, 1995, 40-987.

LR teisės aktai

Lietuvos Respublikos Konstitucija. Lietuvos Respublikos piliečių priimta 1992 m. spalio 25 d. referendume. Valstybės žinios, 1992, 33–1014.

Lietuvos Respublikos civilinis kodeksas. 2000 m. liepos 18 d. VIII-1864. Valstybės žinios, 2000, 74–2262.

Teismų praktika

EŽTT teismų praktika

Delfi AS prieš Estiją [EŽTT], Nr. 64569/09, [2015-06-16]. ECLI:CE:ECHR:2015:-0616JUD006456909.

Von Hannover prieš Vokietiją [EŽTT], Nr. 59320/00, [2004-06-24]. ECLI:CE:ECHR:2004:-0624JUD005932000.

Lietuvos teismų praktika

Lietuvos Aukščiausiojo Teismo 2012 m. vasario 13 d. nutartis civilinėje byloje Nr. 3K-3-22/2012.

Lietuvos Aukščiausiojo Teismo 2024 m. gegužės 16 d. nutartis civilinėje byloje Nr. e3K-3-73-421/2024.

Lietuvos Aukščiausiojo Teismo 2024 m. spalio 8 d. nutartis civilinėje byloje Nr. e3K-3-173-378/2024.

JAV Teismų praktika

Kalifornijos valstijos Aukštesniojo teismo 2025 m. liepos 11 d. nutartis byloje Nr. 23CV028772.

Pietų Niujorko apygardos teismo 2025 m. liepos 10 d. nutartis byloje Nr. 1:24-cv-03770.

Ilinojaus šiaurinės apygardos teismo 2025 m. kovo 20 d. nutartis byloje Nr. 21-cv-00135.
9-ojo Apeliacinio teismo 1988 m. birželio 22 d. nutartis byloje Nr. 849 F.2d 460.

Specialioji literatūra

- ANTINIENĖ, Dalia (2002). Asmens tautinio tapatumo tapsmas. Sociopsichologinės šio proceso interpretacijos. Sociologija. Mintis ir veiksmas, 10.
- BAKANSKAS, Algimantas; BARTKUS, Gintautas; DOMINAS, Giedrius ir kt. (2002). Civilinio kodekso komentaras. Antroji knyga: Asmenys. Vilnius: Justitia.
- Cambridge Dictionary (n.d.). Biometrics. Iš: Cambridge Dictionary [interaktyvus]. <https://dictionary.cambridge.org/dictionary/english/biometrics>.
- CARMAUX, Jules (2025). Jake Paul's AI Gambit: Investments and Deepfake [interaktyvus]. <https://www.clickanalytic.com/jake-pauls-ai-gambit-investments-deepfake/>.
- CHESNEY, Bobby ir CITRON, Danielle (2019). Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. California Law Review.
- Delfi (2026-01-12). Dirbtiniu intelektu sukurtas Ingos Ruginienės šokis papiktino lietuvius: paduočiau į teismą [interaktyvus]. <https://www.delfi.lt/veidai/zmones/ingos-ruginienes-sokis-papiktino-lietuvius-paduociau-i-teisma-120197097>.
- DOUEK, Evelyn (2022). Content moderation as systems thinking. Harvard Law Review.
- EUROPEAN DATA PROTECTION SUPERVISOR (2019). Bendrojo duomenų apsaugos reglamento (BDAR) taikymas ES institucijoms: jūsų teisės skaitmeniniame amžiuje. Publications Office of the European Union. <https://data.europa.eu/doi/10.2804/150178>.
- HE, Shijing; LEI, Yaxiong; ZHANG, Zihan ir kt. (2025). Identity Deepfake Threats to Biometric Authentication Systems: Public and Expert Perspectives. arXiv [interaktyvus]. <https://arxiv.org/abs/2506.06825>.
- HRISTOV, Georgi (2025). Genuine harms behind artificial content: How EU regulation can combat malicious use of deep fake technology. Social Science Research Network [interaktyvus]. <https://ssrn.com/abstract=5634715>.
- JAIN, Anil K.; ROSS, Arun A.; NANDAKUMAR, Karthik (2011). Introduction to Biometrics. New York: Springer.
- MIRSKY, Yisroel; LEE, Wenke (2020). The creation and detection of deepfakes: A survey. arXiv [interaktyvus]. <https://arxiv.org/abs/2004.11138>.
- MURRAY, Michael D. (2024). Deceptive exploitation: Deepfakes, the rights of publicity and privacy, and trademark law (SSRN Working Paper No. 4981531). SSRN. <https://doi.org/10.2139/ssrn.498153>.
- NAGUMOTU, Kavyasri (2022). Deepfakes are taking over social media: Can the law keep up? IDEA: The Law Review of the Franklin Pierce Center for Intellectual Property 62(2), 113–157 [interaktyvus]. https://law.unh.edu/sites/default/files/media/2022/06/nagumotu_pp113-157.pdf.
- NEGREIRO, Mar (2025). Children and Deepfakes. European Parliamentary Research Service, PE 775.855, [interaktyvus]. [https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/775855/EPRS_BRI\(2025\)775855_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/775855/EPRS_BRI(2025)775855_EN.pdf).
- NNAMDI, Nmesoma; ONIYINDE, Adeyemi O. ir ABEGUNDE, Babalola (2023). An appraisal of the implications of deep fakes: The need for urgent international legislations. American Journal of Leadership and Governance, 8(1), 43–52 [interaktyvus]. <https://doi.org/10.47672/ajlg.1540>.

