ASMENS DUOMENYS BESIKEIČIANČIAME PASAULYJE:

praktinis straipsnių rinkinys

Įžanga

Mieli LDAPA nariai,

Pristatome LDAPA narių parengtą praktinių-mokslinių straipsnių apie aktualias Lietuvos duomenų saugos problemas rinkinį. Temų įvairovė plati – darbuotojo sutikimo panaudojimo galimybės, referendumo keliamos duomenų saugos problemos, biometriniai duomenys - tad bus naudingas plačiam specialistų ratui.

Tai praktikai-praktikams tipo leidinys. Jo pasirodymas patvirtina, kad Lietuvoje išaugo kompetentingų ir savo nišas duomenų saugos srityje radusių profesionalų bendruomenė. Taip pat galime pasidžiaugti, kad mūsų nariai supranta atviros prieigos duomenų naudą privatumo praktikos vystymuisi. Dėkojame autoriams už investuotą laiką ir neatlygintiną dalinimąsi savo patirtimi bei įžvalgomis bendram LDAPA narių ir kitų privatumo srities kolegų labui. Smagu, kad LDAPA subūrusios idėjos - kolegiškumas ir nišinių profesinių žinių sklaida – įgauna naujus pavidalus, augina mūsų bendruomenės profesionalumą, kuria aiškią vertę sprendžiant kasdienes problemas.

LDAPA valdyba

TURINYS

TINKAMAS ASMENS DUOMENŲ APSAUGOS UŽTIKRINIMAS VYKDANT PREKIŲ AR PASLAUGŲ RINKODARĄ

Brigida Bacienė, Loreta Andziulytė

Asmens duomenų tvarkymo, vykdant tiesioginę rinkodarą, teisinis reglamentavimas

Pastaraisiais metais dėl 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (toliau BDAR) įsigaliojimo ypač daug dėmesio buvo skiriama asmens duomenų apsaugai ir BDAR nuostatų aiškinimui.

Praktikoje taikant BDAR kildavo klausimų, ar su BDAR įsigaliojimu įvyko esminė asmens duomenų tvarkymo reforma, įskaitant ir tiesioginės rinkodaros srityje ir ar BDAR nuostatos įvedė naujas taisykles palyginus su jau iki BDAR įsigaliojimo taikomomis teisės normomis asmens duomenų tvarkymo aspektu.

Šiame straipsnyje siekiama trumpai apžvelgti pagrindinį teisinį reguliavimą asmens duomenų tvarkymo srityje vykdant tiesioginę rinkodarą, praktinius tokios veiklos aspektus bei pateikti Europos Bendrijos valstybių teisinio reguliavimo ar visuomeninių iniciatyvų ypatumus, saugant duomenų subjektus nuo nepageidaujamų tiesioginės rinkodaros pranešimų.

Prieš teisinių reikalavimų, taikomų tiesioginei rinkodarai, analizę, būtina apsibrėžti, kas yra laikoma tiesiogine rinkodara ir kokiems konkrečiai veiksmams, taikomi duomenų tvarkymo reikalavimai.

Klausimų nekyla, kai siunčiami paprasti pranešimai, kuriais siekiama pareklamuoti prekę, paslaugą ar pačią įmonę, tačiau šiai dienai dėl technologijų pažangos, rinkodaros turinio pateikimo būdas pasikeitė, todėl užuot siuntus paprastus elektroninius laiškus į pašto dėžutes, dabar tikslinė vartotojų elgesiu grindžiama reklama taip pat pasirodo išmaniųjų telefonų ir kompiuterių ekranuose, reklama taip pat įterpiama į išmaniuosius daiktus. Be to, reklama vis tikslingiau pritaikoma konkretiems vartotojams: užuot remiantis paprastais klientus apibūdinančiais profiliais, vartotojų veikla internete ir ne internete vis labiau sekama, duomenys apie ją saugomi ir analizuojami vis sudėtingesniais automatizuotais metodais[1]. Įmonės siekia analizuoti arba prognozuoti konkrečių klientų asmeninius pageidavimus, elgesį ir pažiūras, kuriais remiantis vėliau bus „taikomos priemonės arba priimami sprendimai“ tų klientų atžvilgiu. Todėl, norint sekti asmenis ir kurti jų profilius tiesioginės rinkodaros, vartotojų elgesiu grindžiamos reklamos, prekybos duomenimis, reklamos pagal buvimo vietą arba sekimu grindžiamų skaitmeninės rinkos

[1] 29 straipsnio duomenų apsaugos darbo grupės nuomonė Nr. 06/2014 „Dėl duomenų valdytojo teisėtų interesų sampratos pagal Direktyvos 95/46/EB 7 straipsnį“.

tyrimų tikslais, reikia irgi laikytis asmens duomenų tvarkymui būtinų reikalavimų.

Taigi, tiesioginės rinkodaros sąvoka šiai dienai neapsiriboja tradiciniu pranešimu siuntimu, bet taip pat ir veikla, kuria siekiama analizuoti kliento profilį ir prognozuoti jo elgesį tam, kad vėliau remiantis surinkta informacija būtų galima priimti konkrečius sprendimus.

Šiame straipsnyje nagrinėjant asmens duomenų apsaugos reguliavimą, vykdant prekių ir paslaugų tiesioginę rinkodarą, remiamasi iš esmės dviem pagrindiniais Europos Bendrijos teisės aktais - BDAR ir 2002 m. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (toliau E. Privatumo direktyva), kurią ateityje pakeisti turėtų šiuo metu svarstomas E. Privatumo reglamentas (Europos Komisijos pasiūlymas „Europos Parlamento ir Tarybos reglamentas dėl teisės į privatų gyvenimą ir asmens duomenų apsaugos elektroninių ryšių sektoriuje, kuriuo panaikinama Direktyva 2002/58/EB (Reglamentas dėl privatumo ir elektroninių ryšių“) [2].

BDAR, kuris įsigaliojo 2018 m. gegužės 25 d., yra tiesioginio taikymo aktas, todėl nacionaliniu mastu nėra priimami jį atkartojantys teisės aktai, o reglamentuojama tik tiek, kiek leidžia nacionaliniu mastu nustatyti papildomas taisykles pats BDAR. Lietuvoje galiojantis Lietuvos Respublikos asmens duomenų apsaugos įstatymas (toliau ADTAĮ), papildomai nurodo, kad draudžiama tvarkyti asmens kodą tiesioginės rinkodaros tikslais (ADTAĮ 3 straipsnio 3 dalis).

Ne mažiau svarbus teisės aktas, o ypač nagrinėjamai temai, yra E. Privatumo direktyva, kuria iš esmės buvo siekiama apsaugoti fizinių asmenų pagrindines teises ir ypač jų teisę į privatumą, taip pat teisėtus juridinių asmenų interesus ir nustatyti specialias elektroninių ryšių paslaugų teikimo taisykles. E. Privatumo direktyvos nuostatos[3] laikytinos papildančiomis BDAR reguliavimą ir nustatančiomis papildomą elektroninių ryšių paslaugų naudotojų apsaugą, palyginti su BDAR. E. Privatumo direktyvos nuostatos Lietuvoje yra perkeltos Lietuvos Respublikos elektroninių ryšių įstatymą (toliau ERĮ).

ADTAĮ 2 straipsnio 1 dalyje nustatyta, kad tiesioginė rinkodara laikoma veikla, kurios tikslas – paštu, telefonu arba kitokiu tiesioginiu būdu siūlyti asmenims prekes ar paslaugas ir (arba) teirautis jų nuomonės dėl siūlomų prekių ar paslaugų. Valstybinės duomenų apsaugos inspekcijos nuomone, tiesioginės rinkodaros pasiūlymais nebūtų laikomi, pvz., sveikinimai, elektroninių laiškų siuntimas, kurių turinys susijęs su sutarčių vykdymu, priminimas apie skolą ir

[2] https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A52017PC0010
[3] E. Privatumo direktyvos nuostatos buvo perkeltos į Lietuvos Respublikos elektroninių ryšių įstatymą (toliau ERĮ), kuris iš esmės nustato analogiškas taisyklės, kaip ir E. Privatumo direktyvoje.

kt. Šiuo atveju asmens duomenų tvarkymas turėtų būti grindžiamas bent vienu asmens duomenų teisėto tvarkymo kriterijumi[4].

Tiesioginė rinkodara yra susijusi su „reklamos“ sąvoka. Lietuvos Respublikos reklamos įstatymo 2 straipsnio 8 dalyje numatyta, kad reklama – bet kokia forma ir bet kokiomis priemonėmis skleidžiama informacija, susijusi su asmens ūkine komercine, finansine ar profesine veikla, skatinanti įsigyti prekių ar naudotis paslaugomis, įskaitant nekilnojamojo turto įsigijimą, turtinių teisių ir įsipareigojimų perėmimą.

Kalbant apie „tiesioginės rinkodaros“ sąvoka būtina turėti omenyje, kad po šia sąvoka patenka bet kokios reklaminės medžiagos, skirtos konkretiems asmenims, perdavimas bet kokiomis priemonėmis.

Apibendrinant, tiesioginė rinkodara turi plačią sampratą ir ja galima apibūdinti keliais bendrais požymiais:

(i) reklaminiu pranešimu siekiama pareklamuoti subjektą, prekes, paslaugas, pranešti apie akcijas, pasiūlymus ir pan. Siunčiami pranešimai, kuriais asmenys informuojami apie jų pateiktus užsakymus, nepateks į tiesioginės rinkodaros sąvoką, nes tai laikoma pirkimo sutarties vykdymu;

(ii) reklaminis pranešimas gali būti perduodamas įvairiomis priemonėmis (el. paštu, paštu, telefonu, telefonų programėlių pagalba ir pan.). Šiai dienai tiesioginė rinkodara neapsiriboja vien pašto, elektroninio pašto, SMS, ji buvo išplėtota iki internetu teikiamų paslaugų, pavyzdžiui interneto telefonijos, pokalbių programėlių, kaip *Viber, Whatsapp*, ir t.t.

Žemiau pateikiama BDAR ir E. Privatumo direktyvos nuostatų analizė, susijusi su tiesioginės rinkodaros vykdymu.

E. Privatumo direktyva

E. Privatumo direktyva yra svarbi teisinė privatumo užtikrinimo priemonė skaitmeniniame amžiuje, ypač siekiant apsaugoti asmenis nuo nepageidaujamų pranešimų, teikiamų elektroninėmis priemonėmis.

E. Privatumo direktyva taikoma tiesioginės rinkodaros pranešimams, kurie yra siunčiami elektroninių ryšių pagalba, kas reiškia, kad ši direktyva nėra taikoma tiesioginei rinkodarai, kuri vykdoma pavyzdžiui paprastu paštu, ar tiesiogiai kontaktuojant su asmeniu be elektroninių priemonių pagalbos.

Žemiau pateikiamos pagrindinės tiesioginės rinkodaros pranešimų, siunčiamų elektroninių ryšių pagalba duomenų subjektams sąlygos.

---

[4] https://vdai.lrv.lt/lt/naujienos/tiesiogine-rinkodara-ir-bendrasis-duomenu-apsaugos-reglamentas-bdar

Opt-in ir soft opt in sutikimai

Pagrindinė taisyklė, kuri įtvirtinta E. Privatumo direktyvoje yra ta, kad prieš siunčiant tiesioginės rinkodaros pranešimus, turi būti gautas duomenų subjekto sutikimas[5]. Toks iš anksto duodamas sutikimas dar kitaip vadinamas „*opt-in"* sutikimu.

Pati E. Privatumo direktyva neapibrėžia, kas laikytina „sutikimu", tačiau jos 2 straipsnio f punktas bei preambulės 17 punktas nurodo, kad sutikimas suprantamas taip, kaip „*apibrėžta Direktyvoje 95/46/EB*". Direktyvos 95/46/EC 2 straipsnio h punktas nurodo, kad *„duomenų subjekto sutikimas reiškia bet kurį savanoriškai ir žinomai duotą konkretų duomenų subjekto pareiškimą, kuriuo duomenų subjektas nurodo savo sutikimą, kad būtų tvarkomi su juo susiję duomenys*".

Direktyvą 95/46/EC pakeitė BDAR, todėl nors E. Privatumo direktyvoje apibūdinant „sutikimą" duodama nuoroda į Direktyvą 95/46/EC, tačiau tokios nuorodos turi būti laikomos nuorodomis į BDAR nuostatas, o nuorodos į 29 straipsnio darbo grupės gaires į Europos duomenų apsaugos valdybos (toliau EDAV) gaires[6], todėl nagrinėjant „sutikimą", kaip teisinį pagrindą, turi būti analizuojamos BDAR nuostatos ir EDAV gairės[7].

E. Privatumo direktyvos nuostatos buvo perkeltos į ERĮ, kurios iš esmės nustato analogiškas taisykles. ERĮ 69 straipsnio 1 dalyje nustatyta, kad *elektroninių ryšių paslaugas, įskaitant elektroninio pašto pranešimų siuntimą,*

---

[5] „*Tokio pobūdžio neužsakytiems komerciniams pranešimams tiesioginės rinkodaros tikslais reikėtų iš anksto gauti aiškų gavėjo sutikimą prieš adresuojant jam tokius pranešimus. Vienai bendrai rinkai reikia suderinto požiūrio į šią problemą, kuris leistų taikyti verslui ir naudotojams paprastas taisykles visoje Bendrijoje"* (E.Privatumo direktyvos 40 punktas);
„*Naudoti automatinio skambinimo sistemas be žmogaus įsiterpimo (skambinimo automatus), faksimilinius aparatus (faksus) ar elektroninį paštą tiesioginės rinkodaros tikslais gali būti leidžiama tik gavus išankstinį abonentų sutikimą*" (E.Privatumo direktyvos 13 straipsnio 1 dalis).

[6] BDAR 94 straipsnio 2 dalis.

[7] 29 straipsnio darbo grupė dėl dabartinės E. privatumo direktyvos pažymi, kad nuorodos į panaikintą Direktyvą 95/46/EB laikomos nuorodomis į BDAR8 ; tas pats taikoma ir nuorodoms į dabartinės Direktyvos 2002/58/EB nuostatas dėl sutikimo, nes E. privatumo reglamentas (dar) nebus įsigaliojęs nuo 2018 m. gegužės 25 d. Pagal BDAR 95 straipsnį nenustatoma papildomų prievolių, susijusių su duomenų tvarkymu viešaisiais ryšių tinklais teikiant viešai prieinamas elektroninių ryšių paslaugas, tiek, kiek E. privatumo direktyvoje yra nustatytos specialios prievolės siekiant to paties tikslo. 29 straipsnio darbo grupė pažymi, kad sutikimo reikalavimai pagal BDAR laikomi ne „papildoma prievole", o išankstinėmis teisėto duomenų tvarkymo sąlygomis. Todėl BDAR nustatytos galiojančio sutikimo gavimo sąlygos taikytinos ir tokiomis aplinkybėmis, kurios įeina į E. privatumo direktyvos taikymo sritį.

naudoti tiesioginės rinkodaros tikslu leidžiama tik gavus išankstinį abonento ar registruoto elektroninių ryšių paslaugų naudotojo sutikimą.

Lietuvos Respublikos reklamos įstatymo 13 straipsnis taip pat nurodo, kad siunčiant reklamą yra būtinas vartotojo sutikimas: „*reklama telefonu, telefaksu, teleksu, elektroniniu paštu gali būti teikiama tik reklamos vartotojo sutikimu arba jo prašymu. Draudžiama tiesiogiai teikti reklamą konkrečiam asmeniui, jeigu yra aiškiai išreikštas šio asmens nesutikimas*".

Nors galioja bendra taisyklė, kad norint siųsti reklaminius pranešimus būtinas duomenų subjekto sutikimas, tačiau tiek E. Privatumo direktyva, tiek ERĮ numato vieną išimtį, kada gali būti naudojamasi elektroniniais kontaktiniais duomenimis, neprašant atskiro duomenų subjekto sutikimo, bet leidžiant duomenų subjektui lengvai atsisakyti siunčiamų tiesioginės rinkodaros pranešimų, taip vadinamas „*soft opt-in*" sutikimo variantas.

E. Privatumo direktyvos preambulės 41 punktas numato, kad *„(41) Atsižvelgiant į esamus naudotojų santykius, yra protinga leisti pasinaudoti elektroniniais kontaktiniais duomenimis papildomai siūlant panašių gaminių ir paslaugų, tačiau tik tai pačiai bendrovei, kuri buvo gavusi elektroninius kontaktinius duomenis pagal Direktyvą 95/46/EB. Gavus tokius duomenis, reikia aiškiai ir suprantamai informuoti naudotoją apie tolesnį jų naudojimą tiesioginės rinkodaros tikslais bei suteikti jam galimybę atsisakyti tokio naudojimo. Su kiekvienu nauju pranešimu tiesioginės rinkodaros tikslais naudotojas pakartotinai ir nemokamai informuojamas apie šią galimybę, tačiau apmoka visas atsisakymo perdavimo išlaidas".*

E. Privatumo direktyvos 13 straipsnio 2 dalyje nurodyta, kad „*Nepaisant to, kas pasakyta šio straipsnio 1 dalyje, jeigu fiziniai ar juridiniai asmenys parduodami produktus ar teikdami paslaugas pagal Direktyvą 95/46/EB gauna iš savo klientų jų elektroninio pašto kontaktinius duomenis, šie fiziniai ar juridiniai asmenys gali pasinaudoti elektroniniais kontaktiniais duomenimis savo pačių panašių prekių ar paslaugų tiesioginei rinkodarai su sąlyga, kad klientams yra suteikiama aiški ir lengvai įgyvendinama galimybė nemokamai ir paprastomis priemonėmis nesutikti su tokiu elektroninių kontaktinių duomenų naudojimu arba, jei klientas iš pradžių neprieštaravo tokiam duomenų naudojimui, siunčiant kiekvieną žinutę*".

Tokia pat išimties taisyklė yra numatyta ir ERĮ 69 straipsnio 2 dalyje, kurioje įtvirtinta, kad *asmuo, kuris teikdamas paslaugas ar parduodamas prekes ADTAĮ nustatyta tvarka ir sąlygomis gauna iš savo klientų elektroninio pašto kontaktinius duomenis, gali naudoti šiuos kontaktinius duomenis savo paties panašių prekių ar paslaugų rinkodarai, jei klientams yra suteikiama aiški, nemokama ir lengvai įgyvendinama galimybė nesutikti arba atsisakyti tokio kontaktinių duomenų naudojimo pirmiau nurodytais tikslais, kai šie duomenys yra renkami ir, jei klientas iš pradžių neprieštaravo dėl tokio duomenų naudojimo, siunčiant kiekvieną žinutę*.

Taigi, ERĮ 69 straipsnis įpareigoja iš anksto gauti asmens sutikimą prieš siunčiant tiesioginę rinkodarą, išskyrus išimtį, susijusią su savo klientais, kurių atžvilgiu gali būti naudojamas taip vadinamasis „*soft opt-in*“ sutikimo variantas, suteikiantis asmeniui galimybę atsisakyti duomenų naudojimo tiesioginės rinkodaros tikslu, tačiau nereikalaujantis sutikimo išreikšti aktyviais veiksmais.

Tai reiškia, kad papildomo sutikimo prieš siunčiant reklaminius pranešimus iš savo kliento nereikia gauti, jei yra išpildomos visos žemiau nurodytos sąlygos:

- *naudojamasi savo kliento elektroniniais kontakto duomenimis* – šis reikalavimas paprastai aiškinamas per du aspektus: a) turi būti savo klientas ir b) tiesioginei rinkodarai vykdyti galimas tik elektroninių kontaktinių duomenų naudojimas. Kalbant apie kliento sąvoką, Jungtinės Karalystės priežiūros institucija (Information Commisioner's Office, toliau ICO) savo rekomendacijose „Tiesioginė rinkodara“ nurodė, kad klientu neturi būti laikomas tas, kuris įsigijo kokią nors prekę, o tai reiškia, kad klientu šio įstatymo išimties kontekste gali būti laikomas asmuo, su kuriuo pradėtos derybos dėl pardavimo. ICO nurodo, kad klientu laikomas asmuo, kuris aktyviais veiksmais išreiškė interesą pirkti įmonės produktą ar paslaugą. Taigi, nebūtina, kad tarp asmens ir įmonės jau būtų įvykdyta sutartis.
- *jei elektroniniais kontaktiniais duomenimis naudojamasi savo tokių pačių ar panašių prekių tiesioginei rinkodarai* – išimtimi gali pasinaudoti tik tos įmonės, kurios jau turi savo klientų elektroninių kontaktų duomenis. Tokia išimtis nėra taikoma įmonėms, kurios įsigyja kontaktų bazes. „*Tokių pačių*“ ar „*panašių*“ prekių sąvoka ERĮ nėra įtvirtinta, tačiau remiamasi bendru principu, ko gali tikėtis klientas, atsižvelgiat į tai kokias prekes įsigijo ar kokiomis paslaugomis naudojosi ar dėl kokių prekių ir paslaugų kreipėsi. Kiekvienu konkrečiu atveju vertinama „*tokių pačių*“ ar „*panašių*“ prekių sąvoka atskirai.
- *jei suteikiama galimybė nemokamai ir paprastu būdu atsisakyti tokių pranešimų* – įmonės turi užtikrinti, kad duomenų subjekto teisė atsisakyti reklaminių pranešimų būtų įgyvendinama taip pat paprastai, kaip ir pirminis tokių duomenų rinkimas ir sutikimo gavimas, pavyzdžiui jei tiesioginės rinkodaros pranešimai siunčiami elektronine forma, tai ir teisė jų atsisakyti turi būti įgyvendinama elektronine forma. Geroji praktika laikoma, kai duomenų subjektui suteikiama galimybė tiesiogiai atsakyti į žinutę ar paspausti aktyvią nuorodą „atsisakyti pranešimų“.
- *jei klientas iš pradžių neprieštaravo tokių pranešimų siuntimui*- įmonė duomenų subjektui turi suteikti galimybę nuo pradžių atšaukti savo sutikimą. Nesutikimo su siunčiamais pranešimais teisė turi būti įgyvendinama tiek tuo momentu, kada buvo renkami asmens duomenis, tiek kiekviename siunčiamame tiesioginės rinkodaros pranešime. Įmonės negali preziumuoti, kad visi klientai pageidauja

ateityje gauti tiesioginės rinkodaros pranešimus, todėl negalima remtis vien tik „*soft opt in*“ taisykle, įmonės turi suteikti klientui galimybę atšaukti tokių pranešimų gavimą.

Teisė atšaukti duotą sutikimą

Neatsiejama nuo tiesioginės rinkodaros pranešimų siuntimo, yra duomenų subjekto teisė atšaukti duotą sutikimą. Šiuo atveju nepriklausomai nuo to, ar įmonės naudojasi „*opt-in*“ ar „*soft opt-in*“ sutikimo mechanizmu, ir ar įmonės vykdo tų pačių ar panašių prekių ar paslaugų ar kitų prekių ir paslaugų tiesioginę rinkodara, duomenų subjektas turi absoliučią teisę bet kuriuo momentu atšaukti duotą sutikimą.

Ši duomenų subjekto teisė išplaukia tiek iš E. Privatumo direktyvos ir ją įgyvendinančio ERĮ, tiek iš BDAR, kai bendrai kalbama apie sutikimo atšaukimą.

E. Privatumo direktyvos preambulės 41 punktas numato, kad *„(41)* <...> *Gavus tokius duomenis, reikia aiškiai ir suprantamai informuoti naudotoją apie tolesnį jų naudojimą tiesioginės rinkodaros tikslais bei suteikti jam galimybę atsisakyti tokio naudojimo. Su kiekvienu nauju pranešimu tiesioginės rinkodaros tikslais naudotojas pakartotinai ir nemokamai informuojamas apie šią galimybę, tačiau apmoka visas atsisakymo perdavimo išlaidas“.*

E. Privatumo direktyvos 13 straipsnio 2 dalyje nurodyta, kad „<..> *su sąlyga, kad klientams yra suteikiama aiški ir lengvai įgyvendinama galimybė nemokamai ir paprastomis priemonėmis nesutikti su tokiu elektroninių kontaktinių duomenų naudojimu* <...>“.

ERĮ 69 straipsnio 2 dalyje yra įtvirtinta, kad įmonės turi suteikti *aiškią, nemokamą ir lengvai įgyvendinamą galimybę nesutikti arba atsisakyti tokio kontaktinių duomenų naudojimo pirmiau nurodytais tikslais, kai šie duomenys yra renkami.* Pagal ERĮ 69 straipsnio 3 dalį elektroninio pašto pranešime, kuriuo vykdoma tiesioginė rinkodara, *turi būti nurodoma siuntėjo, kurio vardu informacija siunčiama, tapatybė arba galiojantis adresas, kuriuo elektroninio pašto pranešimą gavęs asmuo galėtų pareikalauti nutraukti tokios informacijos siuntimą*.

Aukščiau nurodytos E. Privatumo direktyvos ir ERĮ nuostatos yra skirtos elektroninių ryšių priemonėmis siunčiamiems pranešimams bei kai kalbama apie išimtis elektroninio paštu siunčiamiems pranešimams, tačiau tai nereiškia, kad kitais atvejais nėra taikomas reikalavimas suteikti teisę duomenų subjektui atšaukti duotą sutikimą.

BDAR 7 straipsnio 3 dalyje nurodyta, kad „*duomenų subjektas turi teisę bet kuriuo metu atšaukti savo sutikimą. Sutikimo atšaukimas nedaro poveikio sutikimu pagrįsto duomenų tvarkymo, atlikto iki sutikimo atšaukimo, teisėtumui. Duomenų subjektas apie tai informuojamas prieš jam duodant sutikimą. Atšaukti sutikimą turi būti taip pat lengva kaip jį duoti*“. BDAR šiuo atveju

įtvirtinta bendra taisyklė, kad visais atvejais, kai asmens duomenų tvarkymo pagrindas yra sutikimas, tai duomenų subjektas turi teisę bet kuriuo metu tą sutikimą atšaukti. Taigi, ši taisyklė taikoma ir kai kalbame apie tiesioginės rinkodaros pranešimus. BDAR, kaip ir E. Privatumo direktyva ir ERĮ nustato ir atšaukimo teisės įgyvendinimo sąlygas, t. y. a) atšaukti sutikimą turi būti taip pat lengva, kaip ir jį duoti; b) duomenų subjektas turi būti informuojamas iš anksto, kad duotą sutikimą gali bet kuriuo metu atšaukti, o taip pat nurodyti, kaip tai gali būti atlikta.

Taigi, visais atvejais, kai asmens duomenų tvarkymas buvo paremtas duomenų subjekto sutikimu, duomenų valdytojas turi suteikti galimybę duomenų subjektui tą sutikimą atšaukti. Tai yra absoliuti ir nepaneigiama duomenų subjekto teisė.

Praktikoje pasitaiko klausimų, kaip turi būti realizuojama duomenų subjekto teisė atsisakyti pranešimų arba atšaukti duotą sutikimą. EDAV Gairėse Nr. 05/2020 „Dėl sutikimo pagal Reglamentą 2016/679“ (toliau EDAV Gairės dėl sutikimo pagal Reglamentą) yra nurodžiusi, kad tais atvejais, kai sutikimas gaunamas elektroninėmis priemonėmis tik vienu pelės paspaudimu, ekrano perbraukimu telefone, klavišo paspaudimu arba per duomenų subjekto naudojamą vartotojo sąsają, duomenų subjektams turi būti sudaryta galimybė sutikimą atšaukti tokiu pačiu lengvu būdu. Be to, duomenų subjektas turi turėti galimybę atšaukti savo sutikimą be žalos ar kitų neigiamų padarinių. Tai, *inter alia*, reiškia, kad duomenų valdytojas privalo sutikimą atšaukti nemokamai, nedarant poveikio paslaugų teikimui.

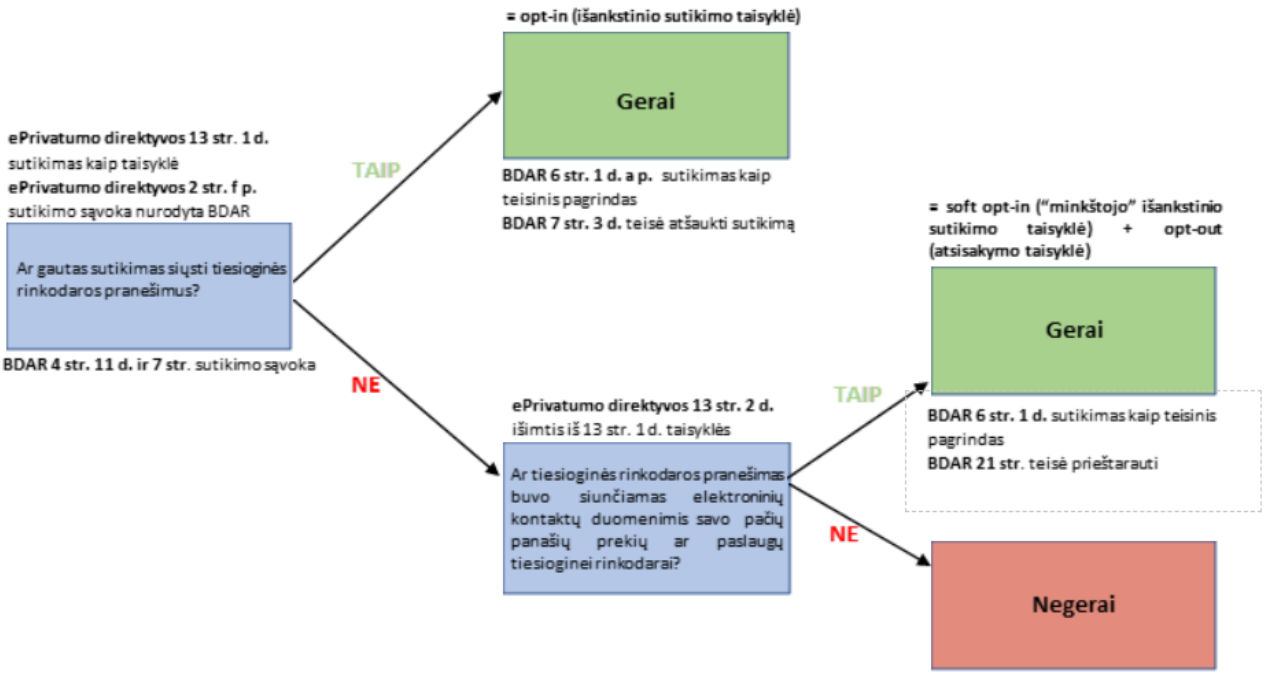
Lengvas sutikimo atšaukimas BDAR yra apibūdinamas, kaip būtinas „sutikimo“, kaip asmens duomenų tvarkymo pagrindo, kriterijus. Jei sutikimo atšaukimas neatitinka BDAR reikalavimų, laikoma, kad sutikimas nebuvo gautas pagal BDAR reikalavimus. Duomenų valdytojas pranešime dėl sutikimo gavimo turi nurodyti duomenų subjektui jo teisę bet kada atšaukti savo duotą sutikimą.

Duomenų valdytojas, gavęs sutikimo atšaukimą, turi nedelsiant nutraukti duomenų tvarkymą remiantis sutikimu, o taip pat ištrinti tokius asmens duomenis darant prielaidą, kad nėra jokio kito tikslo, pateisinančio tolimesnį asmens duomenų tvarkymą. Tais atvejais, kai duomenų subjektas atšaukia savo sutikimą, o duomenų valdytojas nori toliau tvarkyti asmens duomenis kitu teisėtu pagrindu, jis negali nutylėdamas pereiti nuo sutikimo, kaip duomenų tvarkymo pagrindo iki kito teisėto asmens duomenų tvarkymo pagrindo. Apie bet kokį teisėtą duomenų tvarkymo pagrindo pakeitimą turi būti pranešam duomenų subjektui pagal BDAR 13, 14 straipsnius.

Praktinis priežiūros institucijos paskirtos baudos pavyzdys:

2020 m. liepos 13 d. Italijos telekomunikacijų milžinei, įmonei „*Wind Tre S.p.A.*“[8]. Italijos Respublikos duomenų apsaugos priežiūros institucija įmonei skyrė 16 700 000 eurų dydžio baudą dėl neteisėto asmens duomenų tvarkymo tiesioginės rinkodaros tikslais. Atliekant tyrimą dėl įmonės veiklos, buvo išsiaiškinta, kad asmenims, gaunantiems reklaminio pobūdžio pranešimus, nebuvo suteikta teisė atsisakyti šių pranešimų, įmonė neturėjo įsidiegusi sistemos, vedančios asmenų, nepageidaujančių gauti reklaminio pobūdžio pranešimų sąrašą, o galiausiai – vartotojams buvo apribota galimybė naudotis „*Wind Tre S.p.A.*“ mobiliosiomis aplikacijomis „*My3*“ bei „*MyWind*“, kol vartotojai nesuteikė sutikimų dėl jų asmens duomenų tvarkymo tiesioginės rinkodaros tikslais, o tokį sutikimą pateikus, vartotojai savo sutikimą galėjo atšaukti tik praėjus 24 valandoms nuo šių sutikimų pateikimo.

