Vilniaus universiteto Teisės fakulteto

Privatinės teisės katedra

Artūro Anisimenka,

V kurso, darbo ir socialinės teisės

studijų šakos studento

Magistro darbas

Darbuotojo asmens duomenų apsaugos iššūkiai

Employee Personal Data Protection Challenges

Vadovas: doc. dr. Justinas Usonis

Recenzentas: lekt. Arūnas Šuminas

Vilnius

2022

ANOTACIJA IR PAGRINDINIAI ŽODŽIAI

Šiame magistro darbe yra analizuojami BDAR reikalavimai ir su tuo susiję pagrindiniai taikymo iššūkiai darbo santykių srityje. Nagrinėjama darbo santykių šalių interesų pusiausvyros problematika asmens duomenų apsaugos aspektu. Identifikuojami konkretūs su darbuotojo asmens duomenų apsauga susiję iššūkiai ir pasiūlomi galimi teisiniai ir praktiniai sprendimai. Išsamiai išanalizuojama koronaviruso (COVID-19 ligos), nuotolinio darbo, darbuotojų atstovų įtaka duomenų apsaugos kontekste. Taip pat darbe prognozuojami ateityje galintys kilti duomenų apsaugos teisės iššūkiai darbo santykiuose (dirbtinis intelektas ir metavisata).

Pagrindiniai žodžiai: BDAR, darbas, sekimas, stebėsena, koronavirusas, dirbtinis intelektas, metavisata

This master's thesis analyses the requirements of GDPR and the related main application challenges in the field of labour relations. The issue of the balance of interests of the parties to the employment relationship in the field of personal data protection law is examined. Specific challenges related to the protection of employee personal data are identified and possibly legal and practical solutions are proposed. The influence of coronavirus (COVID-19 disease), teleworking, employee representatives in the context of data protection is analysed in detail. The thesis also predicts possible future data protection law challenges in the employment relationship (artificial intelligence and metaverse).

Keywords: GDPR, employment, surveillance, monitoring, coronavirus, artificial intelligence, metaverse

TURINYS

SANTRUMPŲ IR SĄVOKŲ SĄRAŠAS

BDAR arba Reglamentas	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).
Darbo kodeksas	Lietuvos Respublikos darbo kodeksas.
ES	Europos Sąjunga.
Asmens duomenys	bet kokio pobūdžio informacija (tiek tiesioginė, tiek netiesioginė), kuri yra susijusi su fiziniu asmeniu (duomenų subjektu) (BDAR 4 straipsnio 1 punktas).
Duomenų subjektas	gyvas fizinis asmuo, kurio tapatybė yra nustatyta arba gali būti nustatyta (BDAR 4 straipsnio 1 punktas). Šio magistro darbo kontekste įprastai bus laikomas darbuotoju.
Darbuotojas	fizinis asmuo, įsipareigojęs atlygintinai atlikti darbo funkciją pagal darbo sutartį su darbdaviu (Darbo kodekso 21 straipsnio 2 dalis).
Duomenų valdytojas	fizinis arba juridinis asmuo, kuris nustato asmens duomenų tvarkymo tikslus ir priemones (BDAR 4 straipsnio 7 punktas). Šio magistro darbo kontekste įprastai bus laikomas darbdaviu.
Darbdavys arba Bendrovė	asmuo, kurio naudai ir kuriam būdamas pavaldus darbo sutartimi darbo funkciją atlygintinai įsipareigojo atlikti fizinis asmuo (Darbo kodekso 21 straipsnio 3 dalis).
Duomenų tvarkytojas	fizinis arba juridinis asmuo, kuris duomenų valdytojo pavedimu tvarko asmens duomenis (BDAR 4 straipsnio 8 punktas).
Priežiūros institucija	nepriklausoma valdžios institucija, kuri prisideda prie nuoseklaus BDAR taikymo visoje ES ir nagrinėja skundus dėl BDAR pažeidimų. Kiekvienoje ES valstybėje narėje yra po vieną (BDAR 51 straipsnis).
Duomenų tvarkymas	bet kokiomis automatizuotomis ir neautomatizuotomis priemonėmis atliekamos asmens duomenų tvarkymo operacijos ar operacijų seka (rinkimas, sisteminimas, saugojimas, naudojimas, perdavimas, sujungimas, apribojimas, ištrynimas, sunaikinimas ir pan.) (BDAR 4 straipsnio 2 punktas).