- NORKŪNAS, Algis. (2002). Kaltė kaip civilinės atsakomybės pagrindas. *Jurisprudencija*, 28(20).
- Oxford University Press (n.d.). Deepfake. Iš: Oxford English Dictionary [interaktyvus]. <https://doi.org/10.1093/OED/9547101155>.
- PARIS, Britt ir DONOVAN, Joan (2019). Deepfakes and Cheap Fakes. Data & Society Research Institute.
- PENG, Huijuan ir LEE, Pey W. (2025). Reimagining U.S. tort law for deepfake harms: Comparative insights from China and Singapore. Singapore Management University.
- ROMERO MORENO, Felipe (2024). Generative AI and deepfakes: a human rights approach to tackling harmful content. *International Review of Law, Computers & Technology*, 38(3). <https://doi.org/10.1080/13600869.2024.2324540>.
- ŠTITILIS, Darius ir LAURINAITIS, Marius (2009). Tapatybės vagystė elektroninėje erdvėje. *Information & Media*, 50.
- Valstybinė duomenų apsaugos inspekcija (2017). Biometrinių duomenų tvarkymas elektroninėje erdvėje. Rekomendacija [interaktyvus]. https://vdai.lrv.lt/uploads/vdai/documents/files/Rekomend_Biometriniai_2017.pdf.
- Valstybinės lietuvių kalbos komisijos konsultacijų bankas (n.d.). Koks angl. „deepfake“ lietuviškas atitikmuo? Iš: Valstybinė lietuvių kalbos komisija [interaktyvus]. <https://vlkk.lt/konsultacijos/13729-2019-06-18-06-30-56>.
- VACCARI, Cristian; CHADWICK, Andrew (2020). Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News. *Social Media + Society*.
- WESTERLUND, Mika (2019). The Emergence of Deepfake Technology: A Review. *TIM Review*.

SANTRAUKA

Išplitus „deepfake“ technologijoms, atsirado galimybė itin tikroviškai atkurti asmens tapatybės požymius – veidą, balsą ar judesius – ir be jo sutikimo sukurti klaidinantį skaitmeninį turinį. Toks asmens tapatybės panaudojimas kelia grėsmę asmens neturtinėms teisėms ir suponuoja civilinės atsakomybės taikymo klausimus. Atsižvelgiant į tai, šio darbo tikslas – išanalizuoti civilinės atsakomybės taikymą tais atvejais, kai asmens tapatybės elementai be jo sutikimo naudojami „deepfake“ turinio kūrimui ir platinimui. Darbo objektas apima Lietuvos civilinės teisės ir Europos Sąjungos duomenų apsaugos normų taikymą „deepfake“ technologijų kontekste, taip pat Lietuvos ir užsienio teismų praktiką. Darbe nagrinėjama asmens tapatybės samprata, biometrinių duomenų teisinis reglamentavimas ir „deepfake“ technologijų teisinė reikšmė, taip pat vertinama asmens neturtinių teisių apsauga ir civilinės atsakomybės taikymo prielaidos. Atlikta analizė leidžia konstatuoti, kad asmens veido, balso ar judesių panaudojimas „deepfake“ turinyje be jo sutikimo gali pažeisti teisę į atvaizdą, privataus gyvenimo neliečiamumą, garbę ir orumą: tokiais atvejais, nustačius visas

civilinės atsakomybės sąlygas, taikomos civilinės teisės gynimo priemonės, įskaitant neturtinės žalos atlyginimą, o atsakomybės ribos vertinamos atsižvelgiant į pažeidimo pobūdį ir faktines bylos aplinkybes.

SUMMARY

With the proliferation of “deepfake” technologies, it has become possible to highly realistically recreate elements of a person’s identity – such as facial features, voice, or movements – and to generate misleading digital content without their consent. Such use of a person’s identity poses a threat to their personal moral rights and raises questions concerning the application of civil liability. In this context, the aim of this paper is to analyze the application of civil liability in cases where elements of a person’s identity are used without their consent in the creation and dissemination of “deepfake” content. The paper’s objective includes the application of Lithuanian civil law and European Union data protection rules in the context of “deepfake” technologies, as well as Lithuanian and foreign case law. The paper examines the concept of personal identity, the legal regulation of biometric data, and the legal significance of “deepfake” technologies, and assesses the protection of personal moral rights and the conditions for the application of civil liability. The analysis leads to the conclusion that the use of a person’s face, voice, or movements in “deepfake” content without their consent may infringe the right to one’s image, privacy, honor, and dignity: in such cases, where all conditions of civil liability are established, civil law remedies are applied, including compensation for non-pecuniary damage, while the limits of liability are determined with regard to the nature of the infringement and the factual circumstances of the case.