Žemiau pateikiama schema, kaip vertinti tiesioginės rinkodaros pranešimų siuntimą, naudojantis aukščiau aptartais „opt-in“ ir „soft opt-in“ mechanizmais:



Apibendrinant galime teigti, kad įmonės, siekdamos vykdyti tiesioginę rinkodarą, turi atsižvelgti į šiuos pagrindinius aspektus:

[8] 2020 m. liepos 9 d. Italijos asmens duomenų apsaugos priežiūros sprendimas Nr. 9435753. [interaktyvus; žiūrėta 2022 m. gegužės 25 d.]. Prieiga per internetą: <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9435753>.

- Tiesioginė rinkodara gali būti vykdoma tik gavus duomenų subjekto sutikimą;
- Tiesioginė rinkodara gali būti vykdoma savo klientų atžvilgiu be papildomo sutikimo, jei tiesioginė rinkodara vykdoma klientų gautais elektroninių kontaktų duomenimis ir tik panašių ar tų pačių prekių ir paslaugų rinkodarai, jei klientas neprieštaravo dėl tokio duomenų naudojimo kai šie duomenys buvo renkami ir siunčiant kiekvieną žinutę;
- Duomenų subjektui turi būti sudaryta aiški, nemokama ir lengvai įgyvendinama galimybė nesutikti ir atšaukti duotą sutikimą;
- Gavus sutikimo atšaukimą, turi būti nedelsiant imamasi veiksmų nutraukti asmens duomenų, gautų sutikimo pagrindu, tvarkymą.

BDAR

BDAR tiesiogiai nereglamentuoja asmens duomenų tvarkymo tiesioginės rinkodaros tikslais, tačiau BDAR laikytinas universaliu teisės aktu, kurio nuostatos turi būti pritaikomos visoms su asmens duomenų tvarkymu susijusioms veikloms.

Kalbant apie BDAR ir E. Privatumo direktyvos santykį, tai pasakytina, kad E. Privatumo direktyva siekiama suderinti nacionalines nuostatas, būtinas siekiant užtikrinti vienodo lygio pagrindinių teisių ir laisvių, ypač teisės į privatumą ir konfidencialumą, apsaugą tvarkant asmens duomenis elektroninių ryšių sektoriuje, ir užtikrinti laisvą tokių duomenų bei laisvą elektroninių ryšių įrangos ir paslaugų judėjimą Europos Bendrijoje. Šiuo klausimu E. Privatumo direktyva išaiškina ir papildo BDAR nuostatas, kiek tai susiję su asmens duomenų tvarkymu elektroninių ryšių sektoriuje[9].

Kaip jau nurodyta aukščiau, BDAR nuostatos nagrinėjamai temai svarbios „sutikimo“ išaiškinimo aspektu.

Dėl asmens duomenų tvarkomų tiesioginės rinkodaros tikslais teisinio pagrindo

BDAR preambulės 47 punktas gali sudaryti klaidingą įspūdį, kad pagal BDAR asmens duomenų tvarkymas vykdant tiesioginę rinkodarą, gali būti vertinamas, kaip atliekamas teisėto intereso pagrindu, tačiau kaip jau nurodyta aukščiau, kalbant apie E. Privatumo direktyvą, elektronine forma vykdomiems reklamos pranešimams, kaip būtina sąlyga, yra duomenų subjekto sutikimas. Taigi, BDAR turi būti taikomas kartu su E. Privatumo direktyva bei ERĮ, kurie

9 https://edpb.europa.eu/sites/edpb/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_lt.pdf

aiškiai numato, kad asmens duomenų tvarkymo teisiniu pagrindu yra asmens sutikimas.

Šią poziciją taip pat patvirtina ir 2018 m. rugsėjo 16 d. Valstybinės duomenų apsaugos inspekcijos pateiktas patikrinimo apibendrinimas „Asmens duomenų tvarkymo tiesioginės rinkodaros ir lojalumo programos tikslais teisėtumo patikrinimų rezultatų apibendrinimas“. Apibendrinime nurodoma, kad dalis įmonių nepagrįstai rėmėsi BDAR 6 straipsnio 1 dalies f punktu[10]. Įmonės tvarkė asmens duomenis tiesioginės rinkodaros tikslais nurodant, kad tvarkymo teisėtumo sąlyga pritaikyti savo teikiamas paslaugas ar prekes, kiek įmanoma labiau klientų poreikiams bei efektyvinant įmonės verslą. Anot Valstybinės duomenų apsaugos inspekcijos: „*Teisėto intereso sąlyga negali būti taikoma, kadangi šiuo atveju duomenų subjektų (klientų, pirkėjų) interesai yra svarbesni negu duomenų valdytojo, o asmens duomenys profiliavimo tikslais galėtų būti tvarkomi tik su duomenų subjekto sutikimu*[11]“.

Tokių skirtingų teisinių pagrindu buvimas gali būti paaiškinamas tuo, kad tiesioginė rinkodara apima daugelį veiksmų, kaip antai duomenų rinkimas iš potencialių pirkėjų, atitinkamų pranešimų jiems siuntimas, potencialių pirkėjų profilių sudarymas, naršymo istorijos analizė ir t.t. Priklausomai nuo situacijos, sutikimas ir teisėtas interesas abu gali būti asmens duomenų, tvarkomų, vykdant tiesioginę rinkodarą, teisiniu pagrindu, tačiau tuo atveju, jei tiesioginė rinkodara vykdoma elektroninių ryšių pagalba, asmens duomenų tvarkymo teisiniu pagrindu yra sutikimas.

Sutikimo sąlygos

BDAR 4 straipsnio 11 punkte nurodyta, kad „*duomenų subjekto sutikimas – bet koks laisva valia duotas, konkretus ir nedviprasmiškas tinkamai informuoto duomenų subjekto valios išreiškimas pareiškimu arba vienareikšmiais veiksmais kuriais jis sutinka, kad būtų tvarkomi su juo susiję asmens duomenys*“.

[10] Duomenų tvarkymas yra teisėtas tik tuo atveju, jeigu taikoma bent viena iš šių sąlygų, ir tik tokiu mastu, kokiu ji yra taikoma: (f) tvarkyti duomenis būtina siekiant teisėtų duomenų valdytojo arba trečiosios šalies interesų, išskyrus atvejus, kai tokie duomenų subjekto interesai arba pagrindinės teisės ir laisvės, dėl kurių būtina užtikrinti asmens duomenų apsaugą, yra už juos viršesni, ypač kai duomenų subjektas yra vaikas.

[11] 2018 m. rugsėjo 26 d. Valstybinės duomenų inspekcijos asmens duomenų tvarkymo tiesioginės rinkodaros ir lojalumo programos tikslais teisėtumo patikrinimo rezultatų apibendrinimas. [interaktyvus; žiūrėta 2022 m. gegužės 25 d.]. Prieiga per https://vdai.lrv.lt/uploads/vdai/documents/files/Apibendrinimasdeltiesioginesrinkodarosirlojalumo20180926.pdf.

Toliau BDAR nedetalizuoja šiame apibrėžime nurodytų kriterijų, tačiau EDAV Gairėse Dėl sutikimo pagal Reglamentą detaliai išanalizuota „sutikimo“, kaip asmens duomenų teisinio pagrindo, elementai[12].

Gairėse Dėl sutikimo pagal Reglamentą nurodyta, kad sutikimas turi atitikti šiuos kriterijus:

- sutikimas turi būti duotas laisva valia;
- sutikimas turi būti konkretus;
- sutikimas turi būti informuotas;
- sutikimas kaip nedviprasmiškas duomenų subjekto valios išreiškimas pareiškimu arba vienareikšmiais veiksmais, kuriais jis sutinka, kad būtų tvarkomi su juo susiję asmens duomenys.

Žemiau atskirai detalizuojamas kiekvienas sutikimo kriterijus tiesioginės rinkodaros kontekste.

3.1.1 Duotas laisva valia

Kriterijus „laisva valia" reiškia duomenų subjekto galimybę pasirinkti duoti sutikimą ar neduoti. Tais atvejais, kai duomenų subjektas neturi realaus pasirinkimo, yra verčiamas arba žino, kad nedavus sutikimo jam atsiras neigiamos pasekmės, toks sutikimas nėra laikomas duotas laisva valia. Tai pat sutikimas nėra laikomas duotu laisva valia, kai sutikimas yra susiejamas su bendromis sutarties sąlygomis arba jei nurodoma, kad pasirašius sutartį, laikoma, kad duomenų subjektas davė sutikimą. Sutikimas laikomas duotu laisva valia tik tada, kai duomenų subjektui suteikiama reali galimybė jį atšaukti nepatiriant žalos.

EDAV savo Gairėse dėl sutikimo pagal Reglamentą yra nurodžiusi, kad kalbant apie šį sutikimo kriterijų, turi būti įvertintos papildomai ir šios aplinkybės: (i) padėties disbalansas; (ii) sąlygiškumas; (iii) detalumas; (iv) žala.

Padėties disbalansas reiškia, jog turi būti įvertinamas duomenų subjekto bei duomenų valdytojo padėties balansas, t. y. ar duomenų subjektas nėra tokioje padėtyje, kurioje jis negali neduoti sutikimo[13]. Tiesioginės rinkodaros kontekste tokios padėties disbalanso dažnu atveju nesutinkama, todėl detaliau šis kriterijus nebus aptarinėjamas šiame straipsnyje.

---

[12] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf

[13] BDAR preambulės 43 punktas nurodo, kad „*siekiant užtikrinti, kad sutikimas būtų duotas laisva valia, sutikimas neturėtų būti laikomas pagrįstu asmens duomenų tvarkymo teisiniu pagrindu konkrečiu atveju, kai yra aiškus duomenų subjekto ir duomenų valdytojo padėties disbalansas, ypač kai duomenų valdytojas yra valdžios institucija ir dėl to nėra tikėtina, kad sutikimas, atsižvelgiant į visas to konkretaus atvejo aplinkybes, buvo duotas laisva valia*"

Sąlygiškumas reiškia, jog turi būti įvertinta, ar duomenų valdytojas nėra sujungęs sutikimo dėl tiesioginės rinkodaros ir sutikimo dėl sutarties sąlygų ar kitų sąlygų, kaip vieno paketo[14]. Tokiais atvejais asmuo negali atskirti savo valios duoti sutikimą tiesioginės rinkodaros pranešimams ir valios sutarčiai sudaryti ar sutikimo dėl kitų aspektų.

Kaip kelis „sąlygiškumo" pavyzdžių yra pateikus EDAV Gairėse dėl sutikimo pagal Reglamentą:

> *Mobilioji programėlė, skirta redaguoti nuotraukas telefone, prašo vartotojų, kad šie norėdami naudotis šia programėle, turi suaktyvinti telefone GPS lokaciją ir suteikti prieigą prie šių duomenų. Programėlė nurodo, kad šie duomenys bus naudojami reklamos tikslais, tiriant vartotojo elgesį. Nei vietos lokacija, nei vartotojo elgesio analizė, nėra būtini, siekiant teikti nuotraukų redagavimo paslaugas. Taigi, jei vartotojas negali naudotis programėle, nesutikdamas su aukščiau nurodytu duomenų perdavimu, toks sutikimas negali būti laikomas duotu laisva valia.*

> *Bankas prašo klientų sutikimo leisti trečiosioms šalims naudoti mokėjimo informaciją tiesioginės rinkodaros tikslais. Šie asmens duomenų tvarkymo veiksmai nėra būtini vykdant sutartį su banku ir negali būti laikoma įprastinių banko paslaugų teikimu. Jei klientas atsisako duoti sutikimą šiam duomenų tvarkymo veiksmui, ir tai lemtų banko atsisakymą teikti paslaugas, sąskaitos uždarymą arba banko mokesčių padidėjimą, toks sutikimas nors ir duotas su galimybe jo neduoti, nebūtų laikomas duotas laisva valia.*

Detalumas reiškia, jog duomenų subjektai turi būti informuoti apie kiekvieną duomenų tvarkymo tikslą ir jei duomenų tvarkymo pagrindas yra sutikimas, turi turėti galimybę duoti sutikimą arba jo neduoti dėl kiekvienos konkrečios duomenų tvarkymo operacijos[15].

---

[14] BDAR 7 straipsnio 4 dalyje nurodyta, sąlyga „<...> *labiausiai atsižvelgiama į tai, ar, inter alia, sutarties vykdymui, įskaitant paslaugos teikimą, yra nustatyta sąlyga, kad turi būti duotas sutikimas tvarkyti asmens duomenis, kurie nėra būtini tai sutarčiai vykdyti*".

[15] BDAR preambulės 43 punkte nurodyta, kad „<...> *laikoma, kad sutikimas nebuvo duotas laisva valia, jeigu neleidžiama duoti atskiro sutikimo atskiroms asmens duomenų tvarkymo operacijoms, nors tai ir tikslinga atskirais atvejais, arba jeigu sutarties vykdymas, įskaitant paslaugos teikimą, priklauso nuo sutikimo, nepaisant to, kad toks sutikimas nėra būtinas tokiam vykdymui*".

BDAR preambulės 32 punkte nurodyta, kad „*Sutikimas turėtų apimti visą duomenų tvarkymo veiklą, vykdomą tuo pačiu tikslu ar tais pačiais tikslais. Kai duomenys tvarkomi ne vienu tikslu, sutikimas turėtų būti duotas dėl visų duomenų tvarkymo tikslų*".

BDAR 7 straipsnio 4 dalyje nurodyta, kad „*vertinant, ar sutikimas duotas laisva valia, labiausiai atsižvelgiama į tai, ar, inter alia, sutarties vykdymui, įskaitant paslaugos teikimą, yra nustatyta sąlyga, kad turi būti duotas sutikimas tvarkyti asmens duomenis, kurie nėra būtini tai sutarčiai vykdyti*".

EDAV Gairėse dėl sutikimo pagal Reglamentą nurodė tokį pavyzdį, kaip neatitinkantį detalumo sąlygos:

> *Toje pačioje sutikimo užklausoje mažmenininkas prašo savo klientų sutikimo naudoti jų asmens duomenis siųsti jiems rinkodarą elektroniniu paštu, taip pat dalytis šiais duomenimis su kitomis įmonėmis grupės viduje. Šis sutikimas nėra detalus, nes nėra atskirų sutikimų šiems dviem atskiriems tikslams, todėl toks duotas sutikimas negalios*.

Analizuojant galimą *žalą* duomenų subjektui, turi būti įvertintas draudimas duomenų valdytojui sutikimo davimo ar nedavimo nesieti su jokiomis neigiamomis pasekmėmis duomenų subjektui[16]. Neigiamos pasekmės gali pasireikšti tiek materialia, tiek nematerialia forma. Duomenų subjektas turi taip pat neapsunkinti duomenų subjektui atšaukti savo sutikimo. Duomenų valdytojui nustatyta pareiga įrodyti, kad sutikimo atšaukimas nesukelia duomenų subjektui jokių neigiamų pasekmių, išlaidų ar nesudaro jokių kliūčių toliau naudotis paslaugomis.

EDAV Gairėse dėl sutikimo pagal Reglamentą nurodė tokį *žalos* įvertinimo pavyzdį:

> D*uomenų subjektas prenumeruoja mados naujienlaiškį, kuris suteikia bendras nuolaidas. Verslo subjektas prašo duomenų subjekto sutikimo tvarkyti jo asmens duomenis apie apsipirkimo istoriją, patinkančias prekes, kad būtų galima pateikti suasmenintus pasiūlymus, pagrįstus apsipirkimo istorija arba savanoriškai užpildytu klausimynu. Gavus sutikimą, verslo subjektas suteikia personalizuotus pasiūlymus. Kai duomenų subjektas vėliau atšaukia tokį sutikimą, verslo subjektas neteikia personalizuotų pasiūlymų. Tai nėra vertinama, kaip žala, nes personalizuotos nuolaidos laikytinos leistina paskata.*

> *Praktinis priežiūros institucijos paskirtos baudos pavyzdys:*
>
> *2020 m. sausio 15 d. paskyrė Italijos Respublikos duomenų apsaugos priežiūros institucija, telekomunikacijos įmonei „Tim S.p.A.“ . Baudos dydis siekė net 27 800 000 eurų. Italijos Respublikos duomenų apsaugos priežiūros institucija laikotarpiu nuo 2017 m. pradžios iki 2019 m. pradžios gavo šimtus įvairių skundų bei pranešimų iš duomenų subjektų dėl įmonės „Tim S.p.A.“ vykdomų pastovių, itin dažnai pasikartojančių, reklaminio pobūdžio telefoninių skambučių dėl paslaugų teikimo, negavus duomenų subjektų sutikimo, ar duomenų subjektams pateikus aiškų nesutikimą.*

[16] BDAR preambulės 42 punkte nurodyta, kad „<...> *Sutikimas neturėtų būti laikomas duotas laisva valia, jei duomenų subjektas faktiškai neturi laisvo pasirinkimo ar negali atsisakyti sutikti arba sutikimo atšaukti, nepatirdamas žalos*“.

3.1.2. Konkretumas

Reikalavimu, kad sutikimas būtų „konkretus“ siekiama užtikrinti tam tikrą kontrolę ir skaidrumą duomenų subjekto atžvilgiu. Iš esmės šis reikalavimas apima šiuos aspektus[17]:

- *aiškus tikslas* - duomenų subjektas turi teisę žinoti apie visus duomenų tvarkymo tikslus, o taip pat reiškia, kad duodant sutikimą, sutikimas turi būti duodamas kiekvienam tikslui atskirai.
- *Prašymo dėl sutikimo gavimo detalumas* - kiekvienam tikslui turėtų būti pateiktas atskiras prašymas, kad duomenų subjektas galėtų duoti konkretų sutikimą dėl kiekvieno konkretaus tikslo;
- *Aiškus prašymo, susijusio su sutikimo gavimu, atskyrimas nuo kitos informacijos* – duomenų valdytojas, prašydamas iš duomenų subjekto sutikimo, turi prašymą dėl sutikimo atskirti nuo bet kokios kitos informacijos, o tais atvejais, kai prašoma sutikimo skirtingais tikslais, atriboti ir šių sutikimų gavimo būdus.

Praktinis priežiūros institucijos skirtos baudos pavyzdys:

2019 m. gruodžio 11 d. buvo paskirta 8 500 000 eurų bauda Italijos įmonei „*Eni Gas e Luce*“ dėl neteisėtų reklaminio pobūdžio pasiūlymų teikimo telefonu. Italijos duomenų apsaugos priežiūros institucija išsiaiškino, kad įmonė atlikinėjo šimtus reklaminių skambučių asmenims, nesuteikusiems atitinkamų sutikimų, o taip pat, buvo išsiaiškinta, kad įmonė nesiėmė jokių veiksmų dėl techninių bei organizacinių priemonių įdiegimo, kurios padėtų valdyti asmenų gautus ar negautus sutikimus dėl tiesioginės rinkodaros pranešimų ar skambučių. Galiausiai, tyrimo eigoje, buvo nustatyta, kad „*Eni Gas e Luce*“ be atitinkamų asmenų sutikimo, pirko šių asmenų duomenis, kuriais naudojosi atliekant reklaminius skambučius, o taip pat, buvo nustatyta, kad įmonė saugojo asmenų duomenis per ilgai.

3.1.3 Informuotas sutikimas

Informuotas sutikimas reiškia visos reikalingos informacijos suteikimą duomenų subjektui prieš šiam duodant sutikimą, užtikrinant duomenų subjektui galimybę priimti informacija pagrįstą sprendimą, suprasti, kokiam tikslui duodamas sutikimas ir leisti pasinaudoti savo teise atšaukti sutikimą.

[17] BDAR 6 straipsnio 1 dalies a) punkte nurodyta, kad „*duomenų tvarkymas yra teisėtas tik tuo atveju*, <...> *duomenų subjektas davė sutikimą, kad jo asmens duomenys būtų tvarkomi vienu ar keliais konkrečiais tikslais*“.

EDAV Gairėse dėl sutikimo pagal Reglamentą yra nurodžiusi, kokia minimali informacija turėtų būti pateikta duomenų subjektui prieš gaunant sutikimą. Tokią informaciją sudaro:

- duomenų valdytojo tapatybė;
- kiekvienos duomenų tvarkymo operacijos, dėl kurios prašoma sutikimo, tikslas;
- kokie (kokio tipo) asmens duomenys bus renkami ir naudojami;
- teisė atšaukti sutikimą;
- informacija apie asmens duomenų automatizuotu duomenų tvarkymu, įskaitant profiliavimą, grindžiamą sprendimą pagal BDAR 22 straipsnio 2 dalies c punktą;
- galimas asmens duomenų perdavimo į trečiąsias šalis pavojus, jeigu nepriimtas sprendimas dėl tinkamumo pagal 45 straipsnio 3 dalį arba nenustatytos tinkamos apsaugos priemonės pagal 46 straipsnį.

Tais atvejais, kai sutikimu tiesioginės rinkodaros tikslais, kaip asmens duomenų tvarkymo pagrindu remsis keli duomenų valdytojai, tai pranešime dėl sutikimo gavimo, turi būti išvardinti visi duomenų valdytojai.

Praktikoje kyla klausimų, ar būtina sutikime taip pat nurodyti duomenų tvarkytojus, tačiau informacija apie duomenų tvarkytojus dėl jų visai kitos padėties, nėra būtina. Kita vertus nereikia pamiršti apie BDAR 13, 14 straipsnius, kuriuose nurodyta, kokią informaciją duomenų valdytojas turi pateikti duomenų subjektui, įskaitant ir išsamų duomenų gavėjų ar jų kategorijų sąrašą, įskaitant ir duomenų tvarkytojus.

Aukščiau nurodyta informacija laikytina minimalia informacija, kuri turi būti pateikta duomenų subjektui prašant sutikimo, tačiau priklausomai nuo aplinkybių, duomenų valdytojas gali būti įpareigotas pateikti ir daugiau informacijos, kad duomenų subjektas galėtų priimti informacija pagrįstą sprendimą.

BDAR nenurodo konkrečios tokios informacijos pateikimo duomenų subjektui formos. Tai gali būti daroma raštu, pažymint tam tikrus langelius, naudojantis video priemonėmis, internetu ir t.t. Šiuo atveju prašymo dėl sutikimo gavimo pateikimo forma priklauso išimtinai nuo duomenų valdytojo valios. E. Privatumo direktyvos preambulės 17 punktas nurodo, kad „*sutikimas gali būti duotas bet kuriuo tinkamu būdu, specialiu ir pakankamai informatyviu, leidžiančiu naudotojui laisvai išreikšti savo valią, įskaitant ir atitinkamame interneto tinklavietės langelyje dedamą varnelę*“.

Tačiau BDAR nustato konkrečius reikalavimo turinius, kaip tokia informacija turi būti pateikta: „*suprantama ir lengvai prieinama forma, aiškia ir paprasta kalba*“. Tai pirmiausia reiškia, kad pranešimas turi būti suprantamas paprastam

žmogui, ne tik teisininkui, o taip pat tai reiškia, kad pranešimas turi būti suformuluotas atsižvelgiant į auditoriją, kuriai jis yra skiriamas (pavyzdžiui tais atvejais, jei yra pranešimas skiriamas vaikams, tai gali reikti pateikti ir vizualizaciją). Duomenų valdytojai negali teikti ilgų, nesuprantamų arba dviprasmiškų formuluočių, kurios neleidžia duomenų subjektui suprasti kas yra duomenų valdytojas ir kam jis duoda sutikimą.

Praktikoje dažnai kyla klausimas, ar pranešime dėl sutikimo turi būti pateikta visa BDAR 13, 14 straipsniuose nurodyta informacija. 29 straipsnio darbo grupės nuomone, pranešime dėl sutikimo gavimo nebūtina pateikti visos informacijos pagal BDAR 13, 14 straipsnius, tačiau tai nepaneigia duomenų valdytojo šiuose straipsniuose nurodytos pareigos. Ši informacija turi būti pateikta atskirame dokumente, kaip pavyzdžiui privatumo pranešime ar privatumo politikoje.

Praktinis priežiūros institucijos skirtos baudos pavyzdys:

2020 m. birželio 30 d. Vokietijoje vienai iš valstybės didžiausių gyvybės draudimo kompanijų „*AOK Baden-Württemberg*“ skyrė 1 240 000 eurų baudą. Draudimo įmonė nuo 2015 iki 2019 metų organizavo įvairaus pobūdžio loterijas ir tuo pačiu rinko dalyvių asmens duomenis, įskaitant jų kontaktinius duomenis ir duomenis apie tokio asmens priklausymą/narystę sveikatos draudimo įstaigose. „*AOK Baden-Württemberg*“, siekdama siųsti reklaminius pranešimus, pasinaudojo loterijų dalyvių asmens duomenimis. Tokios reklamos sklaidai „*AOK Baden-Württemberg“* pasitelkė technines priemones, o dėl jų nepakankamo saugumo ir tinkamumo reklama buvo išsiųsta ir tiems asmenims, kurie nedavė sutikimo dėl tokių reklaminio pobūdžio pranešimų gavimo. Daugiau nei 500 loterijų dalyvių asmens duomenys buvo naudojami be jų sutikimo reklamos tikslais.

3.1.4. Nedviprasmiškas duomenų subjekto valios išreiškimas[18]

BDAR numato, kad sutikimas turi būti duodamas aiškiai išreiškiant savo valią, pateikiant aiškų pareiškimą arba vienareikšmiais veiksmais. Tai reiškia, kad sutikimui reikalingas aktyvus valios pareiškimas ir sutikimu negali būti laikomas neveikimas.

[18] BDAR preambulės 32 punkte nurodyta, kad „sutikimas turėtų būti duodamas aiškiu aktu patvirtinant, kad yra suteiktas laisva valia, konkretus, informacija pagrįstas ir vienareikšmis nurodymas, kad duomenų subjektas sutinka, kad būtų tvarkomi su juo susiję asmens duomenys, pavyzdžiui raštiškas, įskaitant elektroninėmis priemonėmis,, arba žodinis pareiškimas. Tai galėtų būti atliekama pažymint langelį interneto svetainėje, pasirenkant informacinės visuomenės paslaugų techninius parametrus arba kitu pareiškimu arba poelgiu, iš kurio aiškiai matyti tame kontekste, kad duomenų subjektas sutinka su siūlomu jo asmens duomenų tvarkymu. Todėl tyla, iš anksto pažymėti langeliai arba neveikimas neturėtų būti laikomi sutikimu“

Sutikimo negalima gauti taip pat tuo pačiu veiksmu, kaip susitariant dėl sutarties pasirašymo ar sutinkant su bendromis sutarties sąlygomis. Toks veiksmas neatitiks duomenų subjekto valios išraiškos formos, nes duomenų subjektas bus priverstas duoti sutikimą dėl dviejų klausimų, kurie nėra atskirti.

Rašytinė sutikimo forma dažniausia nesukelia jokių problemų, tačiau šiuolaikinių technologijų pasaulyje tai retai naudojamas būdas. BDAR preambulės 32 punkte nurodyta, kad sutikimas gali būti gaunamas elektroninėmis priemonėmis, pasirenkant informacinės visuomenės paslaugų techninius sprendimus. Taigi, duomenų valdytojui yra leidžiama naudotis ir informacinių technologijų sprendimais. Šiuo atveju būtina atkreipti dėmesį, kad jei toks sutikimas gaunamas tokiu būdu, tai duomenų subjektas turi suprasti kokį veiksmą jis turi atlikti, duoti sutikimą arba jo neduoti, o duomenų valdytojas turi įgyvendinti priemones, kurios leistų vėliau įrodyti, kad duomenų subjektas tą sutikimą davė.

EDAV gairėse dėl sutikimo pagal Reglamentą nurodė, kad juostos perbraukimas telefono ekrane, mojavimas prieš telefono kamerą, išmaniojo telefono pasukimas pagal laikrodžio rodyklę gali būti veiksmai, kuriais duomenų valdytojas duoda sutikimą, jei tik aiškiai pateikiama informacija, kad konkretus veiksmas yra sutikimas su konkrečiu pasiūlymu (*pavyzdžiui jei perbraukiate šią juostą į kairę, sutinkate, kad informacija X būtų naudojama Y tikslui. Pakartokite judesį, kad patvirtintumėte*). Duomenų valdytojas turi sugebėti įrodyti, kad sutikimas buvo gautas tokiu būdu, o duomenų subjektai turi turėti galimybę atšaukti sutikimą taip pat lengvai, kaip jis buvo duotas.

EDAV, kaip netinkamus sutikimo gavimo formas, nurodo šiuos atvejus:

- tyla arba neveikimas;
- iš anksto pažymėti langeliai;
- pareiškimas, kad toliau naršant yra duodamas sutikimas.

29 straipsnio darbo grupė savo nuomonėje dėl neužsakytų pranešimų tiesioginės rinkodaros tikslais pagal Direktyvos 2002/58/EC 13 straipsnį [19] yra nurodžiusi šiuos pagrindinius blogos praktikos pavyzdžius:

- kai klausiama gavėjų sutikimo dėl rinkodaros elektroninių laiškų gavimo bendru elektroniniu laišku, nenurodant konkrečiai nei kokiu būdu būtų siunčiami pranešimai ir kokiais tikslais naudojami. Toks užklausimas ir sutikimo gavimas neatitinka E. Privatumo direktyvos reikalavimų, kad sutikimas turi būti gautas teisėtai, laisvai, ir būtų aiškus ir konkretus;
- sutikimas duodamas kartu su bendromis sutarties sąlygomis, laikomas netinkamai duotu pvz., abonentinė sutartis, kurioje taip pat prašoma sutikimo siųsti pranešimus tiesioginės rinkodaros tikslais);

[19] Opinion 5/2004 on unsolicited communications for marketing purposes under Article 13 of Directive 2002/58/EC

- iš anksto pažymėti langeliai interneto svetainėse taip pat laikomi netinkamai duotais sutikimais;
- numanomas sutikimas, t. y. sutikimas laikomas duotu, kol nebus pareikštas prieštaravimas, taip pat nėra laikomas sutikimu.

Praktinis priežiūros institucijos skirtos baudos pavyzdys:

2020 m. liepos 13 d. Italijos duomenų apsaugos priežiūros institucija skyrė nuobaudą dar vienai Italijos telekomunikacijų įmonei „*Iliad Italia S.p.A*“ dėl BDAR 5 ir 25 straipsnių pažeidimų, kurie kilo, kai iš įmonės klientų, kurie aktyvavo naujas SIM korteles buvo neteisėtai renkami jų asmens duomenys įvairiais tikslais, įskaitant ir tiesioginės rinkodaros tikslus[20]. Visgi, įmonės klientams, aktyvuojant SIM kortelę, nebuvo suteikiama galimybė sutikti ar nesutikti su jų asmens duomenų tvarkymu tiesioginės rinkodaros tikslais, dėl to įmonei „*Iliad Italia S.p.A*“ buvo skirta 800 000 EUR dydžio bauda.

Duomenų subjekto teisės

Jei asmens duomenų tvarkymo veikla yra grindžiama duomenų subjektų sutikimu, tai toks asmens duomenų tvarkymo pagrindas neabejotinai paveiks duomenų subjektų teisių įgyvendinimą.

Tokiais atvejais duomenų subjektai turi teisę į asmens duomenų perkeliamumą (BDAR 20 straipsnis).

EDAV Gairėse dėl sutikimo pagal Reglamentą nurodė, kad teisė nesutikti, kad būtų tvarkomi asmens duomenis (BDAR 21 straipsnis) iš esmės yra labai susijusi su duomenų subjekto teise atšaukti savo sutikimą. Duomenų subjektas turi teisę dėl su jo konkrečiu atveju susijusių priežasčių bet kuriuo metu nesutikti, kad su juo susiję asmens duomenys būtų tvarkomi. Duomenų valdytojas nustoja tvarkyti duomenis, išskyrus atvejus, kai įrodo, kad duomenų tvarkymas yra viršesnis už duomenų subjekto interesus, teises ir laisves, arba siekiant pareikšti, vykdyti ar apginti teisinius reikalavimus[17].

Duomenų subjektai turi taip pat kitas BDAR 16-20 straipsniuose nurodytas duomenų subjektų teises, kaip pvz.: teisė ištrinti, apriboti asmens duomenų tvarkymą, ištaisyti asmens duomenis ir pan.