ĮŽANGA

Informacija yra galia. XXI amžiuje įtaką formuojančia priemone yra asmens duomenų tvarkymas, kurio panaudojimas gali suteikti reikšmingą, o tuo pačiu ir konkurencingą pranašumą rinkoje. Duomenų turėjimas apie besikeičiančius ekonominius ir socialinius procesus, fizinių asmenų gyvenimą gali sukurti komercinę naudą ir leisti daryti įtaką kitiems (pavyzdžiui, Lietuvos Respublikos konkurencijos įstatymo 15 straipsnis). Priklausomai nuo to, kokie yra informacijos turėtojo panaudojimo tikslai, atitinkamai gali kilti teigiami arba neigiami padariniai. BDAR yra suformavęs fundamentalią viziją, jog asmens duomenys turėtų būti tvarkomi taip, kad tai pasitarnautų visai žmonijai (BDAR preambulės 4 punktas). Asmens duomenų tvarkymas XXI amžiuje yra neišvengiamas procesas. Paradoksalu, kad griežtas asmens duomenų tvarkymo taisykles įtvirtinančio teisės akto tikslas nėra asmens duomenų tvarkymo uždraudimas, o kaip tik skatinimas asmens duomenis panaudoti geriems, visuomeniniams tikslams. Ši vertybinė idėja gali būti paaiškinta tuo, kad BDAR neriboja asmens duomenų tvarkymo, o atvirkščiai siekia išgryninti tvarkomus asmens duomenis ir juos efektyviai panaudoti. BDAR yra papildomas saugiklis, kuris užtikrina, kad asmens duomenys bus adekvatūs ir tvarkomi aiškiai nustatytu tikslu, teisėtu, sąžiningu ir skaidriu būdu (BDAR 5 straipsnio 1 dalies a-c punktai).

Taigi, *prima facie* galėtų atrodyti, kad darbdavys turi absoliučią teisę stebėti kaip jo suteiktomis darbo priemonėmis naudojasi darbuotojas. Tarytum yra siekiama pozityvių tikslų: patenkinti darbdavio interesą apsaugoti turtą, užtikrinti darbuotojo produktyvumą ir gal net paties darbuotojo sveikatos apsaugą. Tačiau atsakymas kaip ir daugelyje teisinių situacijų gali būti ir taip, ir ne. Todėl, kad asmens laisvės baigiasi ten, kur prasideda kito asmens laisvės[1]. Būtent ši plona riba egzistuoja tvarkant darbuotojų asmens duomenis.

Temos aktualumas. Pirmiausiai, nagrinėjama tema yra patraukli dėl technologinės pažangos. Naujų priemonių naudojimas ypač paplito koronaviruso (COVID-19 ligos) ir nuotolinio darbo kontekste. Panašu, kad ateitis ruošiasi dar labiau asmens duomenų apsaugą ribojančioms priemonėms.

Antra, pasirinkta tema yra nepakankamai ištirta Lietuvos teisės moksle. Plačiau technologinės pažangos rizikas įžvelgė dr. G. Tamašauskaitė-Janickė. Naujausias įžvalgas, problematiką, darbuotojų asmens duomenų tvarkymo ypatumus tiria lekt. R. Grigonienė. Tuo tarpu

[1] Ši mintis priklauso rašytojui Alfred George Gardiner (1865-1946).

užsienio teisės mokslininkų ši tema nagrinėjama dažniau ir išsamiau. Išsamius tyrimus dėl BDAR įtakos darbuotojo asmens duomenų tvarkymui yra atlikę prof. K. Ball, prof. M. T. Bodie, dr. C. Ogriseg, I. Mandl, J. Nogarede ir kt. nagrinėti autoriai.

Trečia, tema yra svarbi darbo santykių šalims, kurie kasdien susiduria su teisiniais ir praktiniais iššūkiais tvarkant darbuotojų asmens duomenis (nuo įdarbinimo iki darbo santykių nutraukimo įforminimo). Taip atsiranda susikertanti riba: tarp darbdavio interesų apsaugos ir darbuotojo teisės į duomenų apsaugą. Riba dar labiau susiaurėja, kai turime omenyje, kad darbuotojas yra silpnesnioji darbo santykių šalis. Todėl, pagrįstai kyla klausimas: kaip pasiekti darbo santykių šalių pusiausvyros? Kokie yra pagrindiniai iššūkiai? Kaip juos įveikti?

