



Mykolas Romeris
universitetas

Ar BDAR (ne)leidžia duomenų valdytojams užtikrinti saugumą: biometrinių technologijų panaudojimo ypatingos svarbos objektuose atvejis

Prof. Darius Šttilis

Tyrimas atliktas kartu su doc. Mariumi Laurinaičiu (MRU) ir
Egidijumi Vereniu (VDAI)

APIE „SolPriPa 2 WORK“ PROJEKTĄ

2021–2023 m. Valstybinė duomenų apsaugos inspekcija kartu su Mykolo Romerio universitetu įgyvendina „SolPriPa 2 WORK“ projektą „Sprendžiant privatumo paradoksą 2: aukštų duomenų apsaugos, kaip pagrindinės teisės, standartų skatinimas darbo vietoje“. Dvejų metų trukmės projektas iš dalies finansuojamas pagal Europos Sąjungos Teisių, lygybės ir pilietiškumo programą (2014–2020). Tai darbdavių ir darbuotojų informuotumo didinimo projektas apie asmens duomenų apsaugą darbo santykių kontekste.

Projekto tikslai:

1. Suteikti galimybę **darbdaviams** kurti asmens duomenų tvarkymo principus atitinkančią darbo aplinką.
2. Padėti **darbuotojams** ginti savo teisę į asmens duomenų apsaugą, kaip pagrindinę teisę, darbo vietoje.

Tikslinės auditorijos – darbuotojai, kurie yra silpnesnė darbo santykių šalis, ir darbdaviai, ypač tokie specialistai kaip duomenų apsaugos pareigūnai, personalo, komunikacijos, informacinių technologijų specialistai, kiti administracijų darbuotojai. Projekto metu numatyta didelį dėmesį skirti smulkiojo ir vidutinio verslo įmonėms, taip pat viešojo sektoriaus organizacijoms, tokioms kaip ministerijos ir joms pavaldžios institucijos, savivaldybės, teismai.

Veiklos. Įgyvendinant projektą vesti mokymai, parengtos gairės, moksliniai straipsniai, tinklalaidės, toliau vystoma mobilioji aplikacija „ADA gidas“.

Aktualios nuorodos

Projekto informacija internete (<https://vdai.lrv.lt/lt/naudinga-informacija/solpripa-2-work-projektas>)

Mobilioji aplikacija „ADA gidas“ (<https://vdai.lrv.lt/lt/naujienos/ada-gidas-mobilioji-programele-skirta-informacijos-sklaidai-apie-asmens-duomenu-apsauga>)



„SolPriPa 2 WORK“ projektas iš dalies finansuojamas pagal Europos Sąjungos Teisių, lygybės ir pilietiškumo programą (2014–2020).

Konferencijoje pateikiama tik renginio organizatorių nuomonė, jie visiškai atsako už turinį. Europos Komisija neprisiima jokios atsakomybės dėl poveikio, kurį gali sukelti šiame projekte pateikta informacija.

PROJEKTO PARTNERIAI



VALSTYBINĖ
DUOMENŲ
APSAUGOS
INSPEKCIJA



Mykolas Romeris
universitetas

Šiame pranešime kalbėsime apie:

- Problematiką ir apie ypatingos svarbos infrastruktūros apsaugos poreikį;
- Biometrinių technologijų rinką ir duomenų apsaugos poreikį;
- Biometrinių technologijų panaudojimo ES valstybėse teisinį reguliavimą ir praktiką;
- Biometrinių technologijų panaudojimo ne ES valstybėse praktiką ir tendencijas;
- Biometrinių technologijų panaudojimo iššūkiai saugant ypatingos svarbos informacinę infrastruktūrą.

Problematika ir apie ypatingos svarbos infrastruktūros apsaugos poreikis



- Gręsia didesnis pavojus nei bet kada;
 - Kibernetinės grėsmės. Hibridinės kibernetinės grėsmės ir ... vidinės grėsmės.
 - Tapatybės ir prieigos valdymas yra vienos aktualiausių saugumo priemonių organizacijoms, ketinant sumažinti saugumo spragas.
 - Labai svarbu: darbuotojų identifikavimas patenkant į atitinkamos infrastruktūros objektus.
-



Biometrinių technologijų rinka ir tendencijos

- Veido atpažinimo rinka;
- Balso atpažinimo rinka;
- Pirštų atspaudų atpažinimo rinka.

Tendencijos: tradicinius autentifikavimo metodus keičia naujausios biometrinės technologijos. Tų pačių slaptažodžių naudojimo problema.

Sritys, kuriose biometrinių technologijų panaudojimas yra išplėtotas:

- Finansų sritis;
- Sveikatos apsauga;
- Teisėsaugos sektorius.