Kitų Europos Bendrijos šalių specifika

[20] 2020 m. liepos 13 d. Italijos asmens duomenų apsaugos priežiūros sprendimas Nr. 9435807. [interaktyvus; žiūrėta 2022 m. gegužės 25 d.]. Prieiga per internetą: <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9435807>.

Aukščiau nurodytos BDAR ir E. Privatumo nuostatos taikomos ir kitose Europos Bendrijos šalyse, tačiau dalis valstybių pasirinko ir papildomas priemones, kurias saugo duomenų subjekto teises nuo nepageidaujamų tiesioginės rinkodaros pranešimų.

Kai kuriose Europos Sąjungos valstybėse - narėse duomenų subjektų (o kartais ir juridinių asmenų) teisė negauti tiesioginės rinkodaros pranešimų be aukščiau straipsnyje nurodytų priemonių, yra ginama ir taip vadinamais „opt-out“ sąrašais, t.y. sąrašais, į kuriuos asmenys gali įtraukti savo kontaktinius duomenis, jei jie nenori gauti tiesioginės rinkodaros pranešimų (dar kitaip vadinami „Robinzono sąrašais“). Žemiau pateikiami keli tokią praktiką iliustruojantys pavyzdžiai.

Austrijoje tokį „opt-out“ elektroninio pašto adresų sąrašą administruoja Rundfunk und Telekom regulierungs-Gmbh (toliau Austrijos radijo ir telekomunikacijų reguliavimo tarnyba)[21], kuri savo puslapyje viešai skelbia įtraukimo ir išbraukimo iš tokio sąrašo prašymus ir sąlygas[22]. Austrijos E-Komercijos įstatymo 7 str.[23] nurodyta, kad Austrijos radijo ir telekomunikacijų reguliavimo tarnyba tvarko sąrašą, į kurį gali būti nemokamai įrašytas bet kuris fizinis ar juridinis asmuo, kuris nepageidauja elektroniniu paštu gauti tiesioginės rinkodaros pranešimų. Įmonės, siekdamos siųsti tokio pobūdžio pranešimus turi įsitikinti, ar konkretus elektroninio pašto adresas nėra įtrauktas į tokį sąrašą. Papildomai Austrijos radijo ir telekomunikacijų reguliavimo tarnyba numato galimybę ne tik įtraukti konkrečius elektroninio pašto adresus, bet ir visus domenus (kaip pavyzdžiui forma: domain.com), kad tokiu atveju leidžia išvengti tiesioginės rinkodaros pranešimu visiems elektroninio pašto gavėjams, kurie naudoja tokį domeną.

Toks pats „opt-out“ sąrašas, ar kitaip „Robinzono sąrašas“ yra naudojamas ir Vokietijoje[24]. Šis sąrašas yra administruojamas vartotojų teisių apsauga internete ir socialiniame gyvenime užsiimančios I.D.I. Verband organizacijos. Į šį sąrašą gali būti įtraukti telefono numeris (įskaitant mobilųjį), elektroninio pašto adresas, adresas ar fakso numeris. Registruotis gali ne tik fiziniai asmenys, bet taip pat individualią veiklą vykdantys asmenys, smulkiajam verslui priskiriamos įmonės bei laisvos profesijos atstovai. Šis sąrašas veikia taip, kad įmonės siekdamos siųsti tiesioginės rinkodaros pranešimą gali savo kontaktus patikrinti šiam sąraše ir gauti atsakymą, ar tokie kontaktiniai duomenys yra tame sąraše. Įmonės neturi prieigos prie viso „Robinzono sąrašo“, todėl negali juo pasinaudoti tikslu papildyti savo kontaktų bazę.

[21] https://www.rtr.at/
[22] https://www.rtr.at/de/tk/TKKS_ECGEintrag
[23] https://www.ris.bka.gv.at/Dokumente/Erv/ERV_2001_1_152/ERV_2001_1_152.pdf
[24] https://www.robinsonliste.de/

Praktinė problema yra ta, kad tikrinimas „Robinzono sąraše“ Vokietijoje nėra privalomas pagal teisės aktus, todėl iš esmės tai priklauso nuo pačių įmonių kultūros ir vykdomos tiesioginės rinkodaros strategijos.

Nepaisant „Robinzono sąrašo“ neprivalomumo, Vokietijoje jau yra susiformavusi teismų praktika dėl tiesioginės rinkodaros siunčiamos paprastu paštu į pašto dėžutes. Jau nuo 1988 m. teismo sprendimu byloje Nr. AZ VI ZR 182/88 buvo nuspręsta, kad tais atvejais, kai ant pašto dėžučių yra užklijuotas lipdukas „Prašome neteikti jokios reklamos“, tai toks nurodymas reklamos davėjui yra privalomas. Šiuo atveju buvo padaryta tik viena išimtis, kad tais atvejais, kai reklama yra personalizuota ir skirta konkrečiam asmeniui, toks nurodymas ant pašto dėžučių nėra privalomas. Taigi, įspėjančiais lipdukais pažymėtos pašto dėžutės apsaugoja jų šeimininkus tik nuo nepersonalizuotos reklamos, reklaminių skrajučių, nemokamų leidinių ir pan.

Danijoje bei Ispanijoje taip pat taikoma labai panaši praktika. Danijos Rinkodaros Praktikos[25] įstatymo 10 str. 4 d. 2 p. nurodyta, jog įmonės negali siųsti tiesioginės rinkodaros pranešimų asmeniui, jeigu asmuo savo kontaktus yra įtraukęs į „Robinzono sąrašą“. Ispanijos Asmens duomenų apsaugos ir skaitmeninių teisių garantijų įstatymo 23 str.[26] nurodyta, kad gali būti sukurtas sąrašas, į kurį bus įtraukiami kontaktiniai asmenų duomenys, kuriais įmonės negali siųsti tiesioginės rinkodaros pranešimų.

Italija šį klausimą sureguliavo Italijos privatumo kodekse[27], kurio 130 straipsnyje nurodyta, kad atitinkama valstybės institucija yra įpareigota sukurti taip vadinamą ”opt-out” registrą. Tuo tikslu buvo išleistas 2010 m. rugsėjo 7 d. dekretas Nr. 178 dėl viešojo registro sudarymo, į kurį būtų įtraukiami telefono numeriai, kurių turėtojai (savininkai) nepageidauja gauti komercinių pasiūlymų ir reklaminių pranešimų[28]. Šiais teisės aktais buvo apibrėžtos kelios svarbios taisyklės:

- kiekvienas duomenų subjektas turi galimybę savo stacionarų ar mobilųjį telefono numerį įtraukti į „opt-out“ kontaktinių duomenų registrą;
- bet kuris duomenų subjekto duotas sutikimas tiesioginei rinkodarai iki įtraukimo į „opt-out“ sąrašą, laikomas atšauktu nuo to momento, kai asmuo įtraukia savo kontaktus į nurodytą sąrašą;
- kiekvienas subjektas, siekiantis siųsti tiesioginės rinkodaros pranešimus, privalo pateikti prašymą dėl prieigos prie minėto sąrašo suteikimo. Gavęs prieigą jam numatoma pareiga tikrinti kontaktinius

[25] https://www.kfst.dk/media/49887/mfl-english.pdf
[26] https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf
[27] b1787d6b-6bce-07da-a38f-3742e3888c1d (garanteprivacy.it)
[28] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1788873?fbclid=IwAR0NjBAMuNyQpn869EwLUjAr3-iyEiDoHz6TnGl-ALBvwyVYk-HSH2SojCU

duomenis, ar jie nėra įtraukti į nepageidaujamų gauti tiesioginius pranešimus sąrašą;
- duomenų subjektas gali bet kuriuo metu atšaukti savo registraciją nurodytame sąraše;
- buvimas šiame „opt-out“ sąraše nedaro įtakos tiems atvejams, kai tiesioginė rinkodara siunčiama gavus atskirą duomenų subjekto sutikimą.

Apibendrinant galima teigti, jog „opt-out“ sąrašai kol kas yra retenybė Europos Sąjungoje, tačiau, įvertinus tai, kad asmens duomenų apsauga atsižvelgiant į technologijų pažangą ir darosi vis aktualesnė, tai tokios iniciatyvos turėtų tapti įprasta praktika visose valstybėse ir būtų užtikrintas tokio sąrašo privalomumas.

Išvados

1. Asmens duomenų tvarkymas, susijęs su tiesiogine rinkodara, yra reglamentuotas arba išplaukia iš BDAR ir E. Privatumo direktyvos, o nacionaliniu mastu – ADTAĮ ir ERĮ.

2. Teisės aktai numato, kad vykdant tiesioginę rinkodarą, būtina gauti duomenų subjekto sutikimą. Sutikimas turi atitikti šiuos reikalavimus: (i) sutikimas turi būti duotas laisva valia; (ii) sutikimas turi būti konkretus; (iii) sutikimas turi būti informuotas; (iv) sutikimas kaip nedviprasmiškas duomenų subjekto valios išreiškimas pareiškimu arba vienareikšmiais veiksmais, kuriais jis sutinka, kad būtų tvarkomi su juo susiję asmens duomenys.

3. ERĮ nustato išimtį *elektroninių kontaktinių duomenų* naudojimui – asmuo, kuris teikdamas paslaugas ar parduodamas prekes ADTAĮ ir BDAR nustatyta tvarka ir sąlygomis gauna iš savo klientų elektroninius o kontaktinius duomenis, gali naudoti šiuos kontaktinius duomenis savo paties panašių prekių ar paslaugų rinkodarai, jei klientams yra suteikiama aiški, nemokama ir lengvai įgyvendinama galimybė nesutikti arba atsisakyti tokio kontaktinių duomenų naudojimo pirmiau nurodytais tikslais, kai šie duomenys yra renkami ir, jei klientas iš pradžių neprieštaravo dėl tokio duomenų naudojimo, siunčiant kiekvieną žinutę.

4. Sutikimas turi būti gaunamas atskirai dėl kiekvieno tikslo ir dėl kiekvieno konkrečiai naudojamo tiesioginės rinkodaros siuntimo būdo. Sutikimas gali būti gaunamas tiek rašytiniu būdu, tiek elektroninių priemonių pagalba. Duomenų valdytojų atskaitomybės principas reikalauja, kad duomenų valdytojai esant ginčui galėtų pateikti įrodymus, kurie patvirtintų, kad sutikimas buvo gautas tinkamai.

5. Duomenų subjekto sutikimas kartu ir reiškia neatšaukiamą ir absoliučią duomenų subjekto teisę bet kuriuo metu atšaukti savo sutikimą, nesukuriant jokių neigiamų pasekmių duomenų subjektui. Ši teisė negali būti paneigiama ir duomenų subjektas negali atsisakyti šios savo teisės.

6. Dalis Europos Sąjungos valstybių yra pasirinkusios taikyti taip vadinamus „opt-out“ sąrašus. Duomenų subjektai priklausomai nuo valstybės į tokius sąrašus gali įtraukti savo kontaktinius duomenis, kuriais nepageidauja gauti tiesioginės rinkodaros pranešimų. Tokie sąrašai papildomai apsaugo duomenų subjektus nuo nepageidaujamų reklamos pranešimų.

7. Europos Sąjungos priežiūros institucijų praktika rodo, kad baudos už pažeidimus, susijusius su duomenų tvarkymu tiesioginės rinkodaros tikslu, yra pakankamai didelės, kas iš esmės reiškia, kad tokio pobūdžio pažeidimai laikytinai labai sunkiais ir apribojančiais duomenų subjektų teises.

DUOMENŲ NUASMENINIMAS: TAKTIKOS PARINKIMAS BEI RIZIKŲ ĮVERTINIMAS

Martynas Bieliūnas
Privacy Partners Vykdantysis partneris, CIPP/E, CIPM, ISO/IEC 27001 Lead Auditor

Straipsnyje panaudota medžiaga remiantis UAB "Exacaster", Imlitex įmonių grupės, darbo grupės "United 4 Health" bei Google renkamų ir teikiamų duomenų nuasmeninimo modeliais. Autorius dėkoja minimoms organizacijoms už suteiktą informaciją bei įžvalgas kilusiais dirbant su šių organizacijų duomenimis.

Turint prieigą prie didelio duomenų rinkinių skaičiaus bei plačias analizės galimybes anonimiškumas tampa praktiškai neįmanomu.

Įvadas

Duomenų nuasmeninimas yra svarbus asmens duomenų apsaugos aspektas mokslo, verslo ar valstybės veikloje. Kinta duomenų naudojimo pobūdis: jei anksčiau duomenys dažniausiai būdavo naudojami vienoje sistemoje ar procese, skaitmeninės technologijos ir atvirieji duomenys ("*Open data*") atveria valstybės bei įmonių turimus duomenis antriniam panaudojimui, jų susiejimui ir apjungimui. Naudojami analizės metodai taip pat sudėtingėja, taikant automatizuotus ar dirbtiniu intelektu pagrįstus metodus metodus. Viešai pateikiant nuasmenintus atvirųjų duomenų išteklius net nėra žinoma ar ribojama kam šie duomenys bus naudojami. Tai kelia klausimus apie privatumo užtikrinimą - turint neribotus duomenų kiekius bei neribotas analizės galimybes, efektyvus nuasmeninimas tampa neįvykdomu uždaviniu. Sprendimai grindžiami duomenų analitika dideliuose struktūruotų ir nestruktūruotų duomenų masyvuose ("*Data lakes*"), taikant sudėtingus analitinius algoritmus, tame tarpe ir dirbtinio intelekto sprendimus gali efektyviai nustatyti įvairias sąsajas bei dėsningumus naudojant duomenis kurie iš pirmo žvilgsnio yra tinkamai nuasmeninti. Todėl ypač svarbu pasirinkti tinkamus duomenų nuasmeninimo metodus, siekiant išvengti privatumo pažeidimų dėl neplanuoto asmens duomenų atskleidimo ar netgi perteklinio duomenų saugojimo kai atsiranda nenumatytos sąsajos. Šiame procese svarbu tiek bendroji nuasmeninimo taktika (matematiniai modeliai ir procesai) tiek techninė realizacija. Prieiga prie duomenų analizės techninių pajėgumų debesų kompiuterijoje ("*Cloud computing*") yra ribojama tik kainos, kuri turi tendenciją mažėti. Tai leidžia nesudėtingai apjungti įvairius atvirame internete ir vidinėse organizacijų duomenų bazės esančius duomenų rinkinius. To pasėkoje galimi patys įvairiausi re-identifikacijos scenarijai, kai dėl kokių nors priežasčių siekiama iš antrinių duomenų kombinacijų atstatyti konkretų asmenį. Net tais atvejais kai asmuo negali būti atstatomas visiškai tiksliai (su 100% tikimybe, arba P=1), galimas papildomų viešai prieinamų iš interneto duomenų panaudojimas siekiant patikslinti ir galutinai susieti konkretų asmenį su duomenų rinkiniu. Duomenų valdytojams tai kelia papildomas rizikas, pavyzdžiui iš duomenų tvarkytojo pateiktų viešai prieinamų nuasmenintų duomenų atstačius konkretų asmenį galima situacija kai duomenų valdytojas būtų pripažintas kaltu dėl nepakankamo asmens duomenų saugojimo ir netinkamo techninių priemonių parinkimo. Bendrasis Duomenų Apsaugos Reglamentas (26 konstatuojamosios dalies punktas) teigia, jog nuasmeninti duomenys nėra laikomi asmens duomenimis, taip sukuriant aiškią takoskyrą - jei iš duomenų neįmanomas konkretaus asmens atstatymas, nėra keliami reikalavimai jų saugumui ir privatumui taip kaip asmens duomenims. Kita vertus, tokių nuasmenintų duomenų teikėjai kai kuriais atvejais net ir negali žinoti, jog jų teikiami duomenys vėl tapo asmens duomenimis, nes atsirado

pvz. naujas re-identifikacijos algoritmas ar papildomi viešai pateikiami duomenys kurie apjungti su nuasmenintais duomenimis nurodo konkrečius asmenis.
Dažna klaida – pseudonimizuotų duomenų laikymas nuasmenintais duomenimis. Tai, kad konkrečiam įrašui suteikiamas identifikatorius jokiu būdų nepadaro duomenų nuasmenintais.

Tinkamas duomenų nuasmeninimas yra sudėtingas matematinis uždavinys. Duomenų rinkinių struktūra ir sandara dažnai nėra išanalizuojama pakankamai išsamiai, to pasėkoje nuasmeninimas nėra atliekamas kokybiškai. Dažnai neatsižvelgiama į kuriuos nors nuasmeninimo aspektus (pvz. duomenų tankio intervaluose, reikšmių unikalumo, atvirųjų duomenų šaltinių kurie gali būti susiejami, socialinių tinklų pateikiamą informaciją ir pan.). Taip paliekama galimybė re-identifikacijai (sąryšio su konkrečiu asmeniu atstatymui). Šiame straipsnyje apžvelgsime kaip reiktų valdyti duomenų nuasmeninimą, įvertinti nuasmeninimo patikimumą, apžvelgiant tiek proceso modelius, tiek ir kai kuriuos praktinius pavyzdžius. Pateikiama instrukcija, kaip nuasmeninimą reiktų atlikti pažingsniui įvertinant pagrindines rizikas ir atsižvelgiant į konkretaus duomenų rinkinio specifiką. Straipsnis skirtas Duomenų Apsaugos Pareigūnams (DAP), todėl siekiama apžvelgti pagrindines sąvokas ir metodus tinkamus greitam praktiniam pritaikymui. Detalūs matematiniai modeliai ir kai kurių sąvokų išaiškinimai nepateikiami, juos nesudėtinga rasti pagal pateikiamas nuorodas.

Teisiniai sprendimai susiję su netinkamu nuasmeninimu arba jo neatlikimu

Šiame straipsnyje nesiekiama pateikti detalią juridinių precedentų analizę, o daugiau pademonstruoti jog nuasmeninimas jau tampa tema teismų praktikoje (dažnai nuasmeninimas pateikiamas kaip (arba kartu su) organizacinių bei techninių saugumo priemonių nepakankamumu. Sprendimai rodo jog už netinkamą nuasmeninimą taikomos santykinai griežtos sankcijos.

Europa:
Danijos duomenų apsaugos inspekcijos paskirta 160 tūkst EUR bauda (angliškas aprašymas European Data Protection Board saite)[29]- nepaisant to jog taksi keleivių vardai buvo ištrinami po dviejų metų, o likusi informacija paliekama vėlesniam naudojimui, buvo nustatyta jog nuasmeninimas buvo neadekvatus ir nepakankamas.

[29] Danija: https://edpb.europa.eu/news/national-news/2019/danish-data-protection-agency-proposes-dkk-12-million-fine-danish-taxi_en

Italijos duomenų apsaugos inspekcija skyrė 50 tūkst. EUR baudą[30] už nepakankamas saugumo technines ir organizacines priemones, o konkrečiai - neatliktą e-balsavimo duomenų nuasmeninimą.

Austrija: 2018 metais pateiktas išaiškinimas[31] jog duomenų nuasmeninimas yra tolygus jų ištrynimui yra ginčytinas ir rizikingas, turint omenyje jog ne visos organizacijos sugeba kokybiškai nuasmeninti duomenis. Taip pat internete atsirandantys nauji duomenys ar jų rinkiniai gali sukurti situaciją kai anksčiau nuasmenintiems duomenims atsiranda papildomi kvaziidentifikatoriai[32] leidžiantys re-identifikuoti duomenis.

JAV:

Čikagos universitetas dalinosi duomenimis su Google[33] siekiant užtikrinti geresnio lygio medicininių duomenų analizę. Nuasmeninimo priemonės buvo pripažintos nepakankamomis.

Lietuva:

Ši tema paliesta E.Gruodytės ir M.Milčiuvienės straipsnyje apie nuasmeninimą teismų sprendimuose [34] - nuasmeninimas kai tai reikalaujama įstatymo yra kritiškai svarbus asmens reputacijai, ir nagrinėjant praktines situacijas pasitaiko netinkamo nuasmeninimo pavyzdžių. Pastarojo meto pavyzdžiai kai rezonansinėse politinėse bylose publikuojant medžiagą formalus nuasmeninimas visiškai netinka (t.y. visiškai paprasta nutuokti apie kokius asmenis, partijas eina kalba) parodo nuasmeninimo sudėtingumą tokiose situacijose.

Naudotinos metodikos ir naujos tendencijos

VDAI dar 2015 m. pateikė rekomendacijas kurios pakankamai detaliai apžvelgia nuasmeninimo matematinius modelius ir metodikas [35]: (šis

[30] Italija: https://gdpr.eu/italy-gdpr-fine/
[31] Austrija – išaiškinimas: https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20181205_DSB_D123_270_0009_DSB_2018_00/DSBT_20181205_DSB_D123_270_0009_DSB_2018_00.html
[32] Kvaziidentifikatorius – duomuo ar kintamasis kuris nėra unikalus, bet konkrečiu atveju ar derinant su kitais kintamaisiais gali tapti unikaliu (pvz. gatvėje X gali gyventi tik vienas asmuo su pavarde Petraitis ir pan.) https://stats.oecd.org/glossary/detail.asp?ID=6961
[33] https://www.nytimes.com/2019/06/26/technology/google-university-chicago-data-sharing-lawsuit.html
[34] „ANONYMIZATION OF COURT DECISIONS IN THE EU: ACTUAL AND COMPARATIVE ISSUES" (Gruodytė E., Milčiuvienė M.) https://www.vdu.lt/cris/bitstream/20.500.12259/60444/1/ISSN2029-4239_2018_N_2_18.PG_60-70.pdf
[35] VDAI apie nuasmeninimą: https://vdai.lrv.lt/uploads/vdai/documents/files/Rekomend_nuasmeninimo_metodai_2015.pdf

dokumentas remiasi ES Article 29 Working Party pateiktu platesniu dokumentu (Opinion 05/2014 on Anonymisation Techniques [36]). Pažymėtina, jog VDAI paruošta rekomendacija pasižymi tiksliu ir profesionaliu ES dokumento adaptavimu, teisingu matematinių sąvokų naudojimu bei gerai parinkta lietuviška terminologija, susijusia su nuasmeninimu. Šios rekomendacijos yra visiškai aktualios ir dabar daugumai atvejų, kai kalba eina apie įvairių įprastinių duomenų bazių nuasmeninimą. Deja iš praktikos matome jog organizacijose dažnai nėra taikomi net minimaliai būtini nuasmeninimo metodai arba taikomi supaprastintai (pvz. pašalinant tik pagrindinius asmens identifikatorius, bet paliekant informaciją iš kurios įmanoma re-identifikacija). Minimus šiuose dokumentuose nuasmeninimo metodus ir kriterijus galima laikyti klasikiniais: aiškūs ir žinomi matematiniai modeliai, jų taikymas informacinėse sistemose bei tam skirti įrankiai. Tenka pripažinti jog ne visa terminologija (pvz. k anonimiškumas, l įvairovė ir t tankis („*k-anonimity*“, „*l-diversity*“, „*t-closeness*“)[37] naudojama matematiniuose nuasmeninimo modeliuose yra iki aiški Duomenų apsaugos pareigūnams. Tinkamas matematinių modelių ir nuasmeninimo kokybės kriterijų naudojimas jau reikalauja specifinių matematinių bei duomenų bazių programavimo, saugos ir valdymo žinių.

Nuo 2014 m. kai buvo išleistos minėtos rekomendacijos įvykę nemažai pokyčių. Pavyzdžiui, blokų grandinės („*blockchain*“) naudojimas įneša savo specifiką taikant nuasmeninimo algoritmus. Kai kuriais atvejais duomenų esančių blockchain'e nuasmeninimas netgi nėra įmanomas, nes nėra galimas pačios blokų grandinės keitimas, o tik papildymas - taip vadinima „*Blockchain Immutability*" arba „*Irreversibility*“ (liet. Nekintamumo) savybė. Kitaip tariant, jei duomenys koduoti blokų grandinėje turi identifikuojančius asmens duomenis, jų pašalinti arba pakeisti nėra įmanoma. Tokias atvejais reikia jau informacinės sistemos planavimo fazėje numatyti pvz. kelių blokų grandinių naudojimą - tai leistų atskirti identifikuojančius ir nuasmenintus duomenis. Nors skirtingų šalių reguliatoriai, kaip kad Prancūzijos CNIL stebi blokų grandinių sferą ir išleidžia su tuo susijusias rekomendacijas rekomendacijas[38], anonimiškumo užtikrinimo klausimas blockchain'e yra kol kas neliečiamas, laikant blokų grandines tiesiog asmens duomenų saugojimo forma.

[36] Pagrindinis dokumentas kuriuo remtąsi ir VDAI pateiktose rekomendacijose: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

[37] Parametrai, kurie parodo kiek kokybiškai galima anonimizuoti konkretaus duomenų lauko reikšmes: k-anonimity parodo kiek unikalių reikšmių gali būti vienam įrašui, l-diversity metodas leidžia apibendrinti reikšmes, t-closeness parodo kiek reikšmių gali būti konkrečiame intervale.

[38] CNIL apie blockchain'us: https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data

Pastartuoju metu ženkliai didėja nestruktūruotų duomenų naudojimas (duomenys, tekstai, įrašai ir visa kita informacija skirti vėlesniam apdorojimui ir analitikai, tame tarpe ir dirbtinio intelekto („*Artificial Intelligence*“) priemonėmis. Tokio tipo duomenų apdorojimas gali pakankamai nesunkiai rasti dėsningumus bei nustatyti kaip duomenys buvo nuasmeninti ir pagal tai atstatyti pradinius sąryšius su konkrečiais asmenimis. Visiškai nestruktūruotų duomenų nuasmeninimas yra ypač sudėtingas uždavinys, nes tokio tipo duomenys pagal savo pobūdį paprastai yra unikalūs kiekvienam įrašui, todėl jų nuasmeninti prieš tai nesustruktūravus (kad būtų galimas agregavimas) dažnai nėra galimybės. Tais atvejais kai „duomenų ežero“ („*Data lake“)* duomenų saugyklose laikomi įvairūs įrašai iš struktūruotus duomenis teikiančių šaltinių - interneto portalų, daiktų interneto (IoT - Internet of Things) jutiklių, verslo partnerių pateikiamų duomenų bazių - nuasmeninimas yra įmanomas, tik paprastai reikia įvertinti kiekvieną saugykloje esantį duomenų rinkinį atskirai bei atsižvelgti į jų galimus sąryšius.

Socialinių tinklų informacijos naudojimas sukuria naujas rizikas – dažnai apie asmenis galima legaliais būdais gauti tiek informacijos, kad nuasmeninto duomenų rinkinio duomenų laukai gali tapti „paskutine dėlionės detale“. Tai kas anksčiau buvo prieinama tik OSINT („Open-Source Intelligence“) profesionalams, dabar yra prieinama tiek bet kuriam interneto naudotojui, tiek ir automatizuotomis analizės priemonėms.

Kitas svarbus pasikeitimas - Bendrasis Duomenų Apsaugos Reglamentas (BDAR) pabrėžia numatytojo privatumo („Privacy by Design“) svarbą. Ankstesnėje duomenų apsaugos direktyvoje (95/46/EC) šiai temai buvo skirta mažiau dėmesio, be to nebuvo naudojama būtent ši terminologija. Pabrėžtina jog nuasmeninimo algoritmai, matematiniai modeliai ir techninė realizacija turi būti numatyti jau sistemos projektavimo etape ir įdiegti į sistemą ją kuriant (programuojant). Taip užtikrinama integrali ir nuosekli asmens duomenų apsauga. Tais atvejais kai duomenys nuasmeninami jau vėlesniuose etapuose (pvz. tiesiog nuasmeninant anksčiau sukurtą duomenų bazę) paprastai kyla daugiau rizikų dėl galimos re-identifikacijos ar galimo duomenų praradimo.

Daugelyje duomenų apsaugos teisės aktų yra minima pseudonimizacija, visgi gana dažnas ir klaidingas šio proceso supratimas. Pseudonimizacija, skirtingai negu anonimizacija (nuasmeninimas) nenumato negrįžtamo identifikuojančių asmens duomenų pašalinimo. Įprastiniais atvejais tai yra unikalaus identifikatoriaus suteikimas konkrečiam asmeniui bei to identifikatoriaus naudojimas vietoje tiesiogiai identifikuojančių duomenų, pvz. vardo / pavardės, asmens kodo ar jų derinio. Pažymėtina, jog teisingai tvarkant pseudonimizuotus duomenis duomenų bazė ar lentelė kurioje laikomos

identifikatorių sąsajos su konkrečiu asmeniu turėtų būti laikomos atskirai nuo kitų asmens duomenų rizikos mažinimui informacijos saugos požiūriu.

Nuostata, jog nuasmeninimą galima atlikti tiesiog ištrinant minėtą pseudonimų identifikatorių sąsajų su vardais ar asmens kodais lentelę ar duomenų bazę, ir tada likę duomenys tampa nuasmenintais nėra teisinga. Reikia įvertinti ar iš likusių duomenų nėra įmanoma atlikti re-identifikacijos (ar nėra kvaziidentifikatorių, susiejamų laukų, unikalių parametrų ir pan).

Nuasmeninimo galimybės programinėje įrangoje

Kai kurie programinės įrangos paketai, skirti darbui su duomenų bazėmis savyje jau turi paruoštas nuasmeninimo funkcijas. Tokių funkcijų privalumas - jos jau būna įdiegtos ir dažniausiai gana paprastai panaudojamos. Trūkumai - gali pritrūkti galimybių ir universalumo. Keli pavyzdžiai:

- *Oracle* – „Data masking and Subsetting“ funkcionalumų rinkinys duomenų bazių valdymo sistemoje;
- *SAP Hana* verslo valdymo sistema - nuasmeninimo funkcionalumas su automatiniu kriterijų nustatymų („k-anonimity“) ir įvertinimu;
- *Microsoft Azure SQL* duomenų bazių valdymo sistema - Dynamic Data Masking funkcionalumas;
- *Amazon Web Services* - įvairūs duomenų maskavimo ir anonimizavimo funkcionalumai nuo Amazon Macie iki dirbtinio intelekto principais pagrįstų nuasmeninimo algoritmų.

Kitose platformose nuasmeninimo algoritmus ir metodus gali tekti suprogramuoti. Tokiose programavimo platformose kaip Visual Studio, GitHub[39] ir pan. yra pakankamai bibliotekų ir modulių su jau aprašytomis funkcijomis duomenų nuasmeninimui įvairiais metodais populiariomis programavimo kalbomis (Java, Python, C# / C++ ir pan.). Tai taupo programuotojų laiką bei sumažina klaidų tikimybę.

Galiausiai, turint konkrečius duomenų rinkinius yra specializuota programinė įranga skirta duomenų rinkinių nuasmeninimui ir įvairių kriterijų (pvz. k anonimiškumo) nustatymui, kurie reikalingi pasitikrinant ar kokybiškas nuasmeninimo modelis pasirinktas. Keli paminėtini įrankiai - nemokami (Open Source licencijos ir platinimo tipas): https://arx.deidentifier.org/ arba https://amnesia.openaire.eu/ . Profesionalios mokamos programinės įrangos skirtos nuasmeninimui (taip pat paprastai dalis nuasmeninimo funkcijų

[39] Nuasmeninimo modulių pavyzdžiai GitHub platformoje: https://github.com/topics/data-anonymization

naudojama ir maskuojant ar pseudonimizuojant duomenis) galima rasti internete, pvz. https://aircloak.com/ bei kiti pavyzdžiai.

Apibendrinant – tiek standartinėje programinėje įrangoje, tiek ir programavimo platformose dažnu atveju jau yra paruošti nuasmeninimo metodai ir nuasmeninimo efektyvumo įvertinimas. Kuriant sistemas reiktų remtis jau esamais nuasmeninimo modeliais ir algoritmais, nes kuriant savus nuasmeninimo modelius tai reikia daryti kokybiškai, ko pasėkoje reikalinga aukšta programuotojų kvalifikacija ir nemažos laiko sąnaudos. Naudoti kokybiškus jau paruoštus programinės įrangos komponentus bus kur kas efektyviau nei kurti savus modelius.

Pastaruoju metu keliama daug klausimų dėl įvairių identifikatorių naudojimo renkant informaciją apie interneto vartotojus, jų naršymo įpročius bei rezultatus. Vienas iš pirmųjų vykstančių procesų dėl Google Analytics naudojimo taip pat kelia klausimus apie tai, jog nėra užtikrintas tinkamas nuasmeninimas. Platesnė informacija – CNIL sprendime dėl Google Analytics[40] . Tai akivaizdžiai parodo, jog tinkamo nuasmeninimo nebuvimas gali kelti esminę riziką visam įmonės verslo modeliui.