Darbo originalumas. Lietuvos teisės moksle BDAR reikšmė darbuotojų asmens duomenų tvarkymui yra nagrinėta labai mažai. Praktikoje BDAR laikomas kaip labai sudėtingas, griežtas asmens duomenų tvarkymo taisykles įtvirtinantis, neaiškus teisinis instrumentas. Siekiant sukurti teisinį apibrėžtumą darbo santykiuose (Darbo kodekso 2 straipsnio 1 dalis) labai svarbūs tampa teisiniai ir praktiniai patarimai. Šis magistro darbas lyginant su praėjusių metų magistro darbu „BDAR ir darbo teisė“, G. Tamašauskaitės-Janickės, R. Grigonienės, V. Petkevičienė bei kitais užsienio moksliniais darbais yra ypatingas ir tuo, kad pirmą kartą pakankamai išsamiai nagrinėja darbuotojų stebėsenos, koronaviruso (COVID-19 ligos), darbuotojų atstovavimo aspektus darbuotojų asmens duomenų tvarkymo srityje. Taip pat verčia atkreipti dėmesį į tai, kaip technologinė pažanga gali ir toliau paveikti darbo santykių šalis. Todėl yra būtina identifikuoti pagrindinius darbuotojų asmens duomenų apsaugos iššūkius ir padėti darbo santykių šalims pasiruošti juos spręsti. Šis magistro darbas yra gausus praktiniais patarimais, rekomendacijomis, gairėmis, kurie bus naudingi tiek darbuotojui, tiek darbdaviui apsaugant savo interesus.

Tyrimo objektas. Šio darbo objektas yra pagrindiniai BDAR taikymo iššūkiai darbo santykiuose, t. y. BDAR reikšmė darbuotojų asmens duomenų tvarkymui.

Darbo tikslas. Šio darbo tikslas yra išsiaiškinti, kokie yra pagrindiniai su darbuotojų asmens duomenų tvarkymu susiję teisiniai ir praktiniai iššūkiai. Atsižvelgiant į tai, kad pasirinkta tema yra plati, šio magistro darbo kontekste, siekiama apibrėžti darbo santykių šalių pusiausvyrą tvarkant darbuotojų asmens duomenis. Taip pat aptarti, kaip tolimesnė technologinė plėtra gali paveikti darbo santykių šalis.

Darbo uždaviniai. Siekiant įgyvendinti apibrėžtą darbo tikslą, keliami šie uždaviniai:

1) atskleisti darbo santykiuose egzistuojančią darbuotojo asmens duomenų tvarkymo problematiką;
2) išnagrinėti pagrindinius darbuotojo asmens duomenų tvarkymo iššūkius ir pateikti pasiūlymus kaip juos spręsti;
3) ištirti, kokie yra potencialiai ateityje kylantys iššūkiai susiję su darbuotojo asmens duomenų tvarkymu.

Tyrimo metodai. Siekiant kompleksiškai atskleisti pasirinktą temą, naudojami šie tyrimo metodai: **i) sisteminis** – buvo išanalizuoti BDAR ir nacionaliniai teisės aktų reikalavimai darbo santykiuose, bei jų tarpusavio santykis; **ii) teleologinis** – analizuotas BDAR preambulės tekstas, kiti teisės norminiai aktai atskleidžiantys darbo santykių šalių teises ir pareigas, teisės normų paskirtis; **iii) lingvistinis** – paaiškinami BDAR, Lietuvos Respublikos teisės aktų reikalavimai darbuotojo asmens duomenų tvarkymo srityje, analizuojant jų gramatinę, morfologinę ir sintaksinę prasmę; **iv) loginis** – formuojami racionalūs praktiniai patarimai darbuotojo asmens duomenų tvarkymo srityje. Naudojami teisiniai argumentai siekiant sustiprinti teiginius, išvadas, konstatuoti teisinius ir praktinius iššūkius; **v) lyginamasis** – lyginamas BDAR suderinamumas su ES ir Lietuvos Respublikos teismų išaiškinimais, kitų ES priežiūros institucijų sprendimais; **vi) apibendrinamasis** – kiekviena dėstymo dalis apibendrinama tarpinėmis išvadomis, o darbo pabaigoje susisteminami ir pateikiami apibendrinimai iš visų nagrinėtų teisės šaltinių.