Klausimas: kokios technologijos gali būti panaudotos ypatingos svarbos infrastruktūros darbuotojų identifikavimui ir autentifikavimui?

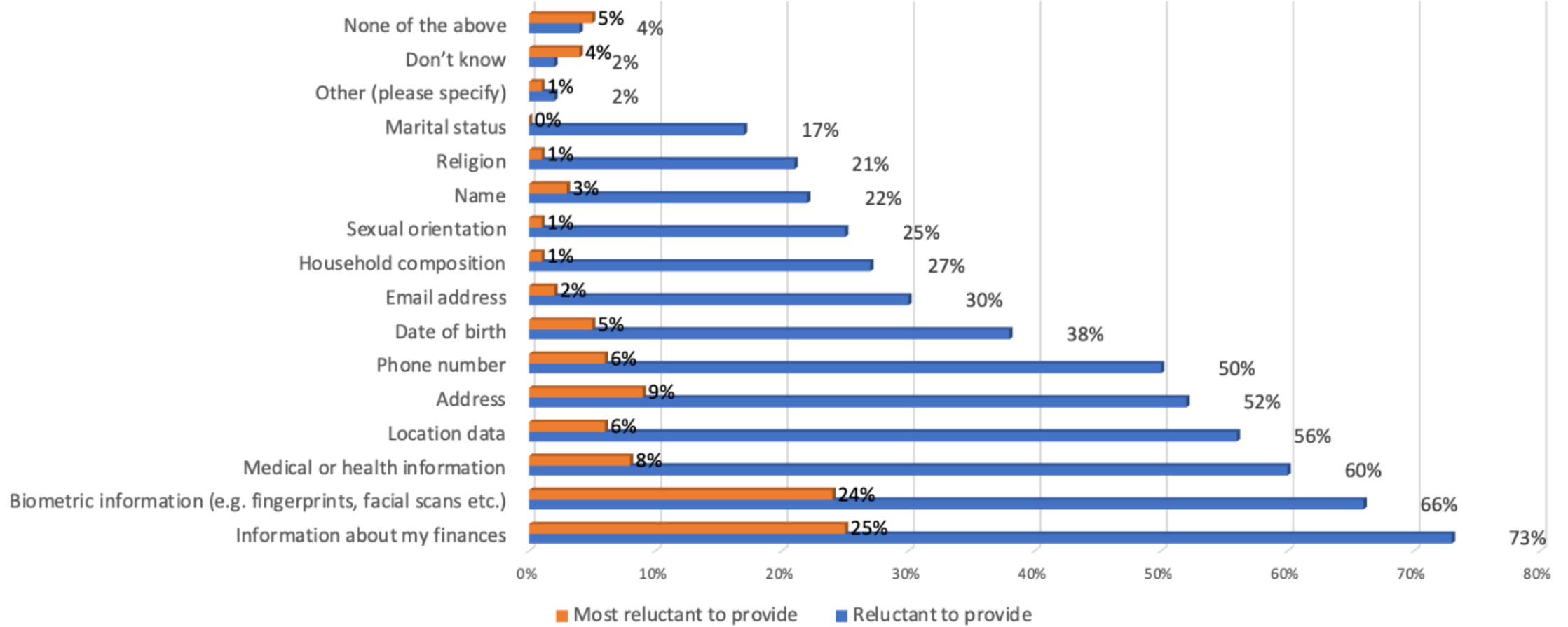


Biometrinių technologijų panaudojimas ES valstybėse: teisinis reguliavimas ir praktika

- Biometrinė informacija: spec. kategorijų asmens duomenys? Svarbu vertinimas. Filmuota vaizdo medžiaga kaip tokia – ne biometriniai duomenys.
- Ideali technologija, leidžianti „nepamiršti“ slaptažodžio vs biometrinių duomenų nepakeičiamumas.
- Iš biometrinių duomenų naudojimo kylanti rizika. Izraelio tyrėjų atliktas tyrimas.
- BDAR 6 ir 9 str.
- 2 variantai: siekiama nustatyti asmens tapatybę ir ne. Atitinkamai ir minimų BDAR straipsnių taikymas. „Neatsekama biometrika“.
- Clearview AI atvejis.



Type of information Australians are reluctant to provide to any organisation



Teisinio reguliavimo pavyzdžiai atskirose ES valstybėse



Biometriniai duomenys

Olandija

Nyderlandai įvedė nacionalinę išimtį, remdamiesi šiuo BDAR 9.2 str. b): Nyderlandų įstatymo 29 straipsnyje įgyvendinant BDAR, t. y. „kai tvarkymas būtinas autentifikavimo ar saugumo sumetimais“. Ši išimtis buvo priimta siekiant, kad darbuotojų biometrinių duomenų tvarkymas gali būti pateisinamas tais atvejais, kai negalima gauti galiojančio sutikimo.