Interneto adresų (IP) identifikatorių naudojimas yra atskiras klausimas. Šie adresai yra būtini sistemų veikimui, nes pats sistemų veikimo principas nenumato situacijų kai komunikacija galima visiškai anonimiškai, t.y. kiekvienas duomenų paketas turi būti priskirtas kažkuriam šaltiniui. IP v4 (didžiausio adreso formatas 255.255.255.255) visa internetinių adresų erdvė tėra 2^{32} arba tikrai 4 294 967 296 adresų. T.y. šiuolaikinėse sistemose patikrinti visus internetinius adresus (pvz. jei reikia surasti reikiamą dėmenį re-identifikacijai) nėra neįvykdomas uždavinys. Aišku, šis uždavinys sprendžiamas IP v6 adresų erdvės naudojimu – ten galimų adresų yra 2^{128} – čia dabartinėmis priemonėmis visų variantų perrinkimas jau yra neįmanomas, todėl įmanoma realus nuasmeninimas pašalinant adreso dalį. Steve Leibson pateikia gerą pavyzdį: IP v6 leidžia suteikti IP adresą kiekvienam atomui žemės paviršiuje, ir adresų erdvės dar pakaktų 100+ žemės planetų.

Tinkamo duomenų nuasmeninimo pavyzdžiai

Pavyzdys 1: Pateikiamas realus pavyzdys iš Google renkamų asmens duomenų. Dirbant su grupe United4Health ir analizuojant COVID-19 sergamumo statistiką vienas iš svarbių kriterijų yra populiacijos mobilumas.

[40] CNIL pirmasis sprendimas dėl google Analytics: https://www.cnil.fr/en/use-google-analytics-and-data-transfers-united-states-cnil-orders-website-manageroperator-comply

Siekiant įvertinti žmonių mobilumą konkrečiame regione, Google pandemijos metu reguliariai publikuoja taip vadinamus "Community Mobility reports"[41]. Šios ataskaitos leidžia įvertinti, kiek laiko praleidžiama namuose, parduotuvėse, transporte ar gamtoje. Duomenys renkami pagal agreguotą vartotojų judėjimo informaciją remiantis geolokaciniais išmaniųjų telefonų duomenimis (GPS).
Analizuojant konkrečiai Lietuvos statistiką kai kurie duomenys ėmė kelti abejones - Vilniaus apskrityje ar Lenkijos regionuose duomenys rodė daug pokyčių, tuo tarp Tauragės apskrityje kai kurių kategorijų objektuose duomenys buvo akivaizdžiai neatitinkantys tikrovės arba tiesiog nerodantys jokių pokyčių. Pasitikslinus paaiškėjo, jog vietos nustatymo duomenimis yra taikoma visa seka įvairių nuasmeninimo metodų: nedideli duomenų iškraipymai įvedant "triukšmą", duomenų ribojimas jei tame objekte buvo mažiau nei nustatyta minimali riba asmenų su išmaniaisiais telefonais, duomenų "sulyginimas" jei pasitaikydavo labai iššokančių iš nustatytų intervalų reikšmių, naudojamų duomenų laukų apribojimas bei kiti metodai (detaliai naudoami nuasmeninimo metodai ir modeliai aprašyti straipsnyje Google COVID-19 Community Mobility Reports: Anonymization Process Description[42], Tai parodo kokia reikšmė teikiama nuasmeninimui pasaulio technologijų lyderių pateikiamuose atvirųjų duomenų rinkiniuose.

Pavyzdys 2: Elektroninių pardavimų portalui keičiant savininką nebeliko teisinio pagrindo turėti anksčiau buvusių klientų duomenis. Tuo tarpu parduotuvės rinkodaros ir statistikos tikslams buvo būtina išsaugoti duomenis apie pirktus produktus. Deja, naudojama el.komercijos platforma neturėjo jokių asmens duomenų nuasmeninimo funkcijų. Išanalizavus duomenis buvo priimtas sprendimas palikti nuasmeninintus pirkimų duomenis pašalinant pirkėjų identifikacinius duomenis ir kai kuriuos kvaziidentifikatorius. Likę įrašai buvo agreguoti apibendrinant juos geografiniame lygyje, patikrinant ar duomenų nuasmeninimą leidžia k-anonimiškumo bei L-įvairovės kriterijai konkrečiai kiekvieno pirkimo duomenims. Technologinė nuasmeninimo proceso realizacija - dėl pakankamai nelanksčios e-komercijos platformos teko parašyti programą (paprastai tokios programos vadinamos „automatizacijos robotais“) automatizuotai pašalinančią nereikalingus asmens duomenis ir pakeičiantį adresus į agreguotus vietovės duomenis atskirai kiekviename įraše. Šiam automatizuotam įrankiui rašyti buvo panaudota Python programavimo kalba.

[41] Google COVID-19 Community Mobility reports: https://www.google.com/covid19/mobility/
[42] Straipsnis “Google COVID-19 Community Mobility Reports: Anonymization Process Description“ (Aktay A. and others https://arxiv.org/pdf/2004.04145.pdf

Praktinis nuasmeninimo įvertinimo modelis duomenų apsaugos pareigūnams

Susiduriant su įvairiais uždaviniais praktinėje veikloje, dažnai matome situacijas kai įmonė nori pasilikti duomenų masyvus statistikai savo naudojimui (pvz. rinkodaros analizei) ar atverti išoriniams vartotojams. Duomenų nuasmeninimas ir jų įvairovės išsaugojimas yra vienas kitam prieštaraujantys procesai, kur būtinas balanso suradimas - tam kad duomenys išlaikytų savo vertę statistikai, rinkodarai, moksliniams tyrimams, bet kartu negalėtų atskleisti susijusio asmens tapatybės. Nuasmeninimo modelių ir metodų paruošimas negali būti paliktas vien programuotojų ar sistemos architektų žinioje - šiame procese strateginiu - taktiniu lygmeniu yra būtinas DAP dalyvavimas įvertinant nuasmeninimo efektyvumą.

Vienas iš principų - kuo ankstesnis duomenų nuasmeninimas jų naudojimo procese. Jei konkretus veiklos procesas leidžia padaryti duomenų nuasmeninimą neprarandant jokių svarbių veiklos funkcijų - reiktų arba įdiegti nuasmeninimą, arba (kai tai įmanoma) iš viso ištrinti asmens duomenis. Ankstyvas nuasmeninimas sumažina rizikas kartu paliekant reikiamų duomenų analizės bei statistinio panaudojimo galimybes.

Laikoma jog bet koks duomenų masyvas yra sudarytas iš tokių tipo laukų:

- *Identifikatoriai* (unikalus, tiesiogiai į asmenį nurodantis ir jį identifikuojantis duomuo, pvz. asmens kodas, vardo ir pavardės kombinacija);
- *Kvaziidentifikatoriai* (duomenų laukas kuris pats nėra unikalus identifikatorius, bet derinant kartu su kitais laukais gali tapti identifikatoriumi;
- *Jautrūs duomenys* (duomenys, kurių atskleidimas sukuria ženklią žąlą ar pavojų duomenų subjektui);
- *Įprastiniai duomenys* (duomenys, kurių atskleidimas nesukelia ženklių pasekmių duomenų subjekto socialinėje - ekonominėje aplinkoje).
  Įprastinė nuasmeninimo proceso problema – kaip užtikrinti jog jautrių ar įprastinių duomenų atskleidimas nesudarytų galimybės iš jų sukurti naujus kvaziidentifikatorius ir pagal tai re-identifikuoti asmenį.

Privacy Partners veikloje paruošėme tokį supaprastintą planą nuasmeninimo metodų parinkimui:

1. ***UŽDAVINIO SUFORMULAVIMAS***

a. Nustatoma, kokius duomenis ir dėl kokių priežasčių reikia palikti tolesniam naudojimui;
b. Naudojimo aprėptis: nustatoma ar tai bus duomenų paruošimas "*case by case*" - pagal reguliarias užklausas (tokiais atvejais reikia spręsti „*differenttial privacy*“

tipo uždavinius diferencinis privatumas), ar tai vienkartinis atvirųjų duomenų rinkinio paruošimas;

c. Konkretizuojama kas gaus prieigą prie asmens duomenų - vidiniam organizacijos naudojimui ar bus pateikiama kaip atvirųjų duomenų rinkinys?

2. DUOMENŲ ĮVERTINIMAS

d. Nustatomi identifikatoriai (tiesiogiai asmenį identifikuojantys laukai, pvz. vardas, pavardė, asmens kodas);
e. Nustatomi vidiniai identifikatoriai (pseudonimai, kodai, unikalus eilės numeris ir pan.), kvazidentifikatoriai;
f. Atsižvelgiama ar duomenų laukai neturi antrinių požymių (pvz. video ar audio įrašas gali tiek turėti identifikuojančią informaciją savyje, tiek turėti metaduomenis apibrėžiančius kada įrašas padarytas ir kas jame dalyvauja);
g. Įvertinami visi reikšmių laukai, jų unikalumas ir jei tas reikalinga - šie pagrindiniai kriterijai: K anonimiškumas („k-anonimity“), l įvairovė („l-diversity“), T tankis („t—closeness“).

3. NUASMENINIMO TAKTIKOS PARINKIMAS

h. Duomenų lauko pašalinimas. Ar galima tiesiog pašalinti (ar prilyginti 0) duomenų lauko reikšmę?
i. Maskavimas („*masking*“ ir „*obfuscation*“). Ar galimas atsitiktinių reikšmių parinkimas? Ar jos kartosis?
j. Perstatymas („*permutation*“) įvertinama duomenų perstatymo galimybė (kurių laukų reikšmes galima tarpusavyje kaitalioti, neprarandant duomenų naudingumo statistikai?
k. „*Tokenisation*“ (reikšmės pakeitimas kitais duomenimis), šifravimas ar pseudonimizavimas taikomas duomenų apsaugai;
l. „*Homomorphjc encryption*“ (duomenys užšifruojami taip, kad atliekant skaičiavimus su duomenimis, rezultatas gaunamas toks pat kaip ir nešifruotų duomenų, bet duomenys nėra atskleidžiami);
m. Statistinio trukšmo įterpimas. Ar yra galimybė įterpti ar modifikuoti duomenis, pridėti papildomus įrašus su nedideliais nuokrypiais;
n. Duomenų skirstymas intervalais („*binning*“) leidžiamų duomenų iškraipymo ribose;
o. Ar nuasmeninimo algoritmai turi nenuspėjamumą ir atsitiktinių skaičių įvedimą („*randomization*“) - pvz. perslenkant visus vieno stulpelio laukus per vieną žemyn tai kiek sumaišo įrašus, bet gali sumaišyti nuspėjamai ir leisti atstatyti tikrąsias reikšmes);
p. Saugumas: ar nėra galimybės "patikrinti" nuasmeninimo algoritmus nesankcionuotai (t.y. įvedus konkrečius duomenis išanalizuoti kaip buvo gauti nuasmeninti duomenys).

4. NAUDOJIMAS IR IŠORINIŲ RIZIKŲ VERTINIMAS

q. Nustatoma ar likę laukai gali turėti unikalią įrašų kombinaciją vienam asmeniui;

r. Įvertinama kokia galimybė ir tikimybė gauti kitus duomenų rinkinius, pagal kuriuos galima nustatyti konkretų asmenį ir vienareikšmiškai jį priskirti konkrečiam įrašui;
s. Re-identifikacijos modelio sudėtingumas: įvertinama kiek sudėtinga galimo re-identifikavimo modelio sukūrimas, ar tai gali būti vertinga (aukšto jautrumo arba kitomis prasmėmis "brangūs" duomenys);
t. Išpuolių, susijų su re-identifikacijos iš nuasmenintų duomenų rizikų įvertinimas („*Inference*“ (išvados padarymas), „*Singling out*“ (išskyrimas) ir „*Linkability*“ (kelių laukų susiejimas);
u. "*Brute force*" - spėjimo ir visų variantų perrinkimo galimybės įvertinimas realiems duomenims;
v. Vertinama "*reverse engineering*" rizika: vertinama imant po vieną lauką ir analizuojant, kokios papildomos informacijos (išorinės ar vidinės) reiktų norint atstatyti įrašo sąsajas su konkrečiu asmeniu bei tokių veiksmų automatizuoto taikymo galimybė.

Svarbu įvertinti pasekmes, kurios grėstų tuo atveju, jei iš nuasmenintų duomenų būtų re-identifikuoti konkretūs asmenys (ar netgi visas jų sąrašas). Pagal kylančias rizikas reiktų pasirinkti nuasmeninimo technologijas, arba padaryti sprendimą nuasmenintų duomenų nenaudoti, o juos ištrinti. Ypač tai svarbu kai dirbama su specialiųjų kategorijų (pagal BDAR) duomenimis ar jautriais duomenimis, t.y. duomenimis kurie nors ir nėra priskirti spec. kategorijų duomenims (rasė, orientacija, medicininiai ar genetiniai duomenys, vaikų asmens duomenys ir pan.) bet gali sukelti ženklias reputacines, turtines, socialines ar kitokias pasekmes. Tokiu atveju galima vertinti situaciją naudojantis įprastinėms PDAV (Poveikio Duomenų Apsaugai vertinimo) metodikas modeliuojant situaciją "kokios būtų pasekmės jei nuasmenintoje duomenų bazėje esantys asmenys būtų re-identifikuoti ir taptų prieinami pašaliniams asmenims be duomenų subjekto leidimo". Taip pat būtina įvertinti kiek pagrįsti verslo, mokslo ar valstybės interesai konkrečiu duomenų panaudojimo atveju: vienos pasekmės asmeniui bus jei re-identifikacijos atveju sužinoma kiek kartų per metus jis lankėsi maisto prekių parduotuvėje, visai kita situacija - jei atskleidžiama pvz. kelianti aukštas reputacines rizikas medicininė diagnozė.

Tais atvejais jei kuriamoje sistemoje yra numatytas nuasmenintų duomenų saugojimas ir naudojimas – nuasmeninimo rizikų vertinimą būtina atlikti kaip PbD („*Privacy by Design*“) vertinimo proceso dalį. Tada galima pasirūpinti kad sistemoje nebūtų laikomi aukštos rizikos nuasmeninti duomenys, pašalinti galimus identifikuojančius parametrus taip užtikrinant tinkamą sistemos atitiktį.

Išvados

Nuasmeninimas siekiant duomenis atsieti nuo konkrečių asmens duomenų subjektų turi savo rizikas. Jos gali kilti tiek iš neteisingai parinkto matematinio nuasmeninimo modelio (palikta per daug duomenų, galimas duomenų susiejimas ir vėlesnė asmens re-identifikacija), tiek dėl technologinės realizacijos (parinktos per daug paprastos, atsekamos technologinės priemonės) ar prie duomenų suteikta per daug plati prieiga.

Būtina suvokti jog nuasmeninimo metu beveik visada mažėja duomenų rinkinio vertė – siekiant pašalinti sąsajas su asmenimis, būtina pašalinti ne tik tiesiogiai identifikuojančią informaciją, bet ir kitus duomenis galinčius sukelti re-identifikaciją (pvz. pašalinus asmens pirkimų istoriją rinkodaros skyriui tokie duomenys gali tapti beverčiais).

Vertinant re-identifikacijos rizikas reikia turėti omenyje jog prieiga prie duomenų internete gali būti praktiškai neribota, taip pat gali būti naudojamas didžiulis įvairių atvirųjų duomenų šaltinių skaičius kuris gali sukurti situacijas kai duomenys, kurie atrodė labai kokybiškai nuasmenininti, bus panaudoti kartu su kitais duomenų šaltiniais ir bus atlikta re-identifikacija.

Atliekant nuasmeninimo kokybės, saugumo ir kylančių rizikų vertinimus būtina naudotis struktūruotomis metodikomis, leidžiančiomis pažingsniui įvertinti konkretaus atvejo rizikas bei parinkti nuasmeninimo taktiką, technologiją ir matematinius modelius. Tokia supaprastinta metodika, tinkama DAP'ų naudojimui kasdieniniame darbe pateikta šiame straipsnyje.

Esant galimybei reikia naudotis jau esamomis priemonėmis įvertinant duomenų rinkinių parametrus svarbius nuasmeninimo procese. Kuriant informacines sistemas, nuasmeninimas turi būti numatomas kartu su kitomis privatumo užtikrinimo priemonėmis vykdant konkrečios sistemos numatytojo privatumo ("*Privacy by Design*") priežiūros procesus.
Net ir nuasmeninus duomenų rinkinius, duomenų valdytojams būtina rūpintis ar pasikeitus situacijai (pvz. internete patalpinus kitus duomenų rinkinius) nuasmeninti duomenys netapo asmens duomenimis, t.y. ar nėra galimybės įvykdyti re-identifikaciją.

ASMENINIŲ PRIETAISŲ NAUDOJIMAS DARBUI ATLIKTI: KAIP RASTI BALANSĄ TARP PATOGUMO, SAUGUMO IR PRIVATUMO

Renata Vasiliauskienė
Vyresnioji teisininkė, advokatų kontora COBALT

Santrauka

Pastaraisiais metais itin smarkiai padidėjo darbuotojų besinaudojančių asmeniniais prietaisais darbui atlikti. Ši tendencija ypač išryškėjo išpopuliarėjus išmaniesiems prietaisams, tačiau ji turi savo trūkumų. Pagrindiniai trūkumai siejami su asmeninių prietaisų naudojimu darbui gali būti apibendrintai suskirstyti į keturias kategorijas: saugumo, teisiniai, psichologiniai ir sociologiniai trūkumai. Šiame straipsnyje pateikiama įvairių tyrimų apžvalga susijusi su asmeninių prietaisų naudojimo saugumo ir teisinėmis problemomis, tokiomis kaip prietaisų praradimas, kenkėjiškų atakų padidėjimas, nesaugaus ryšio naudojimas, konfidencialumo įsipareigojimų pažeidimas, nesaugus duomenų perdavimas į trečiąsias šalis ir teisės į privatų gyvenimą pažeidimas. Nepaisant to, kad rizikos susijusios su asmeninių prietaisų naudojimu yra didelės ir sunkiai išvengiamos, straipsnyje aptarti tyrimai rodo, kad ši tendencija ateityje tik didės, nes žmonės yra linkę privatumą ir saugumą aukoti vardan patogumo, todėl įmonėms yra būtinos vidinės tvarkos, kurios, idealiu atveju, turėtų atspindėti balansą tarp įmonės informacijos, darbuotojo privatumo apsaugos ir patogumo.

Raktiniai žodžiai: asmeniniai prietaisai, privatumas, saugumas, rizikos, grėsmės, BYOD, BDAR, kibernetinė sauga.

Įžanga

Pastaruosius keletą metų asmens duomenų apsaugos tema susilaukė nemažo dėmesio. Didžiąją dalimi tą lėmė Bendrojo duomenų apsaugos reglamento (toliau – „BDAR“) priėmimas. Tačiau, nepaisant šio išaugusio dėmesio, net ir labai uoliai BDAR įgyvendinimui pasirengusioje įmonėje, galima rasti vieną itin pažeidžiamą vietą – tai asmeninių komunikacinių priemonių naudojimas darbo funkcijoms atlikti. Šio straipsnio objektas yra problemų, kurias sukelia asmeninių prietaisų naudojimas darbui, identifikavimas. Praktikoje dažnai tenka susidurti su įmonių vadovais, kurie, bandydami parodyti savo šiuolaikiškumą, deklaruoja, kad pas juos darbuotojai, be įvairių kitų privilegijų turi ir galimybę dirbti iš bet kurio pasaulio krašto, namuose, sodybose, ar kur kitur ir, kas aktualu šiame straipsnyje, neribojant priemonių su kuriomis jie dirba, pasirinkimo, t.y. leidžiant darbui naudoti savo asmeninius telefonus, kompiuterius ir kitas ryšio priemones. Kiekvienam darbdaviui atsakant į klausimą, leisti ar drausti naudoti asmeninius prietaisus darbo funkcijoms atlikti, reikia gerai žinoti tokio darbinio režimo rizikas ir galimas pasekmes. Argumentai „už“ yra intuityviai suvokiami ir nereikalauja didesnių diskusijų: tai patogumas, produktyvumo padidėjimas, reagavimo greitis, galimybė pačiam būti pasiekiamam, pasiekti savo kolegas bet kuriame pasaulio krašte, darbdavio patrauklumas, šiuolaikiškumas ir lankstumas. O štai argumentai „prieš“ tarsi pranyksta kitose platesnėse diskusijose ir nesudaro tinkamos atsvaros. Šio straipsnio tikslas - atkreipti didesnį dėmesį į tai, kokias rizikas sukelia asmeninių prietaisų naudojimas darbui, bus aptartos esminės saugumo ir teisinės problemos bei išryškinti pagrindiniai uždaviniai, kuriuos turi spręsti darbdavys. Konkrečiai, bus apžvelgiami Lietuvos ir pasaulio tyrimai šia tema, analizuojami galimi sprendimai bandant atsakyti į klausimą, kur šiuolaikinėje informacinėje ir greito vartojimo visuomenėje yra balansas tarp darbuotojo patogumo, įmonės konfidencialios informacijos saugumo ir privatumo.

Šio straipsnio aktualumas yra itin svarbus atsižvelgiant į 2020 metų realijas, kadangi dėl COVID-19 pasaulinės pandemijos daugelis darbuotojų praktiškai per vieną dieną buvo išsiųsti tęsti darbus nuotoliniu būdu namuose, o dirbant tokiu režimu greitai pasimatė tokio darbo sukeliamos problemos, kadangi masiškai dirbant iš namų, darbdaviai pajuto, kad jie praranda įmonės informacijos naudojimo kontrolę ir nemaža dalis jų suprato neturintys priemonių užtikrinti, ar darbuotojai prie įmonės informacinių sistemų, elektroninio pašto ir kitų šaltinių jungiasi paisydami saugumo reikalavimų, vidinių tvarkų ir kibernetinės higienos.

Problemos susijusios su asmeninių prietaisų naudojimu darbo funkcijoms

Tobulėjančios informacinės ir komunikacinės priemonės palengvina mūsų gyvenimus, paspartina darbo procesus ir suteikia naujas galimybes. Ar staiga išleisti visą įmonę dirbti nuotoliniu būdu, kaip tai nutiko įvedus Covid-19 karantiną, būtų įmanoma be Teams, Zoom, plačiai paplitusio spartaus interneto ryšio? Greičiausiai ne. Todėl technologijų pažanga ir jų nauda visuomenės tobulėjimui nėra kvestionuojama. Visgi šios galimybės atėjo nebe iššūkių. Itin išaugęs išmaniųjų įrenginių naudojimas, daiktų internetas, galimybė nuotoliniu būdu valdyti prietaisus, programėlių gausa, automatinis informacijos bendrinimas tarp įrenginių – visa tai sukuria puikias sąlygas piktavaliams pasinaudoti techninėmis spragomis ir, deja, žmonių aplaidumu ir neišmanymu. Apibendrintai galima būtų pasakyti, kad pagrindinės rizikos, kurios yra identifikuojamos daugelyje tyrimų, skirtų asmeninių prietaisų naudojimui darbe, gali būti suskirstytos į šias: (i) kibernetinės, (ii) teisinės, (iii) psichologinės ir (iv) sociologinės. Psichologinės ir sociologinės problemos yra labiau susijusios su įmonės kolektyvo tarpusavio ryšių silpnėjimu, persidirbimu, negebėjimu atskirti darbo ir asmeninio gyvenimo, priklausomybe nuo prietaisų ir, kadangi labiau siejasi su tarpasmeniniais santykiais, toliau šiame darbe nebus nagrinėjamos. Šiame straipsnyje bus akcentuojamos informacijos saugumo (kibernetinės) grėsmės ir teisiniai iššūkiai, kadangi jie yra ne tik kartu tarpusavyje glaudžiai susiję, bet ir įvardijami, kaip aktualiausi verslo bendruomenei.

1. Informacijos saugumo problemos

Kaip minėta, informacijos saugumas buvo vienas iš kertinių techninių rūpesčių prasidėjus masiškam nuotoliniam darbui 2020 metų pradžioje ir įvedus visuotinį karantiną. Nagrinėtuose šaltiniuose išskiriamos toliau išvardintos pagrindinės informacijos saugumo (kibernetinės) grėsmės, kai darbui naudojami asmeniniai prietaisai.

1.1. Prietaisų praradimas - tai vis dar yra vienas dažniausių iššūkių įmonės informacijos saugumui ir skirtingų tyrimų duomenimis nuo 39[43] iki 54[44] procentų duomenų saugumo pažeidimų yra susiję būtent su įrangos praradimu (pametimu, vagystėmis ir pan.). Daugelis asmeninių

[43] THE "BRING YOUR OWN DEVICE" TO WORK MOVEMENT:
Engineering Practical Employment and Labor Law Compliance Solutions, 2012, 14p.
[44] https://www.kaspersky.com/blog/the-human-factor-in-it-security/

prietaisų šiuo metu yra mobilūs ir dėl to, palyginus su stacionariomis darbo vietomis, rizika juos pamesti yra kur kas didesnė. Kadangi didžiąją dalimi ši rizika susijusi su taip vadinamu „žmogišku faktoriumi“, akivaizdu, kad ir efektyvi priemonių šiai rizikai suvaldyti beveik nėra. Taigi, įmonių vadovams, sudarant sąlygas savo kolektyvui be apribojimų naudoti asmeninius prietaisus darbui, tiesiog belieka tikėtis, kad tokių žmogiškų klaidų bus kuo mažiau, nes jų visiškai išvengti yra neįmanoma. Ką galima padaryti, tai įpareigoti registruoti visus asmeninius prietaisus, naudojamus darbui, reikalauti privalomai instaliuoti nuotolinę informacijos sunaikinimo funkciją, reikalauti privalomai pranešti apie prarastą asmeninį prietaisą, specialių programėlių pagalba atskirti privačią ir darbinę aplinką, apsaugoti įrenginius stipriu slaptažodžiu ir imtis kitų panašių priemonių, tačiau reikia suprasti, kad jų efektyvumas didžiąją dalimi priklauso nuo darbuotojų sąžiningumo ir supratimo, kokią žalą įmonei gali atnešti vienas prarastas įrenginys – viena saugumo spraga. Analizuojant straipsnius šia tema nepavyko rasti kažkokių stebuklingų priemonių, kurios neutralizuotų žmogiškas klaidas, todėl ši rizika išlieka tarp sunkiausiai suvaldomų ir reikia ją itin atidžiai įvertinti leidžiant savo kolektyvui naudotis asmeninius prietaisus darbui.

1.2. Virusų ir kitų kenkėjiškų programų, skirtų mobiliesiems prietaisams, atakų ženklus padidėjimas. Pastarąjį dešimtmetį stebimas nuolatinis kenkėjiškų atakų didėjimas, todėl itin svarbu laiku atnaujinti antivirusines programas, operacines sistemas, laikytis kibernetinės higienos. Paradoksas tame, kad antivirusinių programų naudojimas ir kitoks kibernetinių atakų užkardymas yra beveik savaime suprantamas, kai kalbame apie kompiuterius, tačiau dar visiškai nesuvokiamas, kai kalba pasisuka apie telefonus, planšetinius kompiuterius, išmaniuosius laikrodžius ir kitus tarpusavyje sujungtus įrenginius. Dar daugiau, dalis išmaniųjų įrenginių, tokių kaip šaldytuvai, termostatai, internetinės saugumo kameros ir daugelis kitų tiesiog neturi tokios galimybės arba pakankamai galios, kad į juos galima būtų instaliuoti antivirusinę programą. Taigi turime situaciją, kai namuose su savo asmeniniu kompiuteriu dirbantis asmuo, sukuria itin nesaugią situaciją, nes jo namų tinkle esantys daiktai atveria saugumo spragą. Dilema, kurią turi išspręsti darbdavys – kaip efektyviai sukontroliuoti, ar asmeniniuose prietaisuose ir namų tinkle yra imamasi visų būtinų saugumo žingsnių. Svarbu akcentuoti, kad net ir vidinių tvarkų turėjimas, darbuotojų instruktavimas ir reguliarūs mokymai saugumo tema neužtikrina, kad patys naudojami prietaisai bus apsaugoti. Taigi, ši problema buvo, yra ir greičiausiai dar ilgą laiką bus opi bet kuriam vadovui, kuris ryžtasi liberalizuoti asmeninių prietaisų naudojimo darbo tikslams tvarką.

1.3. Informacijos bendrinimas – šiuolaikinių technologijų sukurtas iššūkis, kuris reiškia, kad dažnu atveju, net darbuotojui pačiam to neįtariant, darbinė informacija, esanti asmeniniame įrenginyje, gali būti persiunčiama į asmeninę debesies talpyklą. Taip vyksta todėl, kad dalis įrenginių ir naudojamų programėlių automatiškai bendrina informaciją – tokie yra jų numatytieji (angl. *default*) nustatymai. Kaip to išvengti leidžiant darbuotojams naudotis asmeniniais prietaisais? Kaip ir ankstesniu atveju, akivaizdu, kad vien įmonėje patvirtintų saugumo taisyklių tam nepakanka, nes reikia realiai užtikrinti, kad kiekviena nauja programėlė, ar naujas, su asmeniniu telefonu susietas, prietaisas neturi automatinių informacijos bendrinimo nustatymų. Kibernetinio saugumo specialistai tokiai rizikai suvaldyti siūlo specialias programėles, konteinerizaciją ir programinę įrangą leidžiančią asmeniniame įrenginyje atskirti darbinę ir privačią erdvę tokiu būdu užtikrinant, kad bet kokia nauja įdiegta programėlė neturės prieigos prie darbinės aplinkos. Visgi praktikoje kol kas tokių programėlių naudojimas yra sutinkamas gan retai. Priešingai, įmonių vadovų pasiteiravus apie galimybę techninėmis priemonėmis atskirti privačią ir darbinę erdvę asmeniniame telefone, dažniau tenka išgirsti, kad apie tokią galimybę jie sužinojo pirmą kartą.

1.4. Jungimasis prie nesaugaus interneto tinklo. Leidžiant darbuotojams jungtis prie darbo elektroninio pašto ar kitų informacinių sistemų ne iš stacionarios darbo vietos, tikimybė, kad bus jungiamasi prie viešo ar kito nesaugaus interneto ryšio yra didelė. Jungimosi prie viešo belaidžio interneto įpročiai buvo itin detaliai analizuoti 2016 metų Londono universiteto koledžo tyrime[45] *„Why do people use unsecure public Wi-Fi? An investigation on behaviour and factors driving decision".* Šio tyrimo metu nustatyta, kad žmonės dėl savo patogumo ir todėl, kad mano, jog nesaugus scenarijus neįsigyvendins, naudojasi viešu interneto ryšiu, net ir žinodami, kad jis nesaugus. Tyrimo metu taip pat nustatyta, kad moterys yra 3.67 karto[46] dažniau linkusios jungtis prie nesaugaus Wi-Fi ryšio siekdamos atlikti įvairias neskubias, nefinansines operacijas, negu vyrai. Įvairios ankstesnės studijos[47] taip pat parodė, kad, kai žmonės susiduria su konkuruojančiais poreikiais,

---

45 https://www.researchgate.net/publication/319694418_Why_do_people_use_unsecure_public_Wi-Fi_An_investigation_of_behaviour_and_factors_driving_decisions

46 https://www.researchgate.net/publication/319694418_Why_do_people_use_unsecure_public_Wi-Fi_An_investigation_of_behaviour_and_factors_driving_decisions

47 Herley, C. (2009, September). So long, and no thanks for the externalities: the rational rejection of security advice by users. In Proceedings of the 2009 workshop on new security paradigms workshop (pp. 133-144). ACM.

reikalaujančiais jų laiko ir įsigilinimo, jie sumažina savo pastangas skiriamas saugumui, t.y. kai reikia skubiai atlikti užduotį, saugumas yra aukojamas vardan greito rezultato. Be to, nustatyta, kad saugumo mechanizmų sudėtingumas yra kitas iššūkis, su kuriuo susiduria vartotojai, kas irgi lemia tai, kad vengiama naudoti papildomas saugumo priemones.[48]

Apibendrinant minėtas informacijos saugumo problemas, galima pasakyti, kad kiekvienai iš jų yra sukurtas problemos nukenksminimo būdas. Jeigu ne šimtaprocentinis, tai bet jau stipriai sumažinantis riziką. Kaip pavyzdžius galima būtų paminėti VPN ryšio naudojimą, duomenų šifravimą, prieigos teisių apribojimą, programėlių, atskiriančių privačią ir darbinę erdvę įrenginyje naudojimą, nuotolinį informacijos ištrynimą ir kitas. Tačiau yra keletas aspektų, kurie lemia vangų šių priemonių naudojimą. Iš jų turbūt reikšmingiausi yra kibernetinio saugumo žinių trūkumas ir finansinis aspektas - leidžiant darbuotojams naudoti savo asmeninius prietaisus darbui, gerokai išsiplečia infrastruktūros, kurią darbdaviui reikia saugoti sąrašas, todėl ir išlaidos skiriamos informacijos saugumui taip pat gerokai išauga. Dėl šių priežasčių keliant klausimą, kur rasti balansą tarp darbdavio informacijos saugumo ir darbuotojo patogumo, praktikoje matome, kad kol kas dar nugali patogumas ir minėtas tikėjimasis, kad blogasis scenarijus neįsigyvendins.