Svarbiausi šaltiniai. Pagrindiniai pirminiai šaltiniai buvo BDAR preambulės tekstas ir įtvirtinti BDAR reikalavimai, Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija, Europos Sąjungos pagrindinių teisių chartija, kiti tarptautiniai ir Europos Sąjungos norminiai teisės aktai, Lietuvos Respublikos darbo kodeksas, kiti nacionaliniai teisės norminiai aktai. Pagrindiniai antriniai šaltiniai buvo G. Tamašauskaitės-Janickės, R. Grigonienės, V. Petkevičienė *et al.*, K. Ball, M. T. Bodie, C. Ogriseg, I. Mandl, J. Nogarede ir kt. autorių doktrininiai darbai. Šiame darbe buvo vadovaujamasi šiais *soft law* šaltiniais: Europos Sąjungos 29 straipsnio duomenų apsaugos darbo grupės nuomonėmis, Europos duomenų apsaugos valdybos gairėmis, Valstybinės duomenų apsaugos inspekcijos rekomendacijomis. Taip pat reikšmingai analizuoti aktualūs Europos Žmogaus Teisių Teismo, Europos Sąjungos Teisingumo Teismo, Lietuvos vyriausiojo administracinio teismų išaiškinimai ir Europos Sąjungos valstybių narių priežiūros institucijų sprendimai.

1. Darbo santykių šalių interesų pusiausvyros problematika

Darbuotojo teisė į privataus gyvenimo gerbimą egzistuoja dešimtmečius. Darbo santykiams besiplečiant į interneto laikus atsirado poreikis užtikrinti duomenų apsaugą. Taip teisė į privatų gyvenimą pamažu transformavosi. Susiformavo nauja savarankiška teisė į duomenų apsaugą, kuri yra pripažįstama ir tarptautiniu lygmeniu (pavyzdžiui, ES pagrindinių teisių chartijos 8 straipsnis, Sutarties dėl ES veikimo 16 straipsnis). Žinoma, kad nacionaliniu lygmeniu ši apsauga taip pat galioja. Asmens susirašinėjimai, pokalbiai, bet kokio kitokio pobūdžio informacija apie asmens privatų gyvenimą yra neliečiami ir ginami įstatymų (Lietuvos Respublikos Konstitucija, 1992). Darbdavys turi pareigą užtikrinti darbuotojų teises į privataus gyvenimo neliečiamumą ir teises į duomenų apsaugą (Darbo kodekso 27 straipsnis). Visgi, tai neturėtų būti suprantama, kad asmens duomenų tvarkyti negalima. Anaiptol, atitinkamu atveju, netgi atvirkščiai, teisės aktai gali įtvirtinti pareigą darbdaviui tvarkyti darbuotojo asmens duomenis.

Tačiau, tai nereiškia, kad darbdavys turi tik pareigas. Tarptautiniu lygmeniu bendrovei yra pripažįstama laisvė užsiimti verslu (ES pagrindinių teisių chartija, 2016). Lietuvos Respublikos Konstitucijoje asmeniui laisvė turėti verslą yra laiduojama 48 straipsnyje (Lietuvos Respublikos Konstitucija, 1992). Taigi, darbdavys gali turėti pagrįstą interesą ginti savo verslo interesus. Darbo santykiuose kaip viena problematiškiausių situacijų gali būti sankirta tarp darbdavio ir darbuotojo interesų. Darbdavys turi pareigą suteikti reikalingas darbo priemones darbuotojui (Darbo kodekso 31 straipsnio 1 dalis), tuo tarpu darbuotojas turi pareigą tausoti turtą, naudotis darbo priemonėmis pagal paskirtį taip apsaugodamas bendrovės (ne)turtinius interesus (Darbo kodekso 31 straipsnio 2 dalis). Todėl darbdavys turi visapusišką teisę kontroliuoti kaip darbuotojas laikosi savo pareigų ir ne tik šiame kontekste.