Biometriniai duomenys

Vengrija

Darbo kodeksas numato, kad darbuotojo biometriniai duomenys gali būti tvarkomi siekiant užkirsti kelią neautorizuotai prieigai prie daikto ar informacijos dėl ko galėtų kilti rimta ar didžiulė žala darbuotojo ar kitų gyvybei, fiziniam integralumui ar sveikatai arba siekiant apginti svarbius įstatymo saugomus viešuosius interesus.

Biometriniai duomenys

Slovakija

Biometrinių duomenų tvarkymas dėl prieigos suteikimo numatytas, kai siekiama gauti prieigą prie branduolinių objektų.

Taip pat sukurtas teisinis reguliavimas dėl balso biometrinių duomenų tvarkymo, siekiant įsitikinti kliento tapatybę atliekant mokėjimus ir kitais teisės akte numatytais tikslais.

Biometriniai duomenys

Italija

Biometrinių duomenų tvarkymas leidžiamas dėl fizinės ar loginės prieigos suteikimo prie duomenų, jeigu taikomos tinkamos apsaugos priemonės.

Duomenų apsaugos priežiūros institucijų praktika dėl biometrinių duomenų



Biometriniai duomenys

Bulgarija

Banko balso biometrinių duomenų tvarkymas klientų identifikavimo tikslais, panaudojant kartu su kliento telefono numeriu ir paskutiniiais keturiais aktyvios banko kortelės numerio skaitmenimis: toks banko pasirinktas duomenų subjektų identifikavimo būdas galimas tik turint aiškų rašytinį duomenų subjekto sutikimą suteikiant galimybę pasirinkti alternatyvius identifikavimo būdus (iš metinės ataskaitos).

Biometriniai duomenys

Švedija

Mokyklai paskyrė administracinę baudą už veidų atpažinimo technologijos naudojimą mokyklos lankomumo tikslais. Švedijos priežiūros institucijos nuomone tokios technologijos naudojimas buvo neproporcingas siekiamiems tikslams. Taip pat mokinių ir jų tėvų sutikimai negali būti renkami, nes jie negali laisvai pasirinkti būti ar nebūti stebimais.

Biometriniai duomenys

Rumunija

Organizacijos tvarkomi darbuotojų veidų biometriniai duomenys darbo laiko apskaitos tikslais: toks biometrinių duomenų tvarkymas yra neteisėtas, nes yra neproporcingas siekiamiems tikslams. Organizacija siekiamus tikslus galėjo pasiekti mažiau privatumą ribojančiomis priemonėmis.