2. Teisinės rizikos, susijusios su asmeninių prietaisų naudojimu darbe

Kai pagal įmonėje nustatytą tvarką yra leidžiama naudotis asmeniniais prietaisais darbo funkcijoms atlikti, arba kai tokia tvarka apskritai nėra nustatyta, kyla ir įvairios teisinės grėsmės.

2.1. Pagrindiniu teisiniu iššūkiu yra rizika pažeisti darbuotojo privatumą, kadangi naudojantis tais pačias prietaisais ir darbo, ir laisvalaikio tikslais, riba tarp privataus gyvenimo ir darbo tarsi išsitrina. Praktikoje dažnai pasitaiko situacijos, kai įtariant, jog darbuotojas pažeidė įmonės vidines tvarkas, įrodymai yra būtent asmeniniame telefone. Darbdavio galimybės tokiu atveju paimti tokį telefoną ir jame esančius įrodymus vidiniam tyrimui yra labai ribotos (na, nebent iš karto prašant pareigūnų pradėti ikiteisminį tyrimą). Kaip pagrindinį argumentą neperduoti darbdaviui savo telefono, įtariamas darbuotojas dažniausiai naudoja

[48] Mannan, M., & van Oorschot, P. C. (2008, July). Security and usability: the gap in real-world online banking. In Proceedings of the 2007 Workshop on New Security Paradigms (pp. 1-14). ACM

savo teisę į privatumą. Ir beveik visada „laimi“ – darbdavys atsitraukia. Kai telefone viename sąraše yra asmeniniai ir darbiniai kontaktai, subendrintos asmeninio ir darbo elektroninio pašto dėžutės, nuotraukos ir kita informacija, surinkti reikiamus įrodymus nepažeidžiant teisės į privatų gyvenimą, beveik neįmanoma. Ši problema dažnai yra nevertinama kaip rimta iki tol, kol neatsitinka incidentas ir iškyla realus poreikis paimti įrodymus iš asmeninio įrenginio. Deja, įvykus pažeidimui, jau yra per vėlu ką nors pakeisti. Jeigu įmonėje nebuvo tinkamai sureguliuota asmeninių prietaisų naudojimo tvarka, belieka tik apgailestauti ir geriau pasirengti ateičiai.

2.2. Kita aktuali teisinė problema yra darbdavio konfidencialumo įsipareigojimų pažeidimas. Įmonės sudarydamos sandorius dažnai neatkreipia dėmesio į gan standartines konfidencialumo nuostatas, pagal kurias, kaip taisyklė, abi šalys įsipareigoja visą su sutarties sudarymu ir vykdymu susijusią informaciją laikyti paslaptyje ir saugoti nuo neteisėtos prieigos ar atskleidimo trečiosioms šalims. Mažai, kas pagalvoja, kad šio įsipareigojimo yra praktiškai neįmanoma įvykdyti leidžiant savo darbuotojams laisvai, be jokių papildomų saugumo priemonių, naudotis asmeniniais prietaisais darbo tikslais. Dėl ankstesniame skirsnyje minėtų automatinių informacijos bendrinimo nustatymų ir kitų saugumo spragų, kurias sukuria nekontroliuojamas asmeninių prietaisų naudojimas darbui - konfidencialumo įsipareigojimų pažeidimas praktiškai garantuotas.

2.3. Duomenų teikimas į trečiąsias šalis taip pat paminėtinas prie teisinių problemų, kurias gali sukelti nuotolinis darbas, jeigu jam naudojami asmeniniai komunikacijos prietaisai. Atsižvelgiant į šių metų specifiką dėl pandemijos, darbdaviai yra kur kas labiau linkę leisti dirbti nuotoliniu būdu. Didelė tikimybė, kad nuotolinis darbas ateityje išliks gan paplitusi darbo forma, nes tiek darbuotojai, tiek darbdaviai tame įžvelgia nemažai teigiamų aspektų. Tačiau, kai dirbant iš namų, „namai“ yra ne Lietuvoje, o gal net ir ne ES/EEE, vyksta duomenų teikimas į trečiąsias šalis. Tai sukelia dar vieną teisinę problemą, kadangi duomenų teikimas už ES/EEE ribų (ypač po *Schrems II* sprendimo) į nemažą dalį pasaulio valstybių tapo rizikingas. Jeigu įmonėje atsirado darbuotojas, ketinantis dirbti trečiojoje šalyje, darbdavys privalo žinoti, kad reikia imtis papildomų priemonių siekiant užtikrinti, jog duomenų teikimas atitiktų BDAR, t.y. būtų teisėtas ir saugus.

Apibendrinant teisines ir informacijos saugumo problemas, kurios kyla naudojant asmeninius prietaisus darbui, galima numanyti, kad jas sumažintų aiškios vidinės įmonės taisyklės, kuriomis būtų sureguliuotas asmeninių prietaisų naudojimas darbo tikslais, t.y. būtų numatytas draudimas tai daryti arba aiškiai apibrėžti reikalavimai, kuriuos įgyvendinus, būtų galima

pasinaudoti galimybe dirbti su savo asmeniniu prietaisu. Tačiau teisinėje praktikoje retai sutinkant tokio pobūdžio vidines taisykles, buvo nuspręsta atlikti pilotinį tyrimą apie tai, kokia praktika Lietuvoje yra susiklosčiusi asmeninių prietaisų naudojimo darbui tema.

Tyrimų apibendrinimas

Siekiant nustatyti asmeninių prietaisų naudojimo darbo tikslais įpročius, buvo naudojami du mokslinio tyrimo du metodai: apklausa ir dokumentų analizė.

1. Anoniminė apklausa buvo vykdoma pateikiant respondentams du klausimus. Viso gauta 30 anketų iš įvairių Lietuvoje veikiančių įmonių. Apibendrinus respondentų atsakymus, gauti tokie rezultatai: į pirmąjį klausimą - ar Jūsų atstovaujamoje įmonėje yra patvirtintos asmeninių prietaisų (pvz., telefonų, kompiuterių) naudojimo darbui atlikti taisyklės, 16,67 procentai respondentų nežinojo apie tai, ar jų įmonėje yra patvirtinta asmeninių telefonų ir kompiuterių naudojimo tvarka; 25 procentai respondentų teigė, kad jų įmonėje yra patvirtinta tvarka, apibrėžianti asmeninių prietaisų naudojimą, ir 58,33 procentai, kad tokios tvarkos nėra. Atsakymai į antrąjį klausimą – neatsižvelgiant į tai, ar yra patvirtintos asmeninių prietaisų naudojimo taisyklės, kokia praktika vyrauja įmonėje, 45,45 procentai respondentų atsakė, kad vyraujanti praktika yra vengimas naudotis asmeniniais prietaisais darbo tikslais; 27,27 procentai, kad asmeniniais prietaisais naudojasi laisvai be jokių apribojimų. Pasirinkusieji atsakymą „Kita“ dažniausiai nurodė, kad jų įmonėje nėra galimybės naudotis asmeniniais prietaisais arba, kad nėra poreikio naudotis savo asmeniniais prietaisais, nes darbdavys suteikia visas darbui reikalingas priemones. Atskirai paminėtinas ir atsakymas, jog darbdavys nesuteikia darbui skirtų telefonų, tačiau tikisi, kad darbuotojas atsilieps į skambučius būdamas ne darbo vietoje, arba atsakys į skubius elektroninius laiškus. Šie rezultatai rodo, kad Lietuvos įmonių praktika nelabai skiriasi nuo kitų šalių išskyrus vieną rodiklį, t.y. vidinių taisyklių, apibrėžiančių asmeninių prietaisų naudojimą darbui, nebuvimas. Lietuvoje šis rodiklis gerokai didesnis. Palyginimui, 2016 metais 6 iš 10 Amerikos įmonių buvo pasitvirtinusios BYOD (liet. pasiimk savo įrenginį) politikas.[49]

Svarbu paminėti, kad iki 2017 metų didelė dalis Lietuvos įmonių asmeninių prietaisų naudojimo tvarką buvo apsibrėžę tik fragmentiškai, kadangi tokia tvarka buvo neprivaloma, (tokią pareigą darbdaviams numatė tik 2017 m.

[49] https://www.insight.com/en_US/content-and-resources/2017/01182017-byod-statistics-provide-snapshot-of-future.html

įsigaliojęs Darbo kodeksas: 27 str., *„Darbuotojai turi būti supažindinti su informacinių ir komunikacinių technologijų naudojimo bei darbuotojų stebėsenos ir kontrolės darbo vietoje tvarka“*[50]. Įsigaliojus naujajam Darbo kodeksui, dalis įmonių suskubo priimti tokį vidinį dokumentą, deja, ši Darbo kodekso norma nuo 2018 metų, įsigaliojus BDAR, buvo panaikinta ir didelė dalis įmonių iki šiol tokios tvarkos taip ir neturi priėmusios. Todėl nenuostabu, kad didelė dalis apklausoje dalyvavusių įmonių (58,33 procentai) tokios tvarkos neturi.

2. Dokumentų analizės metodu buvo peržiūrėta dvidešimties (11 Lietuvos ir 9 užsienio) bendrovių vidinės tvarkos, skirtos informacinių ir komunikacinių priemonių naudojimui. Konkrečiai, buvo analizuojamos nuostatos skirtos asmeninių prietaisų naudojimo režimui. Nustatyta, kad maždaug penktadalyje tvarkų, asmeninių prietaisų naudojimo darbui režimas iš viso nėra aptartas (aptarimas tik priešingas variantas, t.y. darbo priemonių naudojimas asmeniniams tikslams). Jeigu darbo priemonių naudojimas asmeniniams tikslams yra suprantamas kaip grėsmė darbdavio interesams ir ypač darbo efektyvumui, tai atvirkštinis variantas – asmeninių priemonių naudojimas darbui - yra traktuojamas dažnai kaip teigiamas dalykas - toks darbuotojas suprantamas, kaip uolus ir visada pasiekiamas. Šią situaciją galima paaiškinti turbūt tuo, kad didelė dalis vadovų nežino arba neįvertina asmeninių priemonių naudojimo grėsmių, paminėtų šio straipsnio pirmoje ir antroje dalyse. Peržiūrėjus minėtas tvarkas buvo nustatyta, kad vyraujantis asmeninių prietaisų naudojimo modelis yra lankstus draudimas naudoti asmeninius prietaisus darbui. Lankstus draudimas reiškia, kad kaip bendra taisyklė yra numatytas draudimas, tačiau kartu nurodomos ir tam tikros išimtys, kai naudojimasis prietaisais būtų pateisinimas, tuo pačiu numatant ir pareigą darbuotojui nepagrįstai nedelsiant ištrinti asmeniniame telefone ar kompiuteryje patalpintą informaciją.

3. Kiti tyrimai. Iš Lietuvoje atliktų tyrimų šia tema paminėtinas 2019 metų „Kurk Lietuvai“ programos dalyvių Krašto apsaugos ministerijoje vykdytas projektas „Smulkiojo ir vidutinio verslo įmonių kibernetinio saugumo sąmoningumo didinimas“, kurio metu atlikta apklausa parodė, kad 74 proc. Lietuvos smulkių ir vidutinių įmonių jaučiasi nepasiruošusios arba nežino, ar yra pasiruošusios atremti kibernetines atakas. Po atlikto tyrimo ir interviu ciklo su kibernetinio saugumo ekspertais nustatyta, kad pažeidžiamiausias privačiame sektoriuje yra smulkusis šalies verslas.[51] Taip pat gan išsami saugumo mechanizmų analizė pateikiama 2017 m. Arvydo Bubnio „Asmeninių įrenginių,

[50] https://www.e-tar.lt/portal/lt/legalAct/f6d686707e7011e6b969d7ae07280e89
[51] Kibernetinis saugumas ir verslas: ką turėtų žinoti kiekvienas įmonės vadovas 2020: Nacionalinis kibernetinio saugumo centras, 2020 m. 4 psl.

naudojamų prieigai prie įmonės informacijos, saugos problemų tyrimas“ (KTU). Šiame darbe analizuojami asmeninių įrenginių saugos modeliai, kurie leidžia ne tik efektyviai atskirti privačią ir darbinę erdvę, tačiau ir užtikrinti informacijos saugumą įvairiuose lygmenyse.[52] Keletas užsienio privačių kompanijų, tokių kaip Kaspersky Lab, Ipsos MORI, Littler Mendelson, Webroot taip pat skelbia apie panašius tyrimus. Kaspersky Lab 2015 m. tyrimo duomenimis apie pusę darbuotojų naudoja asmeninius prietaisus darbo funkcijoms atlikti, ir tik 11 procentų darbuotojų, kurie naudojasi asmeniniais prietaisais darbo tikslais galvoja apie saugumą[53]. Ipsos MORI 2013 m. JAV apklausė 2000 asmenų 18-65 amžiaus grupėje ir nustatė, kad 18-24 amžiaus darbuotojai yra labiausiai linkę naudoti asmeninius prietaisus darbo reikmėms. 51 procentas tiriamųjų šioje amžiaus grupėje laiko su darbu susijusius dokumentus savo asmeniniame kompiuteryje ir 42 procentai dokumentus laiko išmaniajame telefone[54]. Gan išsami tarptautinės darbo teisės advokatų kontoros Littler Mendelson tyrimo *The “Bring your own device” to work movement: Engineering Practical Employment and Labor Law Compliance Solutions”* ataskaita apibendrina įvairius tyrimus šia tema ir pateikia didžiausias grėsmes, kurias sukelia asmeninių prietaisų naudojimas.[55] Dar vienas 2014 m. tyrimas atliktas debesijos paslaugų bei interneto kenkėjiškų programų gamintojos Webroot. Šis tyrimas parodė, kad darbuotojai nesiima adekvačių priemonių siekiant apsaugoti darbinę informaciją, t.y. daugiau nei pusė darbuotojų naudoja asmeninius prietaisus darbo reikmėms, nepaisant to, kad jiems yra išduotos ir darbinės priemonės. Be to, 60 procentų darbuotojų asmeninių mobiliųjų telefonų, naudojamų darbo tikslais, neturi arba turi tik gamyklinius saugumo nustatymus[56]; pusė respondentų teigia, kad nustotų naudoti asmeninius prietaisus darbui, jeigu įmonės politika reikalautų instaliuoti papildomas saugumo programėles[57]; didžiausia grėsmė, kurią įvardina darbuotojai, yra darbdavio galimybė turėti prieigą prie asmens duomenų[58].

---

[52] https://core.ac.uk/download/pdf/83930183.pdf
[53] Consumer Security Risks Survey - From scared to aware: digital lives in 2015 https://www.kaspersky.com/about/press-releases/2015_personal-devices-and-corporate-secrets-only-11-of-people-worry-about-keeping-work-files-safe-on-mobile-devices-kaspersky-lab-survey-shows
[54] http://www.mobilevillage.com/huddle-work-personal-devices-study/
[55] THE “BRING YOUR OWN DEVICE” TO WORK MOVEMENT:
Engineering Practical Employment and Labor Law Compliance Solutions https://www.littler.com/files/press/pdf/TheLittlerReport-TheBringYourOwnDeviceToWorkMovement.pdf
[56] https://www.professionalsecurity.co.uk/news/interviews/personal-device-survey/
[57] Ten pat.
[58] Ten pat.

Išvados

Apibendrinus šiuos tyrimus, galima daryti šias išvadas: asmeninių prietaisų naudojimas darbo funkcijoms atlikti yra labai paplitęs reiškinys, ypač jaunesnių nei 24 metų amžiaus darbuotojų grupėje; toks paplitęs ir nevaldomas naudojimas sukelia didelę saugumo spragą visoje įmonės IT saugumo sistemoje; riba tarp asmeninio ir darbinio turinio tarsi išsitrina ir tai sukelia tiek pagrįstų baimių darbuotojų pusėje, tiek papildomų išlaidų darbdaviui; prognozuojama, kad ateityje darbuotojų besinaudojančių savo asmeniniu prietaisais darbo funkcijoms atlikti, tik didės.

Kaip rasti balansą tarp saugumo, patogumo ir privatumo

Atsižvelgiant į šias prognozes ir tendencijas, pagrindiniai uždaviniai, kuriuos turi išspręsti darbdavys analizuojantis klausimą, ar leisti naudoti asmeninius prietaisus darbo funkcijoms atlikti yra šie: kaip užtikrinti informacijos saugumą, kaip nepažeisti įmonės konfidencialumo įsipareigojimų, kaip nepažeisti darbuotojo teisės į privatų gyvenimą ir kartu kaip pasiūlyti patogų bei šiuolaikišką būdą savo darbuotojams nebūnant stacionarioje darbo vietoje atlikti darbines funkcijas – laiku atsakyti į elektroninius laiškus, skambučius, persiųsti svarbią informaciją. Iš pirmo žvilgsnio sunkiai suderinami dalykai, tokie kaip patogumas, saugumas ir privatumas, užsienio šalių praktikoje visgi yra derinami pasitelkiant jau minėtą BYOD (*angl*. Bring your own device) politiką. Šio dokumento esmė – iš vienos pusės, aiškiai apibrėžti darbdavio lūkesčius, informuoti apie grėsmes ir darbuotojo atsakomybę, naudojant asmeninius prietaisus darbo funkcijoms atlikti. Iš kitos – nustatyti darbdavio įsipareigojimus papildomai skirti lėšų saugumo programėlių instaliavimui, mokymams, įmonės konfidencialios informacijos apsaugai bei kompensacijai už telekomunikacinių ryšių naudojimą. Kalbant apie darbuotoją, šiame dokumente, iš vienos pusės galima apibrėžti laisvę pasirinkti dirbti patogiau naudojant savo asmeninį prietaisą, iš kitos – nustatyti įsipareigojimus atriboti privačią informaciją nuo darbinės, laiku atnaujinti operacinę sistemą, informuoti apie prarastą įrenginį, leisti darbdaviui patikrinti, ar teisingai laikomasi saugumo reikalavimų, bei susitarti, kokiomis sąlygomis bus patikrinama įrenginyje esanti darbdavio informacija. Toks vidinis dokumentas, tikrai nėra pajėgus vienas užkardyti visas grėsmes, kurias sukelia asmeninių prietaisų naudojimas, tačiau derinant kartu su atitinkamomis techninėmis saugumo priemonėmis, jis tikrai gali įnešti aiškumo, disciplinos ir pagelbėti, kai prireikia laviruoti tarp darbuotojo teisės į privatumą ir darbdaviui priklausančios informacijos apsaugos.

Rengiant šią politiką pravartu atsižvelgti į Nacionalinio kibernetinio centro rekomendacijas: *"Jeigu Jūsų įmonės darbuotojai turi galimybę dirbti nuotoliniu būdu ir tam naudoja savo asmeninius kompiuterius, apsvarstykite galimybę įsigyti verslo naudojamos antivirusinės programos kopiją arba reikalaukite, kad*

darbuotojai įdiegtų saugią antivirusinę programą į asmeninius prietaisus.[59] *Rekomenduojama riboti darbuotojų prieigą prie socialinių tinklų ir asmeninių el. pašto dėžučių, jei to nereikia darbo funkcijoms atlikti. Taip mažinama rizika, kad Jūsų įmonės darbuotojas susidurs su sukčiavimu ir galimai apkrės įmonės kompiuterį ir tinklą."*[60]

Literatūroje vyraujanti nuomonė yra tokia, kad asmeninių prietaisų naudojimas darbui ateityje tik didės, nes taip yra ne tik patogiau pačiam darbuotojui, tačiau ir darbdaviui, kuris turi galimybę sutaupyti bei padidinti darbo efektyvumą. Be to, nustatyta, kad jaunesnioji karta darbuotojų yra kur kas labiau priklausoma nuo savo išmaniųjų įrenginių ir dažnu atveju draudimas naudotis savo prietaisu atlikti darbą nuotoliniu būdu, jiems yra sunkiai suprantamas. Dėl šių priežasčių taps neišvengiama asmeninių prietaisų naudojimo darbe klausimą kelti vis dažniau ir, atsižvelgus į visus argumentus „už" ir „prieš", priimti sprendimą, kuris idealiu atveju užtikrins įmonės informacijos saugumą ir konfidencialumą, leis veiksmingai atskirti privačią erdvę nuo darbinės bei bus toks patogus, kad skatins darbuotojus nenumoti rankas į savo ir įmonės duomenų saugumą.

[59] Kibernetinis saugumas ir verslas: ką turėtų žinoti kiekvienas įmonės vadovas 2020: Nacionalinis kibernetinio saugumo centras, 2020 m. 38 p.
[60] Kibernetinis saugumas ir verslas: ką turėtų žinoti kiekvienas įmonės vadovas 2020: Nacionalinis kibernetinio saugumo centras, 2020 m. 38 p.

SU RINKIMAIS SUSIJUSIŲ ASMENS DUOMENŲ APSAUGOS EUROPOS SĄJUNGAI PRIKLAUSANČIOSE BALTIJOS JŪROS REGIONO VALSTYBĖSE YPATUMAI

Dr. Andrius Puksas
Mykolo Romerio universiteto Teisės ir viešųjų pirkimų tarnybos vadovas, Lietuvos Respublikos vyriausiosios rinkimų komisijos pirmininko pavaduotojas

Rokas Stabingis
Lietuvos Respublikos vyriausiosios rinkimų komisijos duomenų apsaugos pareigūnas

Santrauka

Su rinkimais susijusių duomenų rinkimas susijęs su viešojo intereso įgyvendinimu. Nuoroda į viešąjį interesą neprieštarauja BDAR įtvirtintiems principams, tačiau duomenų saugojimo 'tiek, kiek reikia' ribos gali būti platesnės. Renkami, apdorojami ir saugomi piliečių duomenys leidžia užtikrinti rinkėjų konstitucines teises bei sudaro prielaidas įgyvendinti jiems nustatytas pareigas, o kartu sukuria ir pareigas tokių duomenų valdytojams bei tvarkytojams užtikrinti aukštus duomenų apsaugos standartus ir įpareigoja saugomus duomenis naudoti tik pagal paskirtį. Kiekviena ES valstybė narė iš esmės dirba su panašiais duomenimis. Tiesa, skiriasi renkamų, apdorojamų ir saugomų asmens duomenų apimtys. Šiame straipsnyje nagrinėjami su rinkimais susijusių duomenų rinkimo, apdorojimo ir saugojimo ypatumai. Juo siekiama įvertinti ES priklausančių Baltijos jūros regiono valstybių (Estijos, Danijos, Latvijos, Lenkijos, Lietuvos, Suomijos, Švedijos ir Vokietijos) praktiką bei nustatytus standartus dirbant su šiais duomenimis.

Raktiniai žodžiai: duomenų apsauga, rinkimai, referendumai, politika.

Įžanga

Europos Sąjungos pagrindinių teisių chartijoje, Sutartyje dėl Europos Sąjungos veikimo bei kituose tarptautiniuose ir nacionaliniuose teisės aktuose įvirtinta fizinių asmenų teisė į asmens duomenų apsaugą kartu su Bendrojo duomenų apsaugos reglamento (BDAR)[61] įsigaliojimu nuo 2018 m. gegužės 25 d. persikėlė į kokybiškai naują lygį. Tiesioginio taikymo BDAR panaikino 1995 m. priimtą ir ES valstybių narių į nacionalinius teisės aktus perkeltą direktyvą[62]. Nepaisant BDAR įtvirtintų universalių nuostatų, kiekviena atskira veiklos sritis pasižymi savo specifika. Su rinkimais ir jų įgyvendinimu susijusių duomenų rinkimas, apdorojimas ir saugojimas nėra išimtis. Atsižvelgiant į tai, jog rinkimuose dalyvauja platus teisės aktuose nustatyto amžiaus cenzo sulaukęs asmenų ratas, kiekvienos valstybės renkamų, apdorojamų ir saugomų duomenų mastas yra didelis.

Renkami, apdorojami ir saugomi piliečių duomenys leidžia užtikrinti šių asmenų konstitucines teises bei sudaro prielaidas įgyvendinti jiems nustatytas pareigas, o kartu sukuria ir pareigas tokių duomenų valdytojams bei tvarkytojams užtikrinti aukštus duomenų apsaugos standartus ir įpareigoja saugomus duomenis naudoti tik pagal paskirtį.

Su rinkimais susijusių duomenų rinkimas susijęs su viešojo intereso įgyvendinimu. Nuoroda į viešąjį interesą neprieštarauja BDAR įtvirtintiems principams, tačiau duomenų saugojimo 'tiek, kiek reikia' ribos gali būti platesnės.

Šiame straipsnyje nagrinėjami su rinkimais susijusių duomenų rinkimo, apdorojimo ir saugojimo ypatumai. Juo siekiama įvertinti ES priklausančių Baltijos jūros regiono valstybių (Estijos, Danijos, Latvijos, Lenkijos, Lietuvos, Suomijos, Švedijos ir Vokietijos) praktiką bei nustatytus standartus dirbant su šiais duomenimis.

Renkamų, apdorojamų ir saugomų su rinkimais susijusių duomenų mastas bei rinkimų rezultatų svarba kelia eilę potencialių grėsmių – nuo neteisėtos prieigos prie duomenų iki kibernetinių atakų. Todėl aktualų įvertinti kaip ES priklausančios Baltijos jūros regiono valstybės (Estija, Danija, Latvija, Lenkija, Lietuva, Suomija, Švedija ir Vokietija) pasiruošusios užtikrinti tokių duomenų saugumą.

Atsižvelgiant į šiame straipsnyje nagrinėjamą objektą, toliau pateikiama medžiaga apima ir asmens duomenis, naudojamus referendumams įgyvendinti.

---

[61] Europos Parlamento ir Tarybos 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). L 119/1.

[62] Europos Parlamento ir Tarybos direktyva (95/46/EB) dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo. L 281.

Su rinkimais susijusių asmens duomenų apsaugos ypatumai

Nepaisant įtvirtinto pilietinės pareigos atlikimo griežtumo lygio (pvz. privalomas ar neprivalomas dalyvavimas rinkimuose), kiekviena ES valstybė narė iš esmės dirba su panašiais duomenimis. Tiesa, skiriasi renkamų, apdorojamų ir saugomų asmens duomenų apimtys. BDAR numato galimybę rinkti duomenis apie asmenų politines pažiūras: „*kai, vykstant rinkimams, demokratinės sistemos veikimui valstybėje narėje užtikrinti būtina, kad politinės partijos surinktų asmens duomenis apie asmenų politines pažiūras, dėl viešojo intereso priežasčių gali būti leista tvarkyti tokius duomenis su sąlyga, kad yra nustatytos tinkamos apsaugos priemonės*".

Saugomų duomenų mastas ir subjektų skaičius kelia ir papildomas rizikas dėl šių duomenų saugumo ir duomenų tvarkytojų bei valdytojų gebėjimo užtikrinti tinkama asmens duomenų apsaugos lygį. Prie su rinkimais susijusių duomenų tinkamos apsaugos klausimų grįžtama periodiškai, pvz. 2005 m. Rezoliucijoje dėl asmens duomenų naudojimo politinei komunikacijai[63] numatyta, kad vykdant bet kokią su asmens duomenų tvarkymu susijusią politinės komunikacijos veiklą, įskaitant ir nesusijusią su rinkimų kampanijomis, turi būti gerbiamos asmenų teisės ir laisvės bei laikomasi duomenų apsaugos principų. 2018 m. pasirodė Europos duomenų apsaugos priežiūros pareigūno nuomonė Dėl manipuliacijų internete ir asmens duomenų[64], kurioje pastebima, kad „*problemos priežastis iš dalies yra neatsakingas, neteisėtas ar neetiškas naudojimasis asmenine informacija. Skaidrumas būtinas, bet nepakankamas. Turinio valdymas gali būti būtinas, tačiau negalima leisti, kad būtų pažeistos pagrindinės teisės. Iš dalies sprendimu būtų griežtas galiojančių taisyklių, ypač BDAR kartu su rinkimų ir žiniasklaidos pliuralizmų normų taikymas.*"

Riziką kelia ir potencialios duomenų vagystės, ir įvairaus pobūdžio kibernetinės atakos. Neapsaugoti ar silpnai apsaugoti duomenys gali būti panaudoti kaip rinkimų rezultatams paveikti, taip ir kitiems su rinkimais nesusijusiems tikslams (tokios duomenų bazės potencialiai patrauklios dėl saugomų duomenų masto). Poveikis rinkimų rezultatams neišvengiamai turėtų rimtų pasekmių.

Atkreiptinas dėmesys, kad aukštas asmens duomenų apsaugos lygis turi būti užtikrintas ir institucijoms besikeičiant informacija – prieiga prie įvairiuose registruose (pvz. nacionaliniai gyventojų registrai) esančių duomenų, taip pat

---

[63] Resolution on the Use of Personal Data for Political Communication – Montreux (Switzerland), 14-16 September, 2005.

[64] European Data Protection Supervisors' Opinion No 3/2018 On online manipulation and personal data (lt. Europos duomenų apsaugos priežiūros pareigūno nuomonė Nr. 3 /2018 Dėl manipuliacijų internete ir asmens duomenų).

tokių duomenų perdavimas turi būti saugus. Taip pat turi būti numatyti scenarijai galimų kibernetinių atakų ar kitokio pobūdžio duomenų praradimo ar nutekėjimo atvejams spręsti.
2018 m. Lietuvos Respublikos Seimo kanceliarijos buvo atliktas tyrimas, kuriuo siekta nustatyti kaip ES valstybėse narės reglamentuojama kandidatų asmens duomenų saugojimo ir viešinimo trukmė[65]. Nustatyta, kad dalyje iš 13 apžvelgtų valstybių kandidatų asmens duomenų trukmė nebuvo numatyta, o dalyje nustatytas konkretus terminas.
Atsakingų institucijų renkami, apdorojami bei saugomi skirtingoms asmenų grupėms priklausantys asmens duomenys, iš kurių dalis priskirtina jautresniems duomenims, taip pat dirbama su duomenimis, apimančiais skirtingas asmenų kategorijas (rinkėjus, kandidatus ir k.t.). Akivaizdu, jog po kurio laiko dalies tokių duomenų saugojimo tikslingumą pateisinti sunku. Vienas iš rimtesnių iššūkių – skirtingoms asmens duomenų kategorijoms numatyti tokius saugojimo terminus, kad tai tenkintų ir viešąjį interesą, ir atitiktų BDAR numatytus principus.

ES priklausančių Baltijos jūros regiono valstybių praktika

2018 m. gegužės 25 d. įsigaliojus naujajam BDAR pirmieji Europos Parlamento rinkimai vyko jau 2019 metais. Siekiant tinkamai pasiruošti jiems ir vėliau vyksiantiems rinkimams buvo parengtos atitinkamos rekomendacijos – Komisijos gairės dėl Sąjungos duomenų apsaugos teisės aktų taikymo rinkimams[66] (toliau – Gairės). Gairėse atkreipiamas dėmesys, kad rinkimų metu dažnai tvarkomi neskelbtini duomenys (pvz. politinės pažiūros, etninė kilmė ir pan.), o rinkimų metu BDAR iš esmės taikomas visoms duomenų tvarkymo operacijoms. Atsižvelgiant į galimą su rinkimais susijusių pažeidimų rimtumą ir potencialiai didelį nukentėjusių asmenų skaičių, didelės baudos turėtų būti laikomos proporcinga priemone. Taip pat siūloma atsižvengti ir į piliečių pasitikėjimo demokratijos procesu klausimo svarbą.
Po Europos Parlamento rinkimų buvo parengta ataskaita[67] (toliau – Ataskaita), kurios dalį sudarė ir nacionalinių duomenų apsaugos institucijų atsakymai į Europos Komisijos pateiktus klausimus. Minėtoje ataskaitoje atkreiptas

[65] Kandidatų į valstybės politikus asmens duomenų saugojimo ir viešinimo terminai Europos Sąjungos valstybėse. Analitinė apžvalga (2018 m. rugsėjo 19 d.) Lietuvos Respublikos Seimo kanceliarijos Informacijos ir komunikacijos departamento tyrimo skyrius, 18/73.
[66] Komisijos gairės dėl Sąjungos duomenų apsaugos teisės aktų taikymo rinkimams. Komisijos gairės dėl Sąjungos duomenų apsaugos teisės aktų taikymo rinkimams. COM(2018) 638 final.
[67] Komisijos komunikatas Europos Parlamentui, Tarybai ir Europos Ekonomikos ir socialinių reikalų komitetui. 2019 m. Europos Parlamento rinkimų ataskaita {SWD(2020) 113 final}. COM(2020) 252 final.

dėmesys, kad į tinklo veiklą jau įsitraukė pusė nacionalinių duomenų apsaugos institucijų. Iš vienos pusės toks įsitraukimas sveikintinas, iš kitos stebina kitos dalies pasyvumas. Iš esmės 2019 m. Europos Parlamento rinkimai praėjo sklandžiai, tačiau Ataskaitoje atkreiptas dėmesys ir į rizikas: *„Pranešta apie pavienius kibernetinius išpuolius, duomenų apsaugos ir kitas su rinkimais susijusias problemas, tačiau nenustatyta jokių slaptų koordinuotų didelio masto pastangų kištis į rinkimus".*

Estijos Respublikos praktika

Nuo 2008 m. sausio 1 d. galiojantis Estijos Respublikos asmens duomenų apsaugos aktas[68] iš esmės atspindi BDAR ir nustato bendruosius asmens duomenų apsaugos reikalavimus. Jį papildo 2000 m. lapkričio 15 d. priimtas Viešosios informacijos aktas[69], reglamentuojantis su teise į informaciją susijusius klausimus.