Taigi, pirma, problema yra dėl skirtingų interesų: darbdavio teisė kontroliuoti kaip darbuotojas laikosi prisiimtų įsipareigojimų prieš darbuotojo teisę į duomenų apsaugą. Taip pat darbdavys turi plačią sprendimų diskreciją, gali daryti įtaką darbuotojo padėčiai darbovietėje. Darbuotojas yra pavaldus darbdavio nurodymams (Darbo kodekso 32 straipsnio 2 dalis). Ši interesų pusiausvyros problematika buvo išsamiai atskleista Europos Žmogaus Teisių Teisme (*Bărbulescu* prieš Rumuniją ..., 2017). Toliau darbo santykių šalių interesų pusiausvyros problematika nagrinėjama darbuotojo asmens duomenų tvarkymo teisėtumo ir skaidrumo aspektais.

1.1. Darbuotojo asmens duomenų tvarkymas teisėtumo aspektu

Natūralu, kad darbuotojas, gali pagrįstai tikėtis, jog jo asmens duomenys darbo santykių metu bus tvarkomi teisėtai (Darbo kodekso 2 straipsnio 1 dalis). Tiek darbdavys, tiek darbuotojas turi bendradarbiauti ir pasitikėti vienas kitu. Kitaip darbo santykiai nebus sėkmingi ir nei vienai iš šalių nesusiklostys palankiai. Darbdavys turi pareigą darbuotojo asmens duomenis tvarkyti teisėtai, sąžiningai ir skaidriai (BDAR 5 straipsnio 1 dalies a punktas). Teisėtumo sąlyga yra grindžiama remiantis vienu iš alternatyvių asmens duomenų tvarkymo teisinių pagrindų (BDAR preambulės 40 punktas).

Tačiau kaip jau minėta anksčiau, darbuotojo asmens duomenų tvarkymas yra dviejų interesų sankirta. Todėl yra svarbu, kad abi šalys stengtųsi suderinti savo interesus ir pasiektų jų pusiausvyros (Darbo kodekso 24 straipsnis). Šiuo aspektu toliau bus nagrinėjami ne visi asmens duomenų tvarkymo teisiniai pagrindai, bet tik tie, kurie yra vieni iš problematiškiausių darbo santykiuose, t. y. asmens duomenų tvarkymas sutikimo ir teisėtų interesų pagrindais.

Darbuotojo asmens duomenų tvarkymas remiantis sutikimu. Įprastai praktikoje duomenų valdytojas klaidingai mano, kad sutikimas yra *saugiausias* teisinis pagrindas. Darbdaviui gali atrodyti, jog bus lengviau pagrįsti turint raštu pasirašytą darbuotojo sutikimą. Teisės aktai netgi įtvirtina pareigą saugoti sutikimą vienerius metus (Lietuvos vyriausiojo archyvaro įsakymas ..., 2011). Tikimasi, kad bus išvengta nesklandumų. Visgi, taip nėra. Duomenų subjekto sutikimas – laisva valia duotas (savanoriškas), konkretus ir tinkamai informuotas (nedviprasmiškas), valios išreiškimas žodžiu, raštu ar konkliudentiniais veiksmais, kad būtų tvarkomi asmens duomenys (BDAR 4 straipsnio 11 punktas). Reglamentas įtvirtina sutikimo sąlygas (BDAR 7 straipsnis), kurias turi realizuoti kiekvienas darbdavys besiremiantis sutikimo pagrindu, įskaitant darbuotojo teisę atšaukti savo sutikimą.

Paprastai darbo santykiuose sutikimas negalės būti laikomas laisva valia duotu. Europos duomenų apsaugos valdyba savo gairėse pažymi darbo santykių galios disbalansą (Europos duomenų apsaugos valdyba, 2020c, p. 9). Taip susiklosto todėl, kad būtent darbdavys turi didžiausią įtaką iš anksto nustatydamas tvarką darbovietėje, o darbuotojas privalo jai paklusti (Darbo kodekso 32 straipsnio 2 dalis). Lekt. R. Grigonienė pritaria šiai pozicijai ir atkreipia dėmesį, kad net ir tuo atveju, jeigu sutikimo laisvanoriškumas būtų įgyvendintas, iššūkių gali kilti su kitomis sutikimo sąlygomis. Grigonienė taip pat skiria dėmesį darbuotojo biometrinių asmens duomenų tvarkymui sutikimo pagrindu (Grigonienė, 2020, p. 350-351).