Biometriniai duomenys

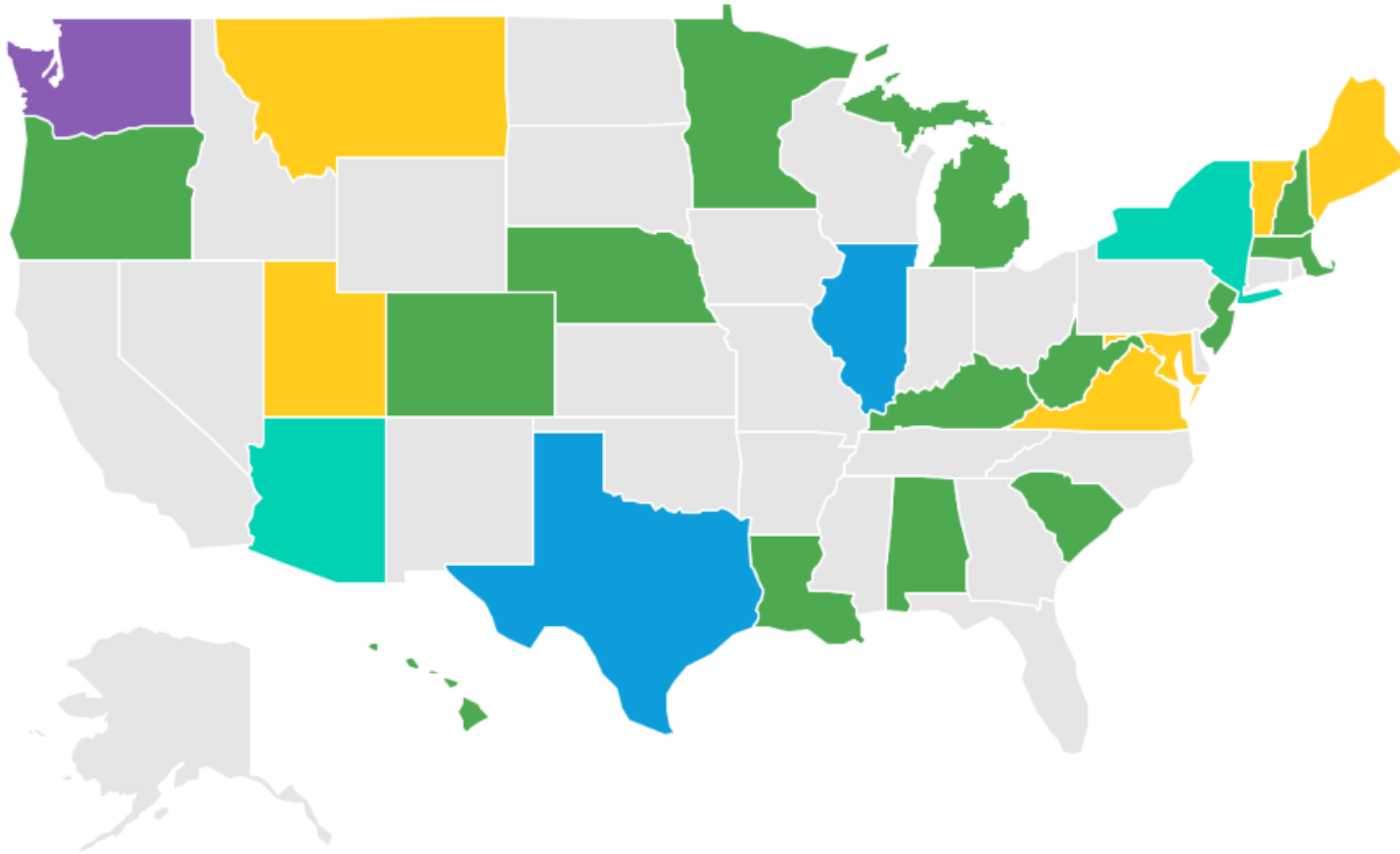
Italija

Paskyrė administracinę baudą už darbuotojų pirštų antspaudų tvarkymą siekiant užtikrinti darbuotojų buvimo darbe kontrolę. Italijos priežiūros institucijos nuomone toks duomenų tvarkymas buvo neproporcingas siekiamiems tikslams ir neturėjo teisinio pagrindo.

Teisinis reguliavimas, susijęs su biometrinių technologijų panaudojimu (ne ES valstybės)

- **Australija** (Privatumo įstatymas, Australijos informacijos komisieriaus gairės ir kt.) juda liberalesniu, tačiau kontroliuojamu keliu: rizikingiausi atvejai, kai asmuo, panaudojant biometrines technologijas gali būti identifikuotas, leidžiami tik įstatymų nustatytais atvejais ir tik tam tikroje srityse.
- **Kanadoje** yra leidžiama panaudoti biometrines technologijas darbo santykių kontekste tvarkant asmens duomenis (balso pavyzdžiai). Kol kas nėra specialių teisės normų, tačiau pasisakoma už papildomą teisinį biometrikos panaudojimo reguliavimą, tam, kad duomenų valdytojams būtų suteiktos aiškios gairės kokiais atvejais ir kaip naudoti biometriką.
- **JAV** – judama link specialaus reguliavimo, nors šiuo metu situacija atskirose valstijose yra labai įvairi.





- Biometrics & tailored facial recognition
- Biometrics (broad)
- Biometrics (tailored)
- Facial recognition (tailored)
- No proposed legislation
- Proposed bills

Biometrinių technologijų panaudojimo iššūkiai saugant ypatingos svarbos informacinę infrastruktūrą



- Dėl darbdavio ir darbuotojo galios disbalanso darbuotojo sutikimas / aiškus sutikimas negalioja?
 - Ar visuomet galimos alternatyvos (kad darbuotojo sutikimas būtų laisvanoriškas)?
 - **Rekomendacija** – ES valstybėse imtis papildomų reglamentavimo veiksmų.
 - Kylančių kibernetinių rizikų ir potencialios žalos visuomenei kontekste ypatingos svarbos infrastruktūros galėtų būti priskiriama prie sričių, kuriose biometrinių technologijų panaudojimas darbuotojų identifikavimui ir autentifikavimui būtų grindžiamas vadovaujantis ES Bendrojo duomenų apsaugos reglamento 6 str. 1 d. c punktu bei BDAR 9 str. 2 d. g punktu.
-



Mykolas Romeris
universitetas

AČIŪ UŽ DĖMESĮ!