Estijos nacionalinis rinkimų komitetas savo interneto svetainėje[70] yra paskelbęs savo asmens duomenų tvarkymo politiką, kurioje numatyti visi asmens duomenų tvarkymo atvejai:

– kandidatų duomenys: skelbiami rinkimų interneto svetainėje;

– lankantis rinkimų interneto svetainėje: renkamas ir saugomas interneto IP adresas, interneto tiekėjo adresas ir pavadinimas, prisijungimo data ir laikas. Statistinė informacija apie internetinio puslapio lankymą;

– siunčiant dokumentą Estijos nacionaliniam rinkimų komitetui: dokumentas registruojamas dokumentų registre;

– kreipiantis dėl darbo ar stažuotės: kandidatų kreipimasis nėra registruojamas dokumentų registre, tačiau informacija apie asmens įdarbinimo ar stažuotės faktą yra vieša. Nelaimėjusių kandidatų duomenys saugomi vienerius metus;

– sutartys su fiziniais asmenimis: informacijos apie asmens duomenis gali prašyti tik pats duomenų subjektas;

– apsilankymas Estijos nacionaliniame rinkimų komitete ir dalyvavimas renginiuose: renginių dalyviai gali būti filmuojami ir fotografuojami, apie renginius informuojama per socialinius tinklus;

– viešieji pirkimai: asmens duomenys gali būti pateikiami vykdant viešųjų pirkimų procedūras.

Estijos Parlamento (Riigikogu) rinkimų akto[71] 28 straipsnis numato, kokie duomenys yra skelbiami apie kandidatus: vardas, pavardė; asmens kodas;

---

[68] Isikuandmete kaitse seadus (Vastu võetud 15.02.2007). Prieiga internetu: https://www.riigiteataja.ee/akt/12802623

[69] Avaliku teabe seadus. Prieiga internetu: https://www.riigiteataja.ee/akt/115032019011?leiaKehtiv

[70] Riigi valimisteenistuse andmekaitsetingimused. Prieiga internetu: https://www.valimised.ee/et/andmekaitsetingimused

[71] Riigikogu Election Act. Prieiga internetu: https://www.riigiteataja.ee/en/eli/ee/514112013015/consolide/current

narystė politinėje partijoje; adresas; telefono numeris; informacija apie išsilavinimą; darbas ir pareigos.
Šią informaciją, išskyrus asmens kodą, adresą ir kontaktinę informaciją, Estijos nacionalinis rinkimų komitetas paskelbia viešai. Panašias nuostatas galima rasti ir kituose rinkimų įstatymuose[72]. Rinkimų įstatymai reglamentuoja skelbiamų duomenų apie kandidatus apimtį. Šių duomenų skelbimas reglamentuojamas Estijos nacionalinio rinkimų komiteto asmens duomenų tvarkymo politikoje.

Danijos Karalystės praktika

2018 m. gegužės 23 d. priimtas Danijos Karalystės duomenų apsaugos aktas[73] numato išimtis iš BDAR. Viena iš tokių išimčių yra netaikyti BDAR tam tikroms informacinių technologijų sistemoms, kurias administruoja viešosios valdžios institucijos ir kurios saugomos tik Danijos Karalystėje. Ši išimtis galima tik tada, kai tai nustato Teisingumo ministerija. Danija, priimdama minėtą aktą, numato nemažai išimčių arba pasilieka teisę tokias išimtis numatyti Teisingumo ministerijos sprendimais. Duomenų apsaugos akte taip pat reglamentuojama Duomenų apsaugos agentūros sudarymo tvarka ir veikla.
Parlamento rinkimų akte[74] numatyta, kad kandidatai paraiškos formą turi pateikti Socialinių reikalų ir vidaus ministerijai. Paraiška turi būti pasirašyta ir joje turi būti ši informacija: kandidato pilnas vardas, pavardė, socialinio draudimo numeris, darbovietė, adresas. Taip pat kandidatas gali nurodyti savo kontaktus arba kontaktinį asmenį. Minėtas įstatymas nustato, kad su rinkimais susijusią medžiagą saugo savivaldybė. Balsavimo dokumentus savivaldybė sunaikina pasibaigus teisminių ginčų terminams, o kita rinkimų medžiaga perduodama saugoti pagal Viešųjų archyvų aktą.
Danijos statistikos departamentas savo interneto svetainėje[75] skelbia informaciją apie kandidatus. Pavyzdžiui, kandidatų į Danijos parlamentą (Folketingą) xls formatu skelbiami šie asmens duomenys: vardas, pavardė, profesija, lytis, amžius, savivaldybė.

Latvijos Respublikos praktika

Nuo 2018 m. liepos 5 d. galiojantis Latvijos Respublikos asmens duomenų tvarkymo įstatymas[76] iš esmės reglamentuoja Valstybinės duomenų

[72] Žr. Estijos Respublikos savivaldybių tarybų rinkimų akto 33 straipsnį. Prieiga internetu: https://www.riigiteataja.ee/en/eli/506112013004/consolide/current.
[73] Act on supplementary provisions to the regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the Data Protection Act). Prieiga internetu: https://www.datatilsynet.dk/media/7753/danish-data-protection-act.pdf
[74] Bekendtgørelse af lov om valg til Folketinget. Prieiga internetu: https://www.retsinformation.dk/eli/lta/2020/1260
[75] Prieiga internetu: http://dst.dk/valg/Valg1684447/other/startside.htm
[76] Fizisko personu datu apstrādes likums. Prieiga internetu: https://likumi.lv/ta/id/300099-fizisko-personu-datu-apstrades-likums

inspekcijos vaidmenį duomenų tvarkymo procese bei duomenų tvarkymo kontrolės procedūras ir jokių asmens duomenų tvarkymo terminų nenustato. Minėto įstatymo 28 straipsnis numato duomenų tvarkymą oficialiuose leidiniuose. Tokie duomenys gali būti ištrinti Valstybinės duomenų inspekcijos sprendimu arba duomenų tvarkytojo sprendimu, jeigu tokie duomenys neatitinka teisinių reikalavimų. Valstybinė duomenų inspekcija gali priimti sprendimą ištrinti duomenis iš oficialaus leidinio, jeigu duomenų subjekto teisė į privatumą yra svarbesnė negu viešasis interesas.

Latvijos Parlamento (Saeimos) rinkimų įstatymas numato kad kartu su kandidatų sąrašu kiekvienas kandidatas turi pateikti pareiškimą, kuriame jis/ji sutinka su tuo, kad, kad jo/jos kandidatūra būtų keliama, taip pat dėl duomenų tvarkymo pagal minėtą įstatymą. Kandidatuodamas kandidatas taip pat turi pateikti šią informaciją apie save[77]: vardas, pavardė, gimimo metai, lytis, tautybė, šeiminė padėtis; asmens kodas; užsienio pilietybės, jei turi; adresas (miestas ar regionas); darbas ir pareigos (įskaitant politines partijas, religines organizacijas, profesines sąjungas, asociacijas ir fondus), o jeigu nedirba – užsiėmimas, statusas; išsilavinimo įstaiga, baigimo metai, išsilavinimo lygis ir specialybė; bendradarbiavimo su SSSR, Latvijos SSR ar kitos užsienio šalies saugumo, žvalgybos tarnybomis kaip laisvai samdomo asmens, agento, slapto buto turėtojo faktas; informacija numatyta Valstybės pareigūnų privačių interesų prevencijos įstatyme.

Aukščiau nurodyta informacija, išskyrus asmens kodą, skelbiama 20 dienų iki rinkimų oficialiame dienraštyje „Latvijas Vēstnesis".

Europos Parlamento rinkimų įstatymas[78] reikalauja nurodyti panašius duomenis kaip ir Latvijos Parlemento (Saeimos) rinkimų įstatyme, tačiau papildomai reikalauja nurodyti Europos Sąjungos pilietybę ne Latvijos piliečiams bei paskutinį gyvenamosios vietos adresą ir gimimo vietą. Neprivalomi duomenys pagal šį įstatymą yra pareigos asociacijose, profesinėse sąjungose, politinėse partijose ir religinėse organizacijose; šeiminė padėtis; kalbų mokėjimas. Informacija skelbiama 19 dienų iki rinkimų oficialiame dienraštyje „Latvijas Vēstnesis" ir Centrinės rinkimų komisijos interneto svetainėje.

Pagal Latvijos Respublikos miestų ir savivaldybių tarybų rinkimų įstatymą[79], kandidatai nurodo jau aukščiau minėtuose įstatymuose nurodytus duomenis. Kandidatų sąrašai skelbiami „Latvijas Vēstnesis", Centrinės rinkimų komisijos interneto svetainėje, taip pat atitinkamų administracinių vienetų rinkimų apylinkėse.

---

[77] Žr. Latvijos Parlamento (Saeimos) rinkimų įstatymo 11 straipsnio 4 dalį. Prieiga internetu: https://likumi.lv/doc.php?id=35261

[78] Eiropas Parlamenta vēlēšanu likums. Prieiga internetu: https://likumi.lv/doc.php?id=84185

[79] Republikas pilsētas domes un novada domes vēlēšanu likums. Prieiga internetu: http://likumi.lv/ta/id/57839-republikas-pilsetas-domes-un-novada-domes-velesanu-likums

Latvijos centrinės rinkimų komisijos 2014 m. gegužės 22 d. sprendime Nr. 48[80] „Dėl kandidatų asmens duomenų Centrinės rinkimų komisijos interneto svetainėje“ numatyta, kad kandidatų į Latvijos Parlamentą (Saeimą), Europos Parlamentą, savivaldybių tarybas asmens duomenys skelbiami tik pareigų ėjimo laikotarpiu, o vėliau skelbiama tik vardas ir pavardė.
Rinkimų įstatymai reglamentuoja skelbiamų asmens duomenų apie kandidatus apimtį, tačiau jų skelbimo terminai ir skelbimo būdas gali skirtis priklausomai nuo rinkimų įstatymo.

Lenkijos Respublikos praktika

2018 m. gegužės 10 d. priimtas Lenkijos Respublikos asmens duomenų apsaugos įstatymas[81] reglamentuoja procedūrinius asmens duomenų apsaugos klausimus tokius kaip asmens duomenų pareigūno paskyrimas, institucijos, atsakingos už duomenų apsaugą, jų veikla, atsakomybė už asmens duomenų reikalavimų pažeidimą.
Lenkijos Respublikos rinkimų kodekso[82] 212 straipsnyje numatyta kokius duomenis reikia pateikti kandidatams į Seimo rinkimuose: vardas, pavardė, profesija, gyvenamoji vieta. Prie kandidatų sąrašų taip pat pridedama rašytinis kandidatų sutikimas būti kandidatu su šiais duomenimis: vardas, pavardė, tėvų vardai, pavardės, data ir vieta, adresas, pilietybė, identifikacinis kodas (PESEL), priklausymas politinei partijai, taip pat informacija apie priklausymą saugumo organams 1944-1990 metais tiems kandidatams, kurie gimė iki 1972 m. rugpjūčio 1 d.
Kandidatų duomenų paskelbimo būdų Lenkijos Respublikos rinkimų kodeksas nereglamentuoja, tačiau jie yra skelbiami Valstybinės rinkimų komisijos svetainėje https://pkw.gov.pl/, kurioje skelbiama kandidato vardas, pavardė, profesija, darbovietė, gimimo vieta, išsilavinimas, amžius, iškėlusi partija.

Lietuvos Respublikos praktika

Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas[83] rinkimuose tvarkomų asmens duomenų nemini, todėl yra taikomas kaip

[80] Lēmums Nr. 48 Par deputātu kandidātu personas datiem Centrālās vēlēšanu komisijas mājaslapā. Prieiga internetu: https://www.cvk.lv/lv/tiesibu-akti/lemumi/2014-gads/nr-48-par-deputatu-kandidatu-personas-datiem-centralas-velesanu-komisijas-majaslapa
[81] Uztawa o ochronie danych osobowych. Prieiga internetu: https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001000/U/D20181000Lj.pdf
[82] Kodeks wyborczy. Prieiga internetu: https://pkw.gov.pl/uploaded_files/1588806909_kodeks-wyborczy-2020-maj.pdf
[83] Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas. Prieiga internetu: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.29193/asr

bendrasis teisės aktas kartu su specialiaisiais teisės aktais laikomais rinkimų įstatymais.

Vadovaujantis Lietuvos Respublikos Seimo rinkimų įstatymu[84], kandidatai turi pateikti kandidato į Seimo narius anketą, gyventojų pajamų mokesčio ir gyventojų turto deklaracijų pagrindinių duomenų išrašus, kandidato privačių interesų deklaraciją, biografiją, kandidato fotonuotrauką. Kandidato į Seimo narius anketoje nurodoma: socialinių tinklų paskyra, pareigos, narystė partijoje, asociacijoje, duomenys apie pilietybę, turėtą teistumą, bendradarbiavimą su specialiosiomis tarnybomis ir pan. Kandidato biografijoje asmuo nurodo: gimimo datą, tautybę, išsilavinimą, darbo patirtį, duomenis apie mokslinę ir pedagoginę veiką, pomėgius, duomenis apie šeimą ir kita. Gyventojų pajamų mokesčio deklaracijos išraše nurodyta už praeitą deklaravimo laikotarpį deklaruota apmokestinamųjų ir neapmokestinamųjų pajamų suma, deklaruota mokėtina pajamų mokesčio suma ir kiti duomenys. Gyventojo turto deklaracijoje nurodytos atskirų turto rūšių vertės. Privačių interesų deklaracijoje nurodyti ryšiais su fiziniais ir juridiniais asmenimis, sandoriai, gautos dovanos ir kiti duomenys, sukeliantys interesų konfliktą. Šie duomenys skelbiami Lietuvos Respublikos vyriausiosios rinkimų komisijos interneto svetainėje www.vrk.lt. Taip pat kartu yra skelbiami politinės kampanijos dalyvio duomenys: apie politinės kampanijos iždininką, aukotojus ir aukas, sandorius, finansavimo ataskaitas, auditą. Duomenų skelbimo terminai yra nustatyti Lietuvos Respublikos vyriausiosios rinkimų komisijos 2019 m. vasario 7 d. sprendimu Nr. Sp-73 patvirtintame „Asmens duomenų tvarkymo Lietuvos Respublikos vyriausioje rinkimų komisijos tvarkos apraše“[85], kuris 2021 m. rugsėjo 30 d. VRK sprendimu Nr. Sp-230 buvo pakeistas atsižvelgiant į naujus rinkimų įstatymų pakeitimus, kurie įsigaliojo 2022 m. sausio 1 d. ir kurie numato naujus asmens duomenų apsaugos reikalavimus per rinkimus. Nuo šios datos kandidatų pareiškiniai duomenys savivaldybių tarybų rinkimuose ir rinkimuose į Europos Parlamentą bus skelbiami tik dešimt metų, kai tuo tarpu Lietuvos Respublikos Seimo ir Respublikos Prezidento rinkimuose tokie duomenys bus skelbiami neterminuotai. Dar viena naujovė – tam tikra informacija apie kandidatą bus skelbiama tik rinkimų kampanijos metu: gimimo vieta, pilietybė, išsilavinimas, užsienio kalbų mokėjimas, pomėgiai, šeiminė padėtis, sutuoktinio ar sutuoktinės vardas (pavardė), vaikų vardai (pavardės), telefono numeris, elektroninio pašto adresas.

[84] Lietuvos Respublikos Seimo rinkimų įstatymas. Prieiga internetu: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.1536/asr

[85] Lietuvos Respublikos vyriausiosios rinkimų komisijos 2019 m. vasario 7 d. sprendimu Nr. Sp-73 patvirtinto „Asmens duomenų tvarkymo Lietuvos Respublikos vyriausioje rinkimų komisijos tvarkos aprašo“.

Suomijos Respublikos praktika

2018 m. gruodžio 5 d. priimtas Suomijos Respublikos duomenų apsaugos aktas (1050/2018)[86] numato priežiūros institucijos veiklos pagrindus. Duomenų apsaugos komisaras veikia prie Teisingumo ministerijos. Minėtas aktas nustato tam tikras asmens duomenų kategorijas, kurioms nėra taikomas minėtas aktas, pavyzdžiui, kai draudimo įmonės tvarko sveikatos duomenis arba kai duomenis yra tvarkomi pagal įstatymą arba duomenų tvarkytojas atlieka jam įstatymo pavestą užduotį.

Suomijos Respublikos rinkimų akto[87] 41 straipsnio 5 dalis nustato, kad kandidatų sąraše turi būti nurodytas kiekvieno kandidato numeris sąraše, vardas, užsiėmimas ar profesija, taip pat savivaldybė visuose rinkimuose, išskyrus savivaldos rinkimus. Bet kuri kita informacija apie kandidatą negali būti nurodoma, nebent reikėtų nustatyti kandidatų tapatybę. Asmens kodai kandidatų sąrašuose nėra nurodomi.

Teisingumo ministerija administruoja Nacionalinį kandidatų registrą, kuriame informacija nemokamai teikiama kandidatui, jį iškėlusiai partijai, taip pat valdžios institucijoms.

Informaciją apie rinkimus skelbiama Teisingumo ministerijos administruojamoje svetainėje https://vaalit.fi/etusivu, kurioje galima rasti duomenis apie visuose rinkimuose dalyvavusius kandidatus: numeris kandidatų sąraše, vardas, pavardė, užsiėmimas arba profesija, pavyzdžiui, studentas, verslininkas, bedarbis, taip pat gali būti nurodomas ir išsilavinimas, nes pagal įstatymą yra leidžiama nurodyti po dvi veiklas, gyvenamosios vietos savivaldybė. Duomenys šioje svetainėje skelbiami nuo 2003 m. rinkimų.

Švedijos Karalystės praktika

2018 m. balandžio 18 d. buvo priimtas Įstatymas dėl Europos Sąjungos duomenų apsaugos reguliavimo papildymo[88]. Minėtas teisės aktas reglamentuoja duomenų tvarkymo teisinius pagrindus, specialių kategorijų asmens duomenų tvarkymą, tokių kaip darbo, socialinės apsaugos, sveikatos apsaugos, viešąjį interesą turinčių duomenų, taip pat numato priežiūros institucijos sprendimų priėmimo procedūras.

---

[86] Tietosuojalaki 1050/2018. Prieiga internetu: https://www.finlex.fi/fi/laki/alkup/2018/20181050

[87] Election Act. Prieiga internetu: https://www.legislationline.org/download/id/7825/file/Finland_Election_Act_1998_am2016_en.pdf

[88] Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning. Prieiga internetu: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2018218-med-kompletterande-bestammelser_sfs-2018-218

Asmens duomenų tvarkymą rinkimų ir referendumų srityje Švedijos Karalystėje reguliuoja specialus įstatymas – Asmens duomenų tvarkymo rinkimuose ir referendumuose (2001:183) įstatymas[89]. Šis teisės aktas reglamentuoja kas yra duomenų valdytojai – Centrinė rinkimų komisija, Parlamentas, savivaldybių tarybos (6 straipsnis). Minėto įstatymo 2 skyrius reguliuoja rinkimų ir referendumų duomenų bazių, kuriose yra duomenys apie rinkėjus ir kandidatus, valdymą. Duomenų bazėse tvarkomi tokie duomenys: gimimo data, socialinio draudimo numeris, vardas, pavardė, adresas, registracijos vieta, turto pažymėjimas, rinkimų apygarda, pilietybė, imigracijos laikas.

Duomenų baze gali naudotis Centrinė rinkimų komisija, savivaldybių tarybos, taip pat asmuo, norintis gauti informaciją apie save. Įstatymas nenustato duomenų saugojimo terminų, tačiau, pavyzdžiui, nurodo, kad informacija duomenų bazėje negali būti ieškoma pagal požymį „pilietybė“, tačiau gali būti ieškoma pagal vardą, pavardę, socialinio draudimo numerį.

Išrinktų kandidatų duomenys skelbiami Centrinės rinkimų komisijos interneto svetainėje www.val.se, kurioje generuojamos ataskaitos xls formatu su kandidatų duomenimis, tokiais kaip vardas, pavardė, amžius, lytis, iškėlusi partija ir panašūs duomenys.

Vokietijos Federacinės Respublikos praktika

2017 m. birželio 30 d. priimtas Federalinis duomenų apsaugos įstatymas (BDSG)[90] reglamentuoja visų pirmiausia Federalinio duomenų apsaugos ir informacijos laisvės komisaro instituciją, jos sudarymą, teises ir pareigas, taip pat santykius su Žemių (*Länder)* duomenų apsaugos institucijomis.

Federalinio rinkimų kodekso (BWO)[91] 34 straipsnis numato, kokius duomenis turi pateikti kandidatuojantys asmenys: vardas, pavardė, profesija arba statusas, gimimo data, gimimo vieta ir adresas (gyvenamoji vieta). Šie duomenys vėliau yra paskelbiami viešai, tačiau vietoj pilnos gimimo datos skelbiami tik gimimo metai, taip pat gali būti neskelbiamas adresas (gyvenamoji vieta), jeigu nurodomas kitas adresas, kuriuo kandidatą galima rasti; vien tik pašto kodo nurodymas nėra pakankamas.

Kandidatų sąrašai publikuojami viešai. Federalinis rinkimų kodeksas numato, kad vieši pranešimai pagal šį kodeksą skelbiami oficialiame leidinyje, taip pat

[89] Lag (2001:183) om behandling av personuppgifter i verksamhet med val och folkomröstningar. Prieiga internetu: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2001183-om-behandling-av-personuppgifter-i_sfs-2001-183

[90] Federal Data Protection Act. Prieiga internetu: https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html#p0012

[91] Bundeswahlordnung (BWO). Prieiga internetu: http://www.gesetze-im-internet.de/bwo_1985/BJNR017690985.html#BJNR017690985BJNG000603377

internete. Kandidatų asmens duomenys turi būti nebeskelbiami internete 6 mėnesiai po rinkimų.
Kandidatai skelbiami interneto svetainėje https://www.bundeswahlleiter.de/, tačiau duomenų apie kandidatavusius kandidatus, pavyzdžiui 2019 m. Europos Parlamento rinkimuose, nėra, nes yra informacinis pranešimas, kad ši informacija nebeskelbiama.

Išvados

1. Baltijos valstybių Lietuvos, Latvijos, Estijos rinkimų įstatymai skelbia daugiau asmens duomenų apie kandidatus negu kitos tirtos valstybės. Neabejotinai Lietuva skelbia daugiausiai asmens duomenų apie kandidatus iš visų tyrinėtų valstybių.
2. Švedija, Suomija, Danija, Vokietija skelbia tik minimalų asmens duomenų rinkinį apie kandidatus. Vokietijoje šis rinkinys yra iš viso neprieinamas praėjus 6 mėnesiams po rinkimų.
3. Lietuva skelbia daug ne tik asmeninių, specialių kategorijų asmens duomenų (tautybė, narystė partijoje, kituose juridiniuose asmenyse), bet ir duomenų apie šeiminę padėtį, sutuoktinį, sugyventinį, vaikus, ko neskelbia nei viena iš tirtų valstybių, išskyrus Latviją. Laikytina, kad Lietuvoje, lyginant su kitomis valstybėmis, yra skelbiama per daug duomenų apie kandidatus. Kai kurie duomenys apie socialinę-ekonominę kandidato padėtį, tokie kaip turimas turtas, pajamos, gali diskriminuoti asmenį dėl turtinės padėties. Duomenys apie šeimą, jos narius gali pažeisti ir trečiųjų asmenų teisę į privatumą. Nuo 2022 m. sausio 1 d. įsigalioję rinkimų įstatymų pakeitimai vertintini teigiamai, kadangi apriboja jautrių duomenų skelbimą. Tačiau nepaisant to, skelbiamų duomenų kiekis išlieka labai didelis lyginant su kitomis regiono valstybėmis.
4. Asmens duomenų saugojimo tvarka ir terminai tirtų valstybių teisės aktuose nėra pakankamai reglamentuoti.

Siūlymai

Siūlytina mažinti Lietuvoje skelbiamų duomenų apimtį apie kandidatus, visų pirma atsisakant specialių kategorijų, socialinių-ekonominių (turto ir pajamų deklaracijų išrašai), duomenų apie privatų asmens gyvenimą (šeimyninė padėtis, šeimos nariai), nes tokių duomenų skelbimas gali pažeisti teisę į asmens privatumą.

BIOMETRIJOS PANAUDOJIMO ASMENS TAPATYBĖS IDENTIFIKAVIMUI ĮVAIROVĖ, GRĖSMĖS IR TEISINIS REGLAMENTAVIMAS

Virginija Poškaitienė
Direktorė „Intendo LT“, MB

Santrauka

Saugių ir patikimų metodų asmens identifikavimui poreikis pastoviai auga. Tačiau kiekviena nauja technologija, tame tarpe ir biometrinis identifikavimas, vienaip ar kitaip įtakoja fizinio asmens gyvenimą. Automatizuotos technologijos, taikomos žmogaus biometrinių savybių panaudojimui to asmens tapatumui nustatyti, kuria patogumą, lengvina ir greitina procesus ir, tuo pačiu, palaipsniui išstumia PIN kodų ar slaptažodžių naudojimą. Biometriniai duomenys gali būti patys įvairiausi, o plečiantis technologijoms, jų panaudojimas taip pat plečiasi.

Biometrinių sistemų darbas yra grindžiamas unikalių asmens biometrinių duomenų panaudojimu jo autentifikavimo arba identifikavimo tikslais. Tačiau, jei slaptažodžių asmuo gali susikurti kiek nori, tai biometrinių duomenų žmogus turi labai ribotą skaičių, todėl jų atskleidimas, nukopijavimas ar sunaikinimas yra grėsmė prarasti galimybę būti identifikuotu, o tai reiškia – prarasti savo tapatybę.

Biometrinių duomenų saugojimui duomenų bazių vis daugėja. Centralizuotose biometrinių duomenų bazėse surenkami, kaupiami ir tvarkomi didžiuliai kiekiai asmenų biometrinių duomenų. Tačiau nekontroliuojamas arba nepakankamai kontroliuojamas biometrinių duomenų rinkimas ir kaupimas duomenų bazėse gali kelti grėsmes fizinio asmens biometrinių duomenų apsaugai ir privatumui, jo teisėms ir laisvėms.

Raktažodžiai: Biometrija, biometriniai duomenys, autentifikavimas, identifikavimas, veido biometrija, piršto atspaudas, duomenų bazė

Įvadas

Saugių ir patikimų metodų asmens identifikavimui poreikis pastoviai auga. Šį poreikį skatina ir įvairūs įvykiai visame pasaulyje, pavyzdžiui teroro aktai ar išplitusi migracija, didelis kiekis įsimintinų ir dažnai besikeičiančių slaptažodžių, daugybė PIN kodų ar kitų priemonių vartotojo atpažinimui. Biometrinės sistemos asmens tapatybės nustatymo procese užima vis platesnį pritaikymą teisėsaugoje, informacinėse sistemose, sveikatos apsaugoje, finansų sektoriuje, įėjimo į ypatingo saugumo pastatus ir teritorijas apsaugos kontrolės sistemose ir daugelyje kitų sričių. Laikui bėgant atsiranda vis naujesnių technologijų, įgalinančių užfiksuoti, nuskaityti ar atpažinti vis daugiau žmogaus biometrinių duomenų. Tačiau kiekviena nauja technologija vienaip ar kitaip įtakoja fizinio asmens gyvenimą. Jos gali kurti patogumą, kontroliuoti, lengvinti ar greitinti procesus. Visų biometrinių sistemų darbas yra grindžiamas unikalių asmens biometrinių duomenų panaudojimu, t. y. fizinio asmens duomenų, kurie yra susiję su asmens išoriniais ar kūno požymiais, elgesiu ir psichologinėmis charakteristikomis. Tokių duomenų rinkimas ir naudojimas įvairiems visuomenės gyvenimo tikslams yra tiesiogiai susijęs su asmens pagrindinių teisių ir laisvių apsauga, kurias reglamentuoja atitinkami teisės aktai. Šie duomenys dažnai naudojami ne tik tapatybei nustatyti, bet ir papildomų identifikavimo ir / ar autentifikavimo programų sukūrimui[92]. Tuo pačiu metu duomenų bazėse surenkami, kaupiami ir tvarkomi didžiuliai kiekiai biometrinių duomenų. Atitinkamai kyla grėsmės dėl tokių aspektų, kaip nekontroliuojamas biometrinių duomenų rinkimas ir kaupimas duomenų bazėse, kas turi teisę tokias duomenų bazes kaupti ar administruoti, kaip duomenų bazės ir jose tvarkomi biometriniai duomenys yra ar turi būti apsaugoti ir pan.

[92] Olga Trukšina, Raimondas Vasiliauskas. *Asmens biometrinių duomenų panaudojimo, nustatant tapatybę biometriniais metodais, teisinio reglamentavimo analizė lietuvos respublikoje*. Visuomenės saugumas ir viešoji tvarka. Mokslinių straipsnių rinkinys. 2014 (12). https://repository.mruni.eu/bitstream/handle/007/15124/Truk%C5%A1ina.pdf?sequence=1&isAllowed=y, [Žiūrėta 2020.10.15.]

Šio straipsnio tikslas yra atskleisti kas yra biometrija, kokios yra biometrinių duomenų savybės, kokie yra ir bei kokiems tikslams gali būti panaudojami asmens biometriniai duomenys, kokie privalumai skatina biometrinių duomenų panaudojimo plėtrą bei kokios grėsmės gali kilti fiziniam asmeniui, jei šiai plėtrai nebus skiriamas pakankamas dėmesys šalies teisinėje bazėje. Straipsnyje neliečiami biometrinių asmens duomenų tvarkymo teisėtumo kriterijai.

Iki šiol didžioji dauguma biometrinių duomenų renkama ir saugoma valstybinės reikšmės duomenų bazėse, pavyzdžiui gyventojų nuotraukos, pirštų atspaudai. Tačiau nemažai duomenų jau renka ir verslas. Šiandien jau dažnas iš mūsų net nesusimąstydami naudojamės veido atpažinimo programa išmaniojo telefono atrakinimui, piršto atspaudu kompiuterio ar mobilaus telefono prieigai, pulsometru ar balso naudojimo funkcija išmaniajame laikrodyje ir pan., ir visa tai, ką pateikiame šioms programėlėms, yra mūsų unikalūs biometriniai duomenys.

Temos aktualumą lemia asmens identifikacijos reikšmingumo augimas visame pasaulyje, o asmens identifikavimas panaudojant unikalius ir praktiškai nesikartojančius biometrinius asmens tapatybės bruožus yra viena iš priemonių, leidžiančių greitai, tiksliai ir efektyviai nustatyti asmens tapatybę. Tačiau šalia patogumo biometrinių duomenų naudojimui neatsiejamai kartu seka tema – ar toks naudojimas saugus ir kaip jis gali įtakoti asmens privatų gyvenimą, ar gali apriboti jo teises ir laisves. Visgi, šių laikų didžiausia užduotis - kaip apsaugoti biometrinius duomenis, kurie, jei bus pažeisti, nebebus atstatomi ar naujai sukuriami, kaip kad PIN kodas, asmens dokumentas ar susikurtas slaptažodis.