Biometriniai duomenys (asmens veidas, balsas, piršto antspaudai, akies rainelė ir pan.) yra specialiųjų kategorijų asmens duomenys (BDAR 9 straipsnio 1 dalis), kuriuos tvarkyti galima tik esant tam tikros papildomoms sąlygoms (BDAR 9 straipsnio 2 dalis). Tokių asmens duomenų atskleidimas sukeltų didesnių pasekmių asmenų teisėms ir laisvėms. R. Grigonienė teigia, kad sutikimas neturėtų būti naudojamas kaip teisinis pagrindas (Grigonienė, 2020, p. 368). Šią poziciją patvirtina ir žemiau aptartos praktinės situacijos.

Lietuvos Respublikos teismų praktikoje jau yra išaiškinimų dėl darbuotojo biometrinių asmens duomenų tvarkymo. Pavyzdžiui, bendri duomenų valdytojai tvarkė darbuotojų pirštų antspaudus vidaus administravimo tikslais. Iš pradžių darbuotojai buvo supažindinti per susirinkimą žodžiu, vėliau po institucijų patikrinimų gauti jų sutikimai raštu. Teismas konstatavo, kad bendrovės neteisėtai tvarkė darbuotojų asmens duomenis, netinkamai supažindino darbuotojus su savo teisėmis (Lietuvos vyriausiojo administracinio teismo 2020 m. balandžio 2 d. sprendimas administracinėje byloje Nr. A-3345-822/2020). Nagrinėta situacija ypatinga ir dėl to, kad darbuotojai buvo iš mažo miestelio. Tokiu būdu sumažinant darbuotojams pasirinkimų laisvę nesutikti ir kylant dar didesnei rizikai jų duomenų saugumui.

Visiškai panaši situacija įvyko Nyderlandų Karalystėje. Tik šiuo atveju, priežiūros institucija paskyrė realią 725,000 EUR baudą. Tarnyba nenustatė, kad bendrovė patektų į išimtis, kai galima tvarkyti darbuotojų biometrinius asmens duomenis. Bendrovė nepagrindė, kad būtų turėjusi aiškiai išreikštus darbuotojų sutikimus ar būtų tvarkiusi asmens duomenis dėl teisėtų interesų (Nyderlandų duomenų apsaugos tarnybos 2020 m. balandžio 30 d. sprendimas).

Tačiau nereikėtų manyti, kad darbdavys negali apskritai tvarkyti biometrinių darbuotojo asmens duomenų. Darbdavys gali turėti interesą viešinti darbuotojo atvaizdą internete (pavyzdžiui, komunikacijos su klientais; įvaizdžio formavimo tikslais). Kaip vienas iš teisinių pagrindų gali būti sutikimas, jeigu atitinka aptartas sutikimo sąlygas. Sutikimas neprivalo būti žodžiu ar raštu. Sutikimas konkliudentiniais veiksmais yra galimas. Administracinis teismas šią nuostatą neseniai patvirtino. Asmuo suprato ir savo noru atvyko į filmavimus, prisisegė mikrofoną, turėjo suderintą tekstą, neprieštaravo būti filmuojamas (Lietuvos vyriausiojo administracinio teismo 2022 m. vasario 9 d. nutartis administracinėje byloje Nr. eA-146-415/2022). Taigi, svarbu įsivertinti: i) duomenų tvarkymo tikslą; ii) pasirinkti reikalingą teisinį pagrindą; iii) gebėti įrodyti, kad atitinka BDAR reikalavimus (BDAR 5 straipsnio 2 dalis). Atsižvelgiant į reikalavimus ir riziką, sutikimas turėtų būti *ultima ratio* darbo santykiuose.