Biometrinių duomenų naudojimo aspektai

Tarp XIX ir XX amžiaus tam, kad įsitikinti kas yra vienas ar kitas asmuo užtekdavo tik žodinio patvirtinimo. XX -o amžiaus antroje pusėje žmogus jau buvo identifikuojamas pagal valstybės institucijų jam išduotą dokumentą. Tuo tarpu, kaip priemonė arba įrankis asmens identifikavimui ilgą laiką buvo tik

žmogaus akis. Kontrolę atliekantis asmuo žiūri į tikrinamo žmogaus veidą ir į jo fotografiją ant pateikto indentifikavimo dokumento, ir tuomet lygina ar asmuo, kurį mato nuotraukoje yra tas pats asmuo, kuris stovi prieš jį. Kadangi asmens tapatybės kortelė priklauso tam asmeniui, tai kortelėje esantis numeris ir kiti duomenys taip pat turėtų priklausyti tam pačiam asmeniui. Taigi, asmens vardas ir numeris lyg ir yra patikrinti ir patvirtinti. Žmogaus akis yra gana puikus „prietaisas" palyginimo procesui, tačiau prastas – absoliučiam matavimo procesui ar greitam ir tiksliam asmens identifikavimui pasinaudojant tokiais biometriniais duomenimis, kaip pirštų atspaudai ir žmogaus kūno išmatavimai. Žmogaus akis gali greitai ir tiksliai palyginti žmogaus veido atvaizdą su jo nuotrauka, tačiau, jei reikėtų greitai palyginti žmogaus piršto atspaudą ant kortelės su žmogaus realaus piršto rievelėmis, patirtų nesėkmę[93].

Šiandien jau tapo įprasta, kad verslas ir vartotojai gali bendrauti pasinaudodami įvairiais būdais - paštu, telefonu, internetu, elektroniniais kanalais ar socialiniais tinklais. Rinkoje jau yra nemažas pasirinkimas ir vis daugėja biometriniais duomenimis pagrįstų žmogaus identifikavimo priemonių. Didžioji dauguma šių technologijų reikalauja tam tikros specializuotos įrangos, kad būtų galima nuskaityti ar užfiksuoti reikiamą biometrinę informaciją ir įtraukti vartotoją atlikti konkrečius nurodytus patikrinamus veiksmus.[94] Šiandien biometriniai duomenys kol kas plačiausiai naudojami teisėsaugos institucijų veikloje nusikalstamų veikų prevencijos ir atskleidimo, asmenų identifikavimo, migracijos ar sienų kirtimo kontrolės tikslais. Tačiau kai kurios viešojo administravimo institucijos jau naudoja biometrinius duomenis asmens identifikavimui. Pavyzdžiui, LR Sodrai[95] galima pateikti savo balso pavyzdį pasirenkant asmens tapatybės nustatymą pagal balso žymenį. Veido atpažinimo sistemos yra labai naudingos kovai su nusikalstamumu ir terorizmu. Kertant valstybės sieną oro uostuose vis dažniau

[93] David J. Hass. *Personal identification. Its modern development and security implications*. USA: ASIS International, 2009. P. 24 – 25.
[94] Ratha, Nalini K. ir Venu Govindaraju. *Advances in Biometrics. Sensors, Algorithms and Systems*. Springer-Verlag London Limited, 2008. P. 203.
[95] Valstybinio socialinio draudimo fondo valdybos prie Socialinės apsaugos ir darbo ministerijos interneto svetainė; https://www.sodra.lt/lt/situacijos/informacija-gyventojams/ismanioji-sodra; [Žiūrėta 2022.05.24.]

naudojame savo pasus su integruotais biometriniais duomenimis greitam identifikavimui. Savo piršto atspaudą mes aktyviai naudojame mobilaus telefono ar kompiuterio atrakinimui. Bankai skatina savo klientus naudotis veido atpažinimo ir piršto atspaudo biometrija asmens identifikavimui jungiantis prie internetinės bankininkystės pasinaudojant išmaniuoju telefonu ar planšetiniu kompiuteriu. Pavyzdžiui Azerbaidžane dar 2017 metais bankinėje sistemoje buvo diegiama BS/2 vaizdo stebėsenos sistema[96], kuomet į savitarnos įrangą integruotas sprendimas kartu su vaizdo kamera suteikia galimybę identifikuoti techninės priežiūros darbuotojų, inkasatorių ir banko klientų tapatybę; taip pat atpažinti asmenis, įtrauktus į „juodąjį sąrašą“. Lietuvos įmonėse vis labiau populiarėja išmanusis biometrinis alkotesteris, kuris naudojant veido atpažinimo technologiją atpažįsta darbuotojus, fiksuoja jų atvykimo į darbo laiką ir automatizuotai tikrina blaivumą[97]. Biometrija padeda spręsti ir krovinių saugumo klausimus[98]. Taipogi, viešbučių svečiams ar sporto klubo lankytojams gali būti patogu pasinaudoti biometrine duomenų nuskaitymo įranga patekimui į patalpas be raktų, kai jie įregistruoja savo biometrinius duomenis registratūroje registracijos metu. Gyvenamųjų butų kompleksai gali naudoti biometrinius duomenis kontroliuodami patekimą į pagrindinį pastato įėjimą, baseiną ar sporto zonas. Biometriniai duomenys taip pat gali būti naudojami personalizavimui, pavyzdžiui, liftas gali būti užprogramuotas nuvežti gyventojus į jų daugiabučio namo aukštą arba automobilyje vairuotojo sėdynės padėtis, veidrodžiai ir klimato kontrolė gali būti nustatomi pagal asmeninius vairuotojo pageidavimus.[99]

Tačiau kartu su šiuolaikinio gyvenimo automatizavimu, biometrijos panaudojimu personalizavimui iškyla vis didesni reikalavimai saugumui ir

---

[96]Biometrinė identifikacija įsitvirtina Azerbaidžano rinkoje. [Publikuota: 2018.11.23.] http://www.news.lt/lt/article.im?id=362427&tid=45

[97] Biometrinis alkotesteris atpažįsta darbuotojus, fiksuoja darbo laiką ir tikrina blaivumą. [Publikuota 2016.05.24.] http://www.statybunaujienos.lt/naujiena/Biometrinis-alkotesteris-atpazista-darbuotojus-fiksuoja-darbo-laika-ir-tikrina-blaivuma/7629.

[98] Asstra associated traffic AG. *Kaip biometrika padeda spręsti krovinių saugumo klausimus*. https://sc.bns.lt/view/item/273487. [Publikuota 2018.06.26.]

[99] Anil K. Jain, Patrick Flynn, Arun A.Ross. *Handbook of biometrics*. (Springer Science+Business Media, 2008). P.506.

privatumui. Kiekvieną dieną daugybę kartų jungiantis prie įvairiausių sistemų ir duomenų bazių užduodami klausimai: „Ar šis asmuo turi teisę patekti į šią sistemą?“, „Ar šis asmuo turi pakankamas teises atlikti tam tikrą veiksmą?“. Ir kiekvieną kartą bandoma išsiaiškinti tą pačią saugumo problemą – kaip teisingai identifikuoti besijungiančius asmenis. Duomenų nuskaitymo tikslumas yra tik vienas aspektų biometrinių identifikavimo metodų panaudojimui. Vieni šaltiniai[100] teigia, kad asmens identifikavimas gali būti pagrįstas informacija iš trijų skirtingų kategorijų šaltinių: pirma, daiktų ar dokumentų, kurie padeda nustatyti konkretaus asmens tapatybę, turėjimas, pavyzdžiui, įvairūs asmens dokumentai, ID kortelė, asmens pasas ir panašiai, fiziniai ar elektroniniai raktai, suteikiantys galimybę patekti į vienas ar kitas patalpas, ir pan.; antra, žinojimas tik konkrečiam asmeniui priklausančios informacijos, pavyzdžiui PIN kodai, praėjimo slaptažodžiai, tam tikri asmenį identifikuojantys faktai, tarkim motinos mergautinė pavardė, ir pan.; ir trečia, biometrinių asmens duomenų, t. y, kad informacija yra susijusi su tam tikru fiziniu esamos tapatybės matavimu, pavyzdžiui, pirštų atspaudai, rainelės ar tinklainės raštas, plaštakos geometrija, eisenos charakteristika, veido ar balso biometrinis modelis ir panašiai. Kitai autoriai[101] asmens identifikavimo procesui priskiria keturis komponentus, tokius kaip (1) asmeniui suteiktas vardas ir pavardė (t. y. lyg ir „etiketė“), kuriuos jis gauna gimdamas; (2) fizinės (biometrinės) asmens savybės; (3) valstybinių institucijų asmeniui išduoti asmens dokumentai; ir (4) fizinio asmens, kaip individo paliekamas pėdsakas visuomenėje ar įrašuose, kai asmuo naudojasi savo asmens identifikaciniais dokumentais, pavyzdžiui, asmens tapatybės dokumentai (dokumentų numeriai) arba jam priskirtas asmens kodas naudojami materialaus turto nuosavybei įrodyti (kreditinių kortelių, bilietų, nekilnojamojo turto ir panašiai), asmens vardo (siekiant identifikuoti konkretų individą) ir suteiktų teisių ar įgaliojimų įrodymui (autorizuotų ar apribotų prieigų suteikimui ir panašiai), individo asmeninių duomenų, tokių kaip amžius, lytis, sveikatos stovis (kai kuriose šalyse), pilietybės ir panašiai patvirtinimui, individo asmeninių

[100] Ratha, Nalini K. ir Venu Govindaraju. *Advances in Biometrics. Sensors, Algorithms and Systems*. Springer-Verlag London Limited, 2008. P. 204 - 205.
[101] David J. Hass. *Personal identification. Its modern development and security implications*. USA: ASIS International, 2009. P.22.

pasiekimų, tokių kaip įgūdžiai, patirtis, žinios, išsilavinimas, kvalifikacijos įrodymui ir pan.[102]

Siekiant efektyviai valdyti verslo procesus elektroninėje erdvėje yra reikšminga būtinybė turėti lanksčias, patikimas ir saugias vartotojo identifikavimo technologijas, galinčias greitai, automatizuotai ir patikimai nustatyti vartotoją. Lengvas naudojimasis, įdiegimo paprastumas ir kaštai yra esminiai kriterijai nustatant ar biometriniai identifikavimo metodai bus naudingi ir priimtini naudojimui.

Asmenybės autentifikavimas ir identifikavimas

Dažnai siekiant įsitikinti asmens, turinio ar dokumento tapatumu ar tikrumu, naudojami žodžiai *autentifikavimas* arba *identifikavimas*.

A*utentifikacija* (dar vadinama *verifikacija*) reiškia „nustatyti, ar atitinka originalą, pirminį šaltinį"[103]. Autentifikacija - procesas, kurio metu vartotojo įvesti duomenys, pavyzdžiui jo paties susikurtas ar jam suteiktas kodas yra palyginamas su duomenų bazėje jau esama informacija - suvestu kodu. Jeigu prisijungimo metu vartotojo įvesti duomenys (kodas) sutampa su turima informacija duomenų bazėje (kodu), tai autentifikacija yra sėkminga ir vartotojas tokiu būdu patvirtina savo tapatybę. Tačiau slaptažodžio ar kodo žinojimas dar nereiškia, kad sistema identifikavo konkretų fizinį asmenį. Sistema tik atpažino kodą pateikusį, t. y., jį žinantį asmenį. Tačiau juo gali būti bet kuris žmogus. Taigi, slapto kodo turėjimas ar PIN kodo žinojimas dar nesuteikia galimybės užtikrinti asmens tapatybės[104]. Praktikoje identifikacija dažniausiai neatsiejama nuo autentifikacijos **–** asmens tapatybės patvirtinimo, todėl dažnai yra painiojama.

[102] David J. Hass. *Personal identification. Its modern development and security implications*. USA: ASIS International, 2009.P.14
[103] Tarptautinių žodžių žodynas, Vilnius, 2013. P 79.
[104] Ratha, Nalini K. ir Venu Govindaraju. *Advances in Biometrics. Sensors, Algorithms and Systems*. Springer-Verlag London Limited, 2008.P.307-308.

Identifikacija yra asmens tapatybės nustatymo procesas. Kiekvienas asmuo yra identifikuojamas nuo pat mažens, kai tik tėvai suteikia jam vardą ir pavardę, kartu su to asmens biometriniais parametrais bei kartu su kompiuterizuotu būdu žmogui suteiktais numeriais (pavyzdžiui, asmens kodu), kuriuos tam tikros valstybinės institucijos neatsiejamai sujungia su jo / jos vardu ir pavarde. Kitaip sakant, mus identifikuojant mes lyg ir atsakome į klausimą „Kas aš esu?“. Mes laikas nuo laiko esame prašomi pateikti ar parodyti savo asmens tapatybės dokumentus (pasą, ID kortelę). Pavyzdžiui mes turime įrodyti savo tapatybę keliaudami, atlikdami finansines operacijas ar įrodyti atitikimą tam tikriems įstatymams, tarkim pilnametystės įrodymui ar dėl amžiaus ribos alkoholio vartojimui ar įsigijimui ir pan. Tačiau ir asmens dokumento turėjimas dar neįrodo, kad prieš mus yra būtent tas asmuo. Dokumentas gali būti suklastotas ar pavogtas. Dokumentu gali pasinaudoti kitas asmuo. Kad būtų naudojamas kaip asmens identifikavimo priemonė, toks dokumentas turėtų būti susietas su konkrečiu asmeniu panaudojant jo biometrinius duomenis. Istoriškai nuotrauka buvo vienintelis biometrinis duomuo, kol šiuolaikinės elektroninės technologijos nepasiūlė kitų biometrinių duomenų praktiniam panaudojimui[105]. Ilgainiui susiformavo ir sąvoka - *biometrinis identifikavimas*, kas paprastai reiškia automatizuotą, panaudojant tam skirtas technologijas, biometrinių duomenų identifikavimo formą, taikomą žmonėms, t. y. išmatuojamų asmens biometrinių savybių panaudojimą to asmens tapatumui nustatyti[106].

[105] Ratha, Nalini K. ir Venu Govindaraju. *Advances in Biometrics. Sensors, Algorithms and Systems*. Springer-Verlag London Limited, 2008. P 24- 25
[106] Ratha, Nalini K. ir Venu Govindaraju. *Advances in Biometrics. Sensors, Algorithms and Systems*. Springer-Verlag London Limited, 2008. P. 109 - 110.

Biometrinio duomens sąvoka

Pats terminas „biometrija“ kilęs iš dviejų žodžių - „bios“, reiškiančio gyvenimą, t. y. gyvo asmens ar organizmo, ir graikų kalbos žodžio „metreo“, reiškiančio matavimą[107].

Vieni šaltiniai „biometriją“ apibūdina kaip mokslą apie žmogaus tapatybės atpažinimą pagal jo unikalius fizinius ar elgesio požymius[108], kiti gi biometriją nusako, kaip mokslo ir technikos sritį, kuri užsiima žmogaus biologinių požymių (fizinių ir fiziologinių) matavimu[109]. Tuo tarpu ISO/IEC 2382:2015[110] standarte biometriniai duomenys aprašomi kaip „konkretūs požymiai, pagal kuriuos galima nustatyti unikalias žmogaus savybes, tokias kaip piršto atspaudas, akies rainelė, balsas, kuriais remiantis galime patvirtinti žmogaus tapatybę“. Istorijoje vieni pirmųjų biometrinių duomenų buvo pradėti naudoti veido atvaizdas (fotografija) ir piršto atspaudas, skirti nusikaltusių asmenų identifikavimui.

ES Bendrajame Duomenų apsaugos Reglamente[111] 2016/976 (toliau - Reglamentas) biometriniai duomenys apibūdinami, kaip po specialaus techninio apdorojimo gauti asmens duomenys, susiję su fizinio asmens fizinėmis, fiziologinėmis arba elgesio savybėmis, pagal kurias galima konkrečiai nustatyti arba patvirtinti to fizinio asmens tapatybę, kaip antai veido atvaizdai arba daktiloskopiniai duomenys.

---

[107] https://www.lietuviuzodynas.lt/terminai/Biometrija
[108] Anil K. Jain, Patrick Flynn, Arun A.Ross. *Handbook of biometrics*. (Springer Science+Business Media, 2008). P. 1.
[109] Kvietkauskas V. ir kt. *Tarptautinių žodžių žodynas*. Vilnius: K. Požėlos spaustuvė, 1985. P. 527.
[110] ISO/IEC 2382:2015
[111] 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos 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), https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:32016R0679

Šiandien mes jau sunkiai suskaičiuojame, kiek įvairių slaptažodžių ar PIN kodų naudojame, prie kiek įvairių sistemų, elektroninių parduotuvių ar interneto svetainių registruojamės. Žmonės su savimi turi nešiotis įvairias korteles, dokumentus ir prisiminti dešimtis slaptažodžių. Tačiau šios priemonės gali būti užmirštos, pamestos, pavogtos ar tiesiog lengvai patekti kitiems asmenims. Tobulėjančios technologijos, besikeičianti aplinka, masinė migracija, didėjantis ir besiplečiantis pasaulinis nusikalstamumas bei socialiniai sukrėtimai, pavyzdžiui rugsėjo 11-osios įvykiai JAV ar didėjantis teroristinių aktų skaičius pasaulyje, paskatino plėtrą saugesnių ir patikimesnių nei asmens dokumentas ar slaptažodis identifikavimo priemonių poreikį. Biometrija tapo pageidaujama alternatyva tradicinėms fizinio asmens identifikavimo formoms[112] ir šių technologijų plėtra intensyviai auga.

Biometrinių duomenų savybės

Mokslininkai teigia (Anil'as K. Jain'as, Patrick'as Flynn'as, Arun'as A. Ross'as), kad įvairūs žmogaus biometriniai duomenys - fizinės kūno savybės ir elgesio charakteristikos, pavyzdžiui, pirštų atspaudai, veido ar plaštakos geometrija, balsas ar eisena, akies rainelė bei tinklainė gali būti apibūdinami remiantis tam tikromis savybėmis – universalumu, unikalumu, pastovumu, galimybe surinkti, tinkamumu, atlikimu ir menka galimybe pergudrauti, dar kartais vadinama „apėjimu"[113], tačiau teisiniame reguliavime šios savybės nėra atspindimos. Biometriniai duomenys, atitinkantys šias savybes, leidžia juos vienodai užrašyti, sukaupti ir saugoti biometrinių duomenų bazėse automatinio asmens atpažinimo tikslais. Visgi nebus nė vieno biometrinio duomens atitinkančio absoliučiai visas žemiau išvardintas biometrinių duomenų savybes. Pastebėtina, kad kiekviena iš šių išvardintų savybių turi savų privalumų ir trūkumų. Konkrečių savybių iš žemiau išvardintų pasirinkimas priklauso ne tik

[112] Ratha, Nalini K. ir Venu Govindaraju. *Advances in Biometrics. Sensors, Algorithms ans systems*. Springer-Verlag London Limited, 2008. P.157.
[113] Anil K. Jain, Patrick Flynn, Arun A. Ross. *Handbook of biometrics.* SpringerScience+Business Media, 2008. P.15. Nurodo: A.K.Jain, R.Bolie, S. Pankanti. *Biometrics. Personal identification in Networked Society*. Kluver Academic Publishers, 1999.

nuo biometrinių duomenų užrašymui, nuskaitymui ar saugojimui skirtų informacinių sistemų, bet ir nuo biometrinių duomenų naudojimo paskirties svarbos (pavyzdžiui, patekimui į ypatingos svarbos pastatus ar patalpas bus pasirenkamos sudėtingesnės informacinės technologijos, kurių pagalba bus siekiama užtikrinti didesnį patekimo saugumą, taigi ir biometrinių savybių rinkinys bus pilnesnis savo apimtimi), tačiau svarbiausia ir visuomet reikalaujama savybė – atlikimas, t. y. atpažinimo tikslumas[114].„[115]

Universalumas (*angl*. universality) parodo, kad kiekvienas žmogus turi turėti būtent tokią savybę. Priešingu atveju tiesiog nebus įmanoma suformuoti asmenų atpažinimui reikalingos duomenų bazės. Pavyzdžiui, tai, kad asmuo turi dešimt rankų pirštų, leidžia jį identifikuoti, net jei dėl kokios nors priežasties jis vieno ar kelių pirštų neturės, arba, tatuiruotė ar randai ant kūno[116] yra specifiniai, unikalūs biometriniai duomenys, tačiau juos turi ne visi žmonės, taigi, nebus universalūs.

Unikalumas arba išskirtinumas (*angl*. uniqueness arba distinctiveness[117]) reiškia, kad bet kurie du žmonės turi būti pakankamai skirtingi, atsižvelgiant tik į šią savybę. Žmogaus asmeniniai biometriniai duomenys per visą žmogaus gyvenimą negali būti pakeisti ar pasikeisti. Tai reiškia, kad asmuo nebegalės toliau gyvenime naudotis savo biometriniais duomenimis identifikavimui, jei jo ar jos biometriniais duomenimis buvo piktnaudžiaujama, pavyzdžiui, buvo atkleisti kitiems asmenims, nukopijuoti ir sunaikinti[118].

---

[114] Anil K. Jain, Patrick Flynn, Arun A. Ross. *Handbook of biometrics*. USA: SpringerScience+Business Media, 2008. P. 15.
[115] Poškaitienė, V. *Biometrinių duomenų tvarkymo teisėsaugos tikslais nacionalinėse duomenų bazėse reglamentavimo problematika*. (Magistro baigiamasis darbas, Mykolo Riomerio Universitetas, 2021). P. 25. Biometrinių duomenų tvarkymo teisėsaugos tikslais nacionalinėse duomenų bazėse reglamentavimo problematika - CENTRAL (lvb.lt)
[116] Anil K. Jain, Patrick Flynn, Arun A. Ross. *Handbook of biometrics*. USA: SpringerScience+Business Media, 2008. P. 231.
[117] Liu, Nancy Yue. *Bio-privacy: privacy regulations and the challenge of biometrics*. USA: Routledge, 2012. P.12.
[118] Ratha, Nalini K. ir Venu Govindaraju. *Advances in Biometrics*. *Sensors, Algorithms ans systems*. UK: Springer-Verlag London Limited, 2008. P. 81 -82.

Pastovumas (*angl*. permanence) parodo, jog savybė turi būti pakankamai atspari ir nekintanti bėgant laikui ar keičiantis aplinkos sąlygoms, pavyzdžiui dėl lengvos galimybės pakeisti plaukų spalvą būtų netinkama savybė, o žmogaus veido kintamumas esant skirtingoms aplinkybėms, tokioms kaip apšvietimas, judesys, emocinės išraiškos, kameros sufokusavimas, makiažas, ar saulės akiniai bei asmens senėjimo požymiai[119] gali sukelti sunkumų užfiksuojant ir vėliau atpažįstant duomenis. Tuo tarpu, akies rainelė labai nedaug keičiasi per žmogaus gyvenimą ir paprastai laikoma pastovesne nei veidas ar balsas. Tačiau svarbu pažymėti, kad nėra absoliučiai tvirtos biometrinės savybės[120].

Galimybė surinkti arba *renkamumas* (*angl.* measurability arba collectability) reiškia biometrinio duomens išmatuojamumą, pavyzdžiui, kai kurių biometrinių duomenų surinkimas arba užfiksavimas reikalauja per daug pastangų ar sudėtingos įrangos arba pats procesas per sudėtingas ir ilgai trunkantis arba aplinkos faktoriai stipriai įtakoja biometrinio duomens kokybę, pavyzdžiui, asmens balsas kaip biometrinis duomuo yra susijęs ne tik su asmeninėmis savybėmis, bet ir su daugeliu aplinkos kintamųjų, nes balso generavimas yra itin sudėtingo proceso rezultatas[121].

Priimtinumas arba *tinkamumas* (*angl*. acceptability) yra tai, kiek žmonėms yra priimtinas, patogus ir lengvas toks asmens biometrinio požymio surinkimas, t. y kiek bendradarbiavimo reikalinga iš asmens pusės surenkant tokį duomenį, pavyzdžiui, veido geometrijos nuskaitymas yra pakankamai lengvas, tuo tarpu DNR požymio pateikimas daug kam sukelia nemalonių jausmų ir reikalauja specialių aplinkybių.

Atlikimas (*angl*. performance), reiškia biometrinio duomens atpažinimo tikslumą ir tam tikslui pasiekti būtinų išteklių ar technologijų lygio poreikį,

[119] *Ibid.*, P. 43.
[120] Liu, Nancy Yue. *Bio-privacy: privacy regulations and the challenge of biometrics*. USA: Routledge, 2012. P. 30.
[121] Liu, Nancy Yue. *Bio-privacy: privacy regulations and the challenge of biometrics*. USA: Routledge, 2012. P. 151.

kuomet, pavyzdžiui, kaip teigia Ravindra Das'as, reikalingi tam tikri matematiniai algoritmai, kad būtų išfiltruotos unikalios ypatybės iš anksčiau užfiksuoto vaizdo, bei specializuota programinė įranga, kad šios unikalios savybės būtų paverstos tam tikra forma, kurią technologija gali suprasti ir pakartotinai naudoti.

Apėjimas arba galimybė pergudrauti (*angl.* circumvention) parodo ar būtų lengva apgauti biometrinių duomens nuskaitymo sistemą apgaulingais metodais, pavyzdžiui nukopijuoti ir pateikti kito asmens pirštų atspaudus arba perdaryti, suklastoti duomenis [122].

Kaip jau minėta, nei viena asmens biometrinė charakteristika, kaip asmens duomuo, neatitiks visų šių pageidautinų savybių, kurios paprastai keliamos biometrinių duomenų nuskaitymui ir užfiksavimui tam skirtose sistemose ar duomenų bazėse[123]. Kitaip tariant, jokia biometrinė charakteristika nėra ideali, tačiau daugelis jų yra atitinkančios *priimtinumo* savybę, t. y. patogus ir lengvas biometrinio požymio surinkimas, nekeliantis fiziniams asmenims, kurių biometrinė charakteristika užfiksuojama, nemalonių pojūčių ar nepriimtinų veiksmų.

Ilgą laiką pirštų atspaudai buvo siejami tik su nusikaltimais ir teisėsauga[124]. Tačiau tobulėjant technologijoms pirštų atspaudai tapo vieni populiariausiai naudojamų biometrinių duomenų[125], o akies rainelė bei tinklainė ateityje gan greitai taps plačiai naudojamos lyginant su kitais biometriniais duomenimis dėl lengvos surinkimo arba užrašymo savybės (*galimybė surinkti arba renkamumas*) ir menkų galimybių apgauti nuskaitančią informacinę sistemą, pavyzdžiui pateikiant kito asmens akies rainelės kopiją (savybė - *apėjimas arba galimybė pergudrauti)*. Be to, šių biometrinių duomenų (pirštų atspaudų

[122] Ravindra Das. *Biometric Technology. Authentication, Biocryptograpfy, and Cloud-Based Architecture.* UK: Taylor & Francis Group LLC, 2015. P. 5.
[123] Anil K. Jain, Patrick Flynn, Arun A. Ross. *Handbook of biometrics*. USA: SpringerScience+Business Media, 2008. P. 15.
[124] Anil K. Jain, Patrick Flynn, Arun A. Ross. *Handbook of biometrics*. USA: SpringerScience+Business Media, 2008. P. 3.
[125] Ratha, Nalini K. ir Venu Govinda.raju. *Advances in Biometrics. Sensors, Algorithms and Systems*.UK: Springer-Verlag London Limited, 2008. P. 307-308.

ar akies rainelės) nuskaitymui ar surinkimui būtinas ir bendradarbiavimas iš subjekto pusės[126]. Didžiajai daugumai šių technologijų būtina tam tikra specializuota ar automatizuota įranga, įgalinanti fiksuoti reikiamą biometrinę informaciją ir įtraukti duomenų subjektą atlikti konkrečius nurodytus patikrinamus veiksmus, pavyzdžiui, priglausti prie įrenginio atmerktą akį akies tinklainės ar rainelės nuskaitymui ir įrašymui į duomenų bazę. O tai reiškia, kad būtų išvengiama biometrinių duomenų nuskaitymo tikimybės asmeniui nežinant ir procese nedalyvaujant[127]. Kaip konstatuojama Valstybinės duomenų apsaugos inspekcijos išleistoje „Rekomendacijoje dėl biometrinių duomenų naudojimo elektroninėje erdvėje“, „biometriniai duomenys yra ilgalaikiai ir nėra lengvai pakeičiami ar išduodami naujai, ką nesunkiai galima atlikti su slaptažodžiais, raktinėmis kortelėmis ar žetonais”[128]. Kurdami slaptažodžius mes turime galimybę pasinaudoti daugybe simbolių ir variantų, „tačiau biometrinių duomenų analizei gali būti panaudota tik keletas žmogaus atributų, pavyzdžiui, dvi akies rainelės, dvi tinklainės, 10 pirštų atspaudų, veidas”[129].

Visgi, nei viena biometrinių duomenų nuskaitymo ir analizės technologija neduoda šimtaprocentinio patikimumo[130], todėl visada išlieka rizika, kad sistema priims jai pateikiamus atpažinimui suklastotus pirštų atspaudus kaip tinkamus, arba, kad dėl sistemoje išsaugoto prastos kokybės biometrinio duomens sistema nepajėgs sulyginti pateikiamo duomens su išsaugotu sistemoje šablonu arba, dar blogiau, dėl tos pačios priežasties suteiks prieigas neįgaliotam asmeniui arba, pavyzdžiui dėl tokios klaidos bus suimtas arba nukentės nekaltas asmuo.

---

[126] Ratha, Nalini K. ir Venu Govinda.raju. *Advances in Biometrics. Sensors, Algorithms and Systems*.UK: Springer-Verlag London Limited, 2008. P. 307-308.
[127] Ratha, Nalini K. ir Venu Govindaraju. *Advances in Biometrics. Sensors, Algorithms and Systems*.UK: Springer-Verlag London Limited, 2008. P. 307-308.
[128] Valstybinės duomenų apsaugos inspekcijos oficiali interneto svetainė. *Biometrinių duomenų tvarkymas elektroninėje erdvėje*. 2017. https://vdai.lrv.lt/uploads/vdai/documents/files/Rekomend_Biometriniai_2017.pdf
[129] *Ibid.*
[130] Ratha, Nalini K. ir Venu Govindaraju. *Advances in Biometrics*. *Sensors, Algorithms ans systems*. UK: Springer-Verlag London Limited, 2008. P. 425.

Taigi, darytina išvada, kad biometriniai duomenys turėtų būti apibrėžiami, kaip visi gyvo fizinio asmens duomenys, kurie a) yra tiesiogiai ar netiesiogiai susiję su unikaliomis ar savitomis asmens fizinėmis, fiziologinėmis arba elgesio charakteristikomis ir b) yra naudojami arba yra tinkami naudoti automatizuotomis priemonėmis c) asmens tapatybės biometrinio atpažinimo bei biometrinio patikrinimo tikslais. Pastebėtina, kad 2015 m. *ISO/IEC 2382:2015*[131] pateikiamoje biometrinių duomenų apibrėžtyje biometriniai duomenys buvo įvardinti kaip specifinės savybės, atspindinčios unikalias asmenines savybes, tačiau 2016 metais patvirtinto Reglamento pateikiamoje biometrinių duomenų apibrėžtyje šios savybės nėra, t. y. kad pagal unikalią ir nepakartojamą tik konkrečiam asmeniui priklausančią jo biometrinę savybę būtų galima „*nustatyti arba patvirtinti to fizinio asmens tapatybę".* Manytina, kad biometrinių duomenų apibrėžtyje turėtų būti įtraukta ir savybė – unikalumas, kaip savitas kiekvienos asmenybės bruožų derinys, dėl šios savybės išskiriantis subjektą iš visų kitų.[132]

Biometrinių duomenų įvairovė

Šiuo metu **pirštų atspaudai** yra bene populiariausia biometrinio atpažinimo priemonė. Piršto atspaudas pilnai susiformuoja maždaug septintame vaisiaus gyvavimo mėnesyje ir praktiškai nesikeičia per visą žmogaus gyvavimo laikotarpį, išskyrus incidentus ar nelaimingus atsitikimus, pavyzdžiui pjūviai ant pirštų galiukų[133]. Tačiau ši priemonė gali būti nepatikima dėl keleto aspektų, pavyzdžiui dėl skirtingo nuskaitymo sistemos jautrumo, dėl piršto atspaudo nuskaitymo netikslumų dėl drėgno odos paviršiaus arba nešvaraus nuskaitymo sensoriaus paviršiaus, be to gana lengva asmens piršto atspaudą gauti net jam nežinant, taigi ir padaryti jo kopiją.

---

[131] ISO / IEC 2382-37: 2017. https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:-37:ed-2:v1:en

[132] Poškaitienė, V. *Biometrinių duomenų tvarkymo teisėsaugos tikslais nacionalinėse duomenų bazėse reglamentavimo problematika*. (Magistro baigiamasis darbas, Mykolo Riomerio Universitetas, 2021). P. 25. Biometrinių duomenų tvarkymo teisėsaugos tikslais nacionalinėse duomenų bazėse reglamentavimo problematika - CENTRAL (lvb.lt)

[133] Anil K. Jain, Patrick Flynn, Arun A. Ross. *Handbook of biometrics.* SpringerScience+Business Media, 2008. P. 23.

Veido geometrijos identifikavimo tarp kitų biometrinių identifikavimo technologijų privalumas yra tai, kad jis yra pilnai bekontaktis ir suteikia galimybę identifikuoti asmenį eigoje, jam judant. Minimalus arbe beveik visai nereikalingas asmens bendradarbiavimas ar papildomi veiksmai norint nuskaityti veido geometriją. Taigi ši technologija leidžia lengvai surinkti duomenis. Bet kartu gana lengva gauti atvaizdo kopiją asmeniui nežinant, pavyzdžiui pasinaudojant atspindinčiais paviršiais. Dėl šios priežasties veido geometrijos nuskaitymo technologiją bandoma papildyti veido kraujagyslių tinklo atpažinimu. Kadangi kraujagyslių tinklas yra po žmogaus oda ir yra matomas dėka kraujo tekėjimo jomis, jų beveik neįmanoma suklastoti ar apgauti įrangą[134]. Žymiai didesnio dėmesio veido biometrijos panaudojimui sulaukė 3D veido biometrija dėl savo gebėjimo įveikti kai kuriuos tradicinius 2D veido biometrijos nuskaitymo trūkumus, pavyzdžiui dėl netinkamos veido išraiškos ar krypties arba apšvietimo kokybės. 3D veido biometrijos atpažinimo technologijos[135] išgauna giluminį veido atvaizdą. Tačiau tai reikalauja, kad vartotojas būtų labai arti kameros, o kai kurie įrenginiai gali tiksliai užfiksuoti vaizdą tik jei asmuo kelias sekundes nejuda. Tačiau pagal asmens veido biometrijos duomenį lengvai įmanoma nustatyti keletą kitų asmens duomenų (pavyzdžiu, tikėjimą, tautybę, lytį), kurių tvarkymui Reglamentas nustato griežtas sąlygas.

Vis dėlto, problema kylanti identifikuojant asmenį pasinaudojant jo / jos veido biometrija ir lyginant jį su duomenų bazėje esančiais vis dar kelia daug iššūkių. Taip yra dėl žmogaus veido kintamumo veikiant skirtingoms išorės aplinkybėms, tokioms kaip apšvietimas, judėjimas, emocinės žmogaus išraiškos, kameros sufokusavimas, žmogaus senėjimo įtakoti veido pokyčiai, makiažo ir kosmetinių operacijų įtaka ar saulės akiniai. Dažnai šios aplinkybės reikšmingai įtakoja asmens veido atpažinimo procesą, ypač kai sistema turi

[134] Ratha, Nalini K. ir Venu Govindaraju. *Advances in Biometrics. Sensors, Algorithms and Systems*. Springer-Verlag London Limited, 2008. P. 169.
[135] Anil K. Jain, Patrick Flynn, Arun A. Ross. *Handbook of biometrics*. SpringerScience+Business Media, 2008. P. 211.

identifikuoti asmenį didelėje veidų duomenų bazėje[136] ar judančiame žmonių sraute.

Akies rainelės atpažinimas yra vienas iš pačių tiksliausių biometrinių asmens identifikatorių. Lengvas naudojimasis ir įdiegimas yra pagrindiniai teigiami aspektai sistema besinaudojančiam vartotojui. Akies rainelės atpažinimo tikslumui aktualiausi aspektai yra atstumas, užfiksavimo apimtis, rainelės nuskanavimo laikas, vartotojo judesiai, vartotojo žvilgsnio kryptis bei supanti aplinka[137]. Kas tikrai aišku, rainelės nuskaitymo sistema bus jautri apšvietimui, kurį padidina arba slopina pati rainelės nuskaitymo technologija. Pavyzdžiui rūkas ar dulkės ore gali įtakoti nuskaitymo kokybę, saulės spindulių arba šviesos sukelti atspindžiai gali uždengti dominančias akies sritis, ryški šviesa gali sukelti sunkumų, susijusių su automatiniu identifikavimo sistemos valdymu, ir panašiai. Tačiau nepaisant šių galimų nuskaitymo problemų, Jungtiniai Arabų Emyratai (toliau - JAE) dar 2001 metais pasienio postuose įdiegė privalomą visiems keleiviams, atvykstantiems į JAE sausuma, jūra ar oru, patikrinimą akies rainelės atpažinimo sistema[138]. Kiekvieno keleivio akies rainelės raštas, asmeniui sekundę ar dvi žiūrint į akies rainelės nuskaitymo kamerą, matematiškai užkoduojamas, o gautas vaizdas siunčiamas į centrinę duomenų bazę, kur lyginamas su 420 tūkst. asmenų, kurie buvo išsiųsti iš JAE už įvairius pažeidimus, atvaizdais. Kiekvienam atvaizdui palyginti su visais duomenimis, saugomais centrinėje duomenų bazėje, prireikia mažiau nei vienos sekundės. Šia sistema buvo siekiama užkirsti kelią deportuotiems asmenims grįžimui į JAE po jų išsiuntimo iš šalies[139]. Nors asmuo buvo įtraukiamas į deportuotų asmenų sąrašą, kuriame nurodomi konkretūs duomenys, tačiau asmuo galėtų atvykti su nauju pasu ir šiek tiek kitokiu vardu, pavarde ir, remdamasis naujais asmens dokumentais, vėl galėtų patekti į šalį. Naudojant labai aukštos kokybės ir tikslumo rainelės atpažinimo technologiją,

[136] Anil K. Jain, Patrick Flynn, Arun A. Ross. *Handbook of biometrics*. SpringerScience+Business Media, 2008. P. 43.
[137] Ratha, Nalini K. ir Venu Govindaraju. *Advances in Biometrics. Sensors, Algorithms and Systems*. Springer-Verlag London Limited, 2008. P. 107 - 109.
[138] The National Academy of Sciences interneto svetainė. *Iris recognition border-crossing system in the UAE.* https://trid.trb.org/view/741851 [Prisijungta 2022.05.23.]
[139] Anil K. Jain, Patrick Flynn, Arun A. Ross. *Handbook of biometrics*. SpringerScience+Business Media, 2008. P. 461.

atvykstančio į JAE žmogaus rainelė, netgi asmeniui esant su akiniais, jam artėjant prie pasienio darbuotojo darbo vietoje įrengtos kameros pagalba per sekundės dalį sutikrinama su saugomu duomenų bazėje akies rainelės šablonu, užfiksuotu prieš asmenį deportuojant. Tai yra tai, ko asmuo negali pakeisti ar išvengti, ir tai daroma be jokių jo asmens dokumentų tikrinimo.

Pirmasis komercinis **plaštakos geometrijos**[140] skaitytuvas buvo įdiegtas 1970 m. JAV. Šiai technologijai buvo keliamas tikslas suteikti prieigą įgaliotiems vartotojams. Dėl šios technologijos patikimumo ir mažo klaidų lygio jis tapo pirmąja biometrinio matavimo technologija, tinkama didelėms rinkoms, tokioms kaip darbuotojų laiko ir lankomumo registravimui ar prieigos kontrolei. Dėl paprastų biometrinių nuskaitymo galimybių - plaštaka lengvai pateikiama - šis metodas buvo ekonomiškas, patogus vartotojui, praktiškas ir gan plačiai naudojamas iki šiol.

Plaštakos kraujagyslių[141] atpažinimo metode asmens identifikavimui yra naudojami plaštakos kraujagyslių struktūros atpažinimo modeliai. Bekontaktės kraujagyslių struktūros atpažinimo technologijos[142] pirmą kartą buvo įdiegtos Japonijos bankinėje sistemoje klientų identifikavimui 2004 m. Tai buvo pirmoji stambi taikomoji technologija privačios Japonijos kompanijos panaudota biometriniam identifikavimui paslaugoms, skirtoms plačiajai visuomenei. Be to, kartu su kitomis taikomomis technologijomis, ši technologija buvo integruota į durų atidarymo apsaugos sistemas. Kadangi kraujagyslės yra žmogaus kūne, plaštakos kraujagyslių struktūrą sudėtinga atkartoti ar suklastoti, be to šios technologijos suteikia aukštą tikslumo lygį. Asmens identifikavimui panaudojant kraujagyslių struktūros atpažinimo technologijas gali būti panaudojama tiek plaštakos, tiek rankos arba pirštų

[140] Anil K. Jain, Patrick Flynn, Arun A. Ross. *Handbook of biometrics*. SpringerScience+Business Media, 2008. P. 93 - 94.
[141] Ratha, Nalini K. ir Venu Govindaraju. *Advances in Biometrics. Sensors, Algorithms and Systems*. Springer-Verlag London Limited, 2008. P. 75 - 76.
[142] Ratha, Nalini K. ir Venu Govindaraju. *Advances in Biometrics. Sensors, Algorithms and Systems*. Springer-Verlag London Limited, 2008. P. 75 - 76.

kraujagyslių struktūra arba akies tinklainėje esančių kraujagyslių struktūra. Kraujagyslių struktūra negali būti pavogta ją nufotografuojant, nukopijuojant ar atsekant. Tai reiškia, kad įprastinėmis sąlygomis kraujagyslių struktūros suklastojimas būtų ypatingai sudėtingas. Kiekvieno žmogaus kraujagyslių struktūra unikali. Netgi identiški dvyniai turi skirtingas kraujagyslių struktūras. Be to, kraujagyslių struktūra nesikeičia su žmogaus amžiumi, išskyrus traumų ar ligų atvejus.

Automatinis kalbančiojo **balso identifikavimas** yra atliekamas remiantis jo ar jos balso atpažinimu[143]. Šis veiksmas gali būti įgyvendinamas keliais būdais. Pavyzdžiui, šis veiksmas gali būti skirtas identifikuoti (išskirti) kalbantįjį iš kitų kalbančiųjų tarpo pagal įkalbėtą testinį pavyzdį. Kalbėtojo identifikavimui gali būti naudojamos ir sistemos, susijusios su tekstu (kai reikia pasakyti konkretų įrašytą tekstą, pvz. banko sąskaitos numerio patvirtinimui, kuomet vartotojas pasako skaičių seką) ir nesusijusios su konkrečiu tekstu. Kalbančiojo balso biometrijos pranašumas yra tas, kad kalbos signale fiksuojama kelių faktorių informacija, t. y. identifikuojami balso tembro duomenys ir informacija, susijusi su kalbėtojo žiniomis, kai kalbama apie konkretų tekstą[144].

Interaktyvaus, t. y. sujungto su kompiuteriu, asmens **parašo atpažinimas** yra socialiai ir teisėtai pripažintas ir priimtinas bei plačiai naudojamas kaip asmens tapatybės patvirtinimo metodas[145]. Tokio biometrinio duomens privalumas tas, kad parašą lengva gauti ir pateikti tiesiog rašikliu ant popieriaus lapo, arba elektroninėmis priemonėmis, turinčiomis jutiklius, pavyzdžiui planšetiniai kompiuteriai, įranga su jutiminiu ekranu (*angl.* touch screens) ir panašiai. Tačiau asmens parašo biometrijos panaudojimo trūkumai yra mažas universalumas, nes ne visi gali pasirašyti, pavyzdžiui vaikai ar senoliai dėl kai

[143] Ratha, Nalini K. ir Venu Govindaraju. *Advances in Biometrics. Sensors, Algorithms and Systems*. Springer-Verlag London Limited, 2008. P. 184.
[144] Ratha, Nalini K. ir Venu Govindaraju. *Advances in Biometrics. Sensors, Algorithms and Systems*. Springer-Verlag London Limited, 2008. P.204 – 205.
[145] Anil K. Jain, Patrick Flynn, Arun A. Ross. *Handbook pf biometrics*. SpringerScience+Business Media, 2008. P. 189.

kurių senatvinių ligų arba neįgalūs asmenys, nepastovumas, nes žmogaus parašas ilgainiui gali skirtis, ir pažeidžiamumas panaudojant klastotes.

Kiti asmens identifikavimo būdai, tokie kaip genetinis identifikavimas, pavyzdžiui DNR mėginys, ar identifikavimas pagal odontologinius įrodymus, pavyzdžiui, dantų nuotraukas, dažniausiai naudojami įtariamojo ir aukos atpažinimui ir nėra naudojami plačiosios visuomenės reikmėms dėl savo sudėtingumo ir kitų biometrijos duomenims užfiksuoti nepritaikomų savybių.

Kylančios grėsmės

Platus ir nekontroliuojamas biometrijos naudojimas kelia susirūpinimą asmenų pagrindinių teisių ir laisvių apsaugos atžvilgiu, yra opus klausimas duomenų apsaugos požiūriu bei asmens teisės į privatumą aspektu. Lietuvos Valstybinės Duomenų apsaugos inspekcijos nuomone[146], biometrinių duomenų panaudojimas praktikoje tampa vis dažniau naudojama, efektyvi, pažangi ir sąlyginai nebrangi asmens identifikavimo sistema. Tai bene geriausias kaštų ir naudos santykis kokybiškai ir patogiai identifikuoti duomenų subjektą, nereikalaujant iš jo nieko papildomo, kai reikia vienareikšmiškai nustatyti asmens tapatybę, tačiau tai siejasi ir su tam tikromis grėsmėmis.

Pagrindinės biometrinių duomenų savybės, tie unikalūs ir beveik nesikeičiantys per žmogaus gyvenimą bruožai, taip pat yra ir jų Achilo kulnas[147]. Žmogaus biometriniai duomenys yra ilgalaikiai ir per visą žmogaus gyvenimą negali būti pakeisti ar pasikeisti, priešingai nei PIN kodas ar slaptažodis. Kurdamas slaptažodį, duomenų subjektas gali rinktis iš daugybės simbolių, tačiau biometrinių duomenų analizei gali būti panaudota tik keletas žmogaus atributų, pavyzdžiui, dvi akies rainelės, dvi tinklainės, 10 pirštų

[146] Valstybinės duomenų apsaugos inspekcijos oficiali interneto svetainė. *Biometrinių duomenų tvarkymas elektroninėje erdvėje*. 2017. https://vdai.lrv.lt/uploads/vdai/documents/files/Rekomend_Biometriniai_2017.pdf

[147] Ratha, Nalini K. ir Venu Govindaraju. *Advances in Biometrics. Sensors, Algorithms and Systems*. Springer-Verlag London Limited, 2008. P. 425.

atspaudų, veido atvaizdas[148]. Tai reiškia, kad asmuo nebegalės toliau gyvenime naudotis savo biometriniais duomenimis identifikavimui, jei jo ar jos biometriniais duomenimis buvo piktnaudžiaujama[149], pavyzdžiui bus pažeista duomenų bazė ar joje kaupiami ir saugomi biometriniai duomenys, asmens biometriniai duomenys buvo atkleisti kitiems asmenims, nukopijuoti ar sunaikinti. Asmeniui kyla grėsmė prarasti galimybę būti identifikuotu, o tai reiškia – prarasti savo tapatybę.

Biometrinių duomenų tikslumas, tiek jų nuskaitymo ir patalpinimo duomenų bazėse metu, tiek analizės dėl atitikties metu taipogi nesuteikia 100 procentinio tikslumo garantijos. Biometrinis autentifikavimas remiasi matematine tikimybe nustatant kaip tiksliai nuskaityti subjekto duomenys sutampa su užfiksuotu įrašu sistemoje, o tai reiškia, kad egzistuoja paklaidos ribos, priklausančios nuo daugelio jau aukščiau minėtų aspektų, tokių kaip sensorių jautrumas, apšvietimas, atstumas, technologijų kokybė ir pan. Sistema, nuskaitydama informaciją, gali suklysti ir palaikyti vieną asmenį kitu. Kai subjekto duomenys nesutampa su įrašu, autentifikavimas yra nepatvirtinamas ir tolimesnis priėjimas prie sistemos yra uždraustas[150]. O tokiu atveju identifikuojamas asmuo susidurs su problemomis, bandydamas įrodyti, kad sistema suklydo. Be to, biometrinė duomenų nuskaitymo sistema turi turėti galimybę užfiksuoti ir atpažinti bandymus apeiti sistemą naudojant tam tikrus dirbtinius pavyzdžius, t. y. atpažinti ar biometrinį duomenį pateikia gyvas žmogus ar galbūt yra pateikiama latentinė piršto atspaudo kopija, ir tuo pačiu nesukelti nepatogumų naudotis sistema autentiškam (tikrajam) įgaliotam asmeniui[151]. Visada išlieka netikslumo rizika, o tuo pačiu ir klaidų, tame tarpe ir

[148] Valstybinės duomenų apsaugos inspekcijos oficiali interneto svetainė. *Biometrinių duomenų tvarkymas elektroninėje erdvėje*. 2017. https://vdai.lrv.lt/uploads/vdai/documents/files/Rekomend_Biometriniai_2017.pdf

[149] Ratha, Nalini K. ir Venu Govindaraju. *Advances in Biometrics. Sensors, Algorithms and Systems*. Springer-Verlag London Limited, 2008. P . 81 -82

[150] Valstybinės duomenų apsaugos inspekcijos oficiali interneto svetainė. *Biometrinių duomenų tvarkymas elektroninėje erdvėje*. 2017. https://vdai.lrv.lt/uploads/vdai/documents/files/Rekomend_Biometriniai_2017.pdf

[151] Ratha, Nalini K. ir Venu Govindaraju. *Advances in Biometrics. Sensors, Algorithms and Systems*. Springer-Verlag London Limited, 2008. P.3.

tyčinių, rizika. Kadangi kai kuriuos iš asmens biometrinių duomenų pakankamai lengva gauti, nukopijuoti asmeniui nežinant, biometriniam identifikavimui naudoti tik vieną biometrinį duomenį yra gana nesaugu. Vienas iš saugumo iššūkių yra apgaulės tikimybė, pavyzdžiui, tiesiog padaryti kopijas arba suklastotus pirštų atspaudus nuo tikrų gyvo žmogaus pirštų ar jų atspaudų. Todėl jau dabar ieškoma būdų užkirsti kelią tokiems veiksmams panaudojant panaikinamus biometrinius duomenis (kai biometriniai duomenys įrašomi į kortelę) arba kompleksinius atpažinimo sprendimus[152]. Pavyzdžiui, kadangi automatinių veido atpažinimo sistemų veikimo kokybė ypač priklauso nuo tinkamo apšvietimo, pasitelkiamas kelių faktorių veido atpažinimas, kai panaudojami kartu šiluminis infraraudonųjų spindulių ir ne infraraudonųjų spindulių vaizdas atskirai[153] arba kartu, diegiamas kelių biometrinių duomenų kompleksas kartu naudojant atpažinimui to paties žmogaus veido ir, pavyzdžiui, ausies geometriją[154] ir panašūs sprendimai.

Visgi ypač didelis pavojus asmens privačiam gyvenimui kyla kaupiant ir saugant biometrinius asmens duomenis didelės apimties duomenų registruose dėl biometrinių duomenų vagysčių. Ir nors dažnai biometriniai duomenys, kaip ir slaptažodžiai, yra saugomi skaitmeniniu formatu centralizuotose sistemose, tačiau tikimybė, kad kaupiami duomenys gali būti nutekinti ar įvyktų vagystė, išlieka[155]. Biometrinių duomenų saugojimui skirtų duomenų bazių vis daugėja. Šiandien jose biometrinius duomenis kaupia tiek valstybinės institucijos, tiek privatus verslas. Kuo bus daugiau tokių biometrinių duomenų bazių ir kuo jos bus didesnės, tuo didesnė pažeidimų tikimybė. Kyla daug klausimų. Ar valdžios institucijų valdomos duomenų bazės gerai apsaugotos? Ar organizacijos arba privačios įmonės, kurios

[152] Ratha, Nalini K. ir Venu Govindaraju. *Advances in Biometrics. Sensors, Algorithms and Systems*. Springer-Verlag London Limited, 2008. P.307-308
[153] Anil K. Jain, Patrick Flynn, Arun A. Ross. *Handbook pf biometrics*. SpringerScience+Business Media, 2008. P. 293-294
[154] Anil K. Jain, Patrick Flynn, Arun A. Ross. *Handbook pf biometrics*. SpringerScience+Business Media, 2008. P.316
[155] Valstybinės duomenų apsaugos inspekcijos oficiali interneto svetainė. *Biometrinių duomenų tvarkymas elektroninėje erdvėje*. 2017. https://vdai.lrv.lt/uploads/vdai/documents/files/Rekomend_Biometriniai_2017.pdf

šiandien kaupia duomenis duomenų bazėse, tačiau pritrūkus pinigų, nesusigundys panaudoti jų tvarkomus biometrinius duomenis komerciniais tikslais? Todėl kyla reikšmingi teisiniai ir administraciniai klausimai - kaip biometriniai duomenys bus prižiūrimi, kam ir kokiu pagrindu suteikiama teisė kaupti ir prieiti prie biometrinių duomenų bazių, kaip apsaugomos pačios duomenų bazės ir panašiai.

Biometrinių duomenų tvarkymą Lietuvoje reglamentuojantys įstatymai

Reglamente[156] (ES) 2016/679 **biometriniai duomenys traktuojami kaip specialių kategorijų asmens duomenys, kurių tvarkymas pagal Reglamento 9 straipsnio 1 dalies nuostatas yra draudžiamas, kai** tokiu tvarkymu siekiama konkrečiai nustatyti fizinio asmens tapatybę, nebent, pagal to paties straipsnio 2 dalį turime vieną iš dešimties tame straipsnyje numatytų išimčių. **Biometrinių duomenų saugojimo būdų reglamentavimas Bendrajame Duomenų Apsaugos Reglamente paliktas valstybių narių diskrecijai**. Reglamento **9 straipsnio 4 dalies nuostatose teigiama, kad „**Valstybės narės gali toliau taikyti arba nustatyti papildomas sąlygas, įskaitant apribojimus, genetinių duomenų, biometrinių duomenų arba sveikatos duomenų tvarkymui". Tačiau Lietuvos Respublikos Asmens duomenų teisinės apsaugos įstatymas[157] biometrinių duomenų tvarkymui papildomų sąlygų nenumato.

Keletas kitų Lietuvos Respublikos įstatymų taip pat reglamentuoja biometrinių duomenų tvarkymo aspektus[158]. LR asmens tapatybės kortelės ir paso

[156] 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos 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), https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:32016R0679

[157] Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo Nr. I-1374 pakeitimo įstatymas 2018 m. birželio 30 d. Nr. XIII-1426.

[158] Gecevičienė, O. *Ar biometrinių duomenų (skaitmeninių veido atvaizdo bei pirštų atspaudų) kaupimas bei saugojimas gyventojų registre nepažeidžia asmens teisės į*

įstatymo[159], 5 straipsnio 7 dalis apibrėžia, kad „išduodamose asmens tapatybės kortelėse elektroniniu būdu fiksuojami <...> piliečio biometriniai duomenys tapatybei patvirtinti – veido atvaizdas ir dviejų pirštų atspaudai, taip pat asmens atpažinimo elektroninėje erdvėje sertifikatas ir kvalifikuotas sertifikatas“, o 8 dalis tą patį sako apie išduodamus piliečių pasus. LR asmens tapatybės kortelės ir paso įstatymas, Tarnybinio paso[160] ir Gyventojų registro[161] įstatymo pakeitimo ir papildymo įstatymai nustatė biometrinių duomenų (skaitmeninių veido atvaizdo bei pirštų atspaudų) pasuose naudojimą ir jų kaupimą bei saugojimą Gyventojų registre. Pastebėtina, kad Lietuva, nepaisant Europos Parlamento, Europos Sąjungos 29 Straipsnio darbo grupės ir įvairių ekspertų nuomonės rinktis saugesnius biometrinius duomenis, pavyzdžiui, rankos kontūrą, pasirinko ypač nesaugiais laikomus duomenis, nes jie atskleidžia ypatingą informaciją apie asmenį ir gali būti naudojami kartu su įvairiomis technologijomis[162]. Pavyzdžiui, piršto atspaudų duomenys gali nurodyti įvairias genetines anomalijas ar polinkį į tam tikras ligas. Be to, jie palieka pėdsaką, o naudojant pėdsakus paliekančius biometrinius duomenis iškyla reali grėsmė, kad jie bus renkami ir saugomi be asmens sutikimo. Veido atvaizdo biometriniai duomenys gali būti naudojami kartu su nuotolinio veido atpažinimo technologija, kuri leidžia identifikuoti asmenį ir sekti jį per atstumą be jo žinios ir sutikimo. Taip iškyla reali piktnaudžiavimo ir visuotinės kontrolės grėsmė. Dar iki šių įstatymų priėmimo Europos Parlamentas siūlė uždrausti biometrinius duomenis kaupti duomenų bazėse ir leisti juos saugoti tik asmens dokumente. Į duomenų bazes galima įsilaužti, klastoti, keisti ir naikinti jose saugomus biometrinius duomenis. Saugant biometrinę informaciją įvairiose duomenų bazėse, kyla duomenų bazių susijungimo ir

privataus gyvenimo gerbimą? (Teisės magistro darbas, Vytauto Didžiojo Universitetas, 2008.). P. 15. https://www.vdu.lt/cris/entities/etd/7165d9d1-7a2c-4f14-a0e3-923ea1c4c04d/details

[159] LR Asmens tapatybės kortelės ir paso įstatymas, 2014 m. gruodžio 23 d. Nr. XII-1519.

[160] Lietuvos Respublikos tarnybinio paso įstatymas, Nr. XIII-2297, 2019-07-09. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.94414/asr

[161] LR Gyventojų registro įstatymo pakeitimo ir papildymo įstatymas, Nr. XII-1297, 2014 m. lapkričio 6 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/a00ba9d068d111e48710f0162bf7b9c5 .

[162] https://www.tv3.lt/naujiena/projektai/269433/butina-issami-diskusija-apie-planuojama-biometriniu-duomenu-naudojima

nekontroliuojamo duomenų panaudojimo rizika. Taip būtų sukurta ypač patogi infrastruktūra valstybei sužinoti apie asmenis beveik viską[163].

Šiandien daugiausia klausimų kyla dėl centralizuoto biometrinių duomenų saugojimo Gyventojų registre. LR Gyventojų registro įstatymo[164] 4 straipsnyje nustatyta, kad LR Gyventojų registras yra pagrindinis valstybės registras**.** Šio straipsnio 2 dalyje nurodyta registro paskirtis - rinkti, kaupti, apdoroti ir saugoti šiame įstatyme išvardytus duomenis apie asmenis; teikti šiuos duomenis Lietuvos Respublikos valdžios institucijoms, viešojo administravimo subjektams, kitiems valstybės registrams ir valstybės informacinėms sistemoms, kitiems juridiniams asmenims, jų filialams, atstovybėms, įstatymų nustatytas funkcijas atliekantiems valstybės įgaliotiems asmenims, taip pat fiziniams asmenims įstatymų ir kitų teisės aktų nustatyta tvarka. Remiantis Gyventojų registro įstatymo 11 straipsnio 5 punktu ir Gyventojų registro nuostatais[165], teisėtvarkos, žvalgybos ir asmens dokumentus išduodančioms įstaigoms gali būti teikiami asmens veido atvaizdas, pirštų atspaudai ir parašas, valstybės institucijoms juridinę galią turintiems dokumentams gaminti teikiami asmens veido atvaizdas ir parašas, tačiau tik tuo atveju, jeigu yra asmens sutikimas. Veido atvaizdas gali būti teikiamas finansų įstaigoms tik tų asmenų, kuriems ketinama suteikti finansines paslaugas, susijusias su rizikos prisiėmimu. Veido atvaizdas taip pat teikiamas sveikatos priežiūros įstaigoms nenustatytos asmens tapatybės pacientų asmens tapatybei patvirtinti ir (ar) nustatyti, notarams ir antstoliams – teisės aktuose nustatytoms funkcijoms atlikti, kai to reikia kaip papildomos kokiems tikslams asmens identifikavimo priemonės asmens tapatybei nustatyti, o institucijoms, atliekančioms nelegalaus darbo, nedeklaruoto darbo ir nedeklaruotos savarankiškos veiklos kontrolę, – tiek, kiek tai būtina asmens tapatybei nustatyti atliekant šią kontrolę. Įstatyme vis dar išlieka atviras klausimas,

[163] https://www.tv3.lt/naujiena/projektai/269433/butina-issami-diskusija-apie-planuojama-biometriniu-duomenu-naudojima
[164] LR Gyventojų registro įstatymas *Nr. XII-1297,* 2014-11-06.
[165] Lietuvos Respublikos Vyriausybės Nutarimas dėl Lietuvos respublikos gyventojų registro nuostatų patvirtinimo, 2014 m. gruodžio 23 d. Nr. 1495, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/478d0920903111e48028e9b85331c55d/asr

kokiems tikslams ir kokiais atvejais asmens biometriniai duomenys teikiami teisėtvarkos ir žvalgybos institucijoms.

Atsižvelgiant į LR Gyventojų registro paskirtį bei jo sąsajas su kitais valstybės registrais, biometrinių duomenų centralizuotas saugojimas valstybės mastu padidina šių duomenų naudojimo kaip rakto, susiejančio skirtingas duomenų bazes ir įgalinančio apibūdinti asmenų įpročius, galimybę[166]. Valstybės įmonė Registrų centras yra Gyventojų registro tvarkytojas, įgaliotas Gyventojų registro valdytojo - Lietuvos Respublikos teisingumo ministerijos, registruoti Gyventojų registro objektus, tvarkyti duomenis ir kartu su Teisingumo ministerija pagal kompetenciją atsako už duomenų saugą. Tačiau 2020 metų liepos mėnesio įvykiai, kuomet liūtis užliejo Registrų centro patalpas[167] ir serverinę, sukėlė daug abejonių dėl centralizuotame registre saugomų biometrinių duomenų saugumo bei galimų grėsmių fiziniams asmenims, jei duomenys būtų sugadinti, sunaikinti ar patektų į neįgaliotų asmenų rankas. Atkreiptinas dėmesys ir į tai, kad vis dar nėra reglamentuojamas įstatymais privataus verslo renkamų, kaupiamų ir tvarkomų fizinių asmenų biometrinių duomenų bazių administravimas. Visa atsakomybė paliekama tik verslo atitikčiai Reglamento nuostatoms.

---

166 Gecevičienė, O. *Ar biometrinių duomenų (skaitmeninių veido atvaizdo bei pirštų atspaudų) kaupimas bei saugojimas gyventojų registre nepažeidžia asmens teisės į privataus gyvenimo gerbimą?* (Teisės magistro darbas, Vytauto Didžiojo Universitetas, 2008). P.25. https://www.vdu.lt/cris/entities/etd/7165d9d1-7a2c-4f14-a0e3-923ea1c4c04d/details

167 Karsokaitė, V. *Liūtis, užpylusi Registrų centro serverinę, sutrikdė ir NT vertintojų darbą*. https://www.15min.lt/verslas/naujiena/kvadratinis-metras/nekilnojamasis-turtas/del-uzpiltos-registru-centro-serverines-stringa-ir-nt-vertintoju-darbas-973-1350558, [Publikuota 2020.07.21.]

Išvados

Biometrinių duomenų nuskaitymo ir analizės technologijų plėtra ir besiplečiantis biometrinių duomenų panaudojimas kasdieniniame gyvenime sukuria privalumų ir naudų tiek fiziniam asmeniui, tiek valstybinėms institucijoms, tiek verslui.

Kalbant apie subjektus, turinčius prieigą prie centralizuotai saugomų biometrinių duomenų, svarbu užtikrinti, kad tai būtų tik kompetentingos institucijos bei aiškiai apriboti tikslai ir sąlygos biometrinių duomenų gavimui ir tvarkymui.

Siekiant užtikrinti fizinio asmens teises į privatumą ir duomenų apsaugą, didesnis dėmesys turėtų būti skiriamas asmens identifikavimui panaudojant kompleksinius sprendimus.

Siekiant apsaugoti fizinių asmenų privatumą ir užtikrinti jų biometrinių duomenų apsaugą, teisėtvarkoje turi būti aiškiai ir tiksliai reglamentuotas biometrinių duomenų naudojimas bei kaupimas tiek valstybinių institucijų, tiek privataus verslo duomenų bazėse.

Taigi, kol nėra aiškiai sureguliuotų LR teisės aktų, neapibrėžtas biometrinių duomenų naudojimas pažeidžia asmens teisę į privataus gyvenimo gerbimą.

Lietuvos duomenų
apsaugos pareigūnų
asociacija