Darbuotojo asmens duomenų tvarkymas teisėtų interesų pagrindais. Reglamentas įtvirtina alternatyvų teisinį pagrindą, t. y. kai tvarkyti asmens duomenis būtina siekiant teisėtų duomenų valdytojo arba trečiosios šalies interesų ir tik tuo atveju, kai tokie interesai yra viršesni už duomenų subjekto interesus (BDAR 6 straipsnio 1 dalies f punktas). Šis teisinis pagrindas skiriasi nuo sutikimo: i) subjektų skaičiumi – galima remtis tiek duomenų valdytojo, tiek trečiosios šalies interesais; ii) žymiai lankstesnis, nes įvedama vertinamoji sąvoka „interesas“ – kuri gali būti plačiai suprantama. Asmens duomenų apsaugos prasme yra svarbus duomenų tvarkymo tikslas. Interesas gali būti paaiškintas kaip poreikis tvarkyti asmens duomenis, kuris suteikia naudą duomenų valdytojui arba visuomenei (ES 29 straipsnio duomenų apsaugos darbo grupė, 2014, p. 24). Remiantis šiuo pagrindu reikia atlikti teisėtų interesų balanso testą. Atliekant testą, reikia visapusiškai atsižvelgti į daugelį veiksnių, siekiant užtikrinti, kad būtų tinkamai atsižvelgta į duomenų subjektų interesus ir pagrindines teises (ES 29 straipsnio duomenų apsaugos darbo grupė, 2014, p. 3). Kada galima remtis teisėtų interesų pagrindu? Kokias sąlygas turi atitikti?

Pirma, turi būti teisėtas interesas, kurių siekia duomenų valdytojas arba trečioji šalis. Reiškia, kad tai negali prieštarauti nacionaliniams teisės aktams. Turi būti suformuotas pagrįstas duomenų tvarkymo tikslas. Pavyzdžiui, Europos Sąjungos Teisingumo Teismo byloje buvo įvardinta, kad teisėtas interesas yra pagrįstas ketinimu pareikšti ieškinį žalą padariusiam asmeniui (*Rīgas satiksme ...,* 2017). Duomenų apsaugos darbo grupė įvardija, kad teisėtas interesas gali būti ir darbuotojų stebėjimas darbuotojų saugumo, jų kontrolės, darbdavio fizinio turto, IT ir tinklo saugumo valdymo tikslais (ES 29 straipsnio duomenų apsaugos darbo grupė, 2014, p. 25). COVID-19 ligos kontekste ypač didžiulę reikšmę galėjo turėti darbdavio pareiga užtikrinti saugias darbo sąlygas (Darbo kodekso 158 straipsnis).

Darbuotojo stebėsena gali būti ypač intensyvi, aktyvi naudojantis elektroninėmis priemonėmis. Darbdavys naudodamasis informacinėmis technologijomis gali pasitelkti įvairias technines ir organizacines priemones, kurių pagalba būtų surinkti dideli kiekiai informacijos apie darbuotoją (įskaitant metaduomenis). G. Tamašauskaitė-Janickė atkreipia dėmesį, kad būtent šiame kontekste atsiranda didžiausia rizika darbuotojo teisei į privatų gyvenimą (Tamašauskaitė-Janickė, 2016, p. 82). Taigi, svarbu turėti aiškų duomenų tvarkymo tikslą, kuriuo siekiama naudos sau arba kitiems. Taip pat atsižvelgti į galimas rizikas darbuotojo teisei į privataus gyvenimo gerbimą ir įsivertinti suformuotus teisėtus interesus toliau aptariamomis sąlygomis.

Antra, galima tvarkyti darbuotojo asmens duomenis tik tokia apimtimi, kuri yra būtina ir proporcinga siekiamiems duomenų tvarkymo tikslams. Pavyzdžiui, asmens kodas gali būti privaloma asmens duomenų kategorija siekiant pareikšti ieškinį, nes kitu atveju tai būtų neįmanoma (*Rīgas satiksme* ..., 2017). Bendrovė, priklausanti įmonių grupei, gali turėti teisėtą interesą tvarkyti darbuotojo asmens duomenis, kuriuos perduotų kitai bendrovei (darbo laiko apskaita, darbuotojo pareigybių pavadinimas, darbo užmokesčio dydis). Šiuos duomenis tvarkytų žmogiškųjų išteklių administravimo tikslais, pavyzdžiui, siekiant išmokėti darbo užmokestį darbuotojams (BDAR preambulės 48 punktas). Todėl yra ne tik svarbu turėti teisėtą interesą tvarkyti darbuotojo asmens duomenis, bet tuo pačiu atlikti teisinį ir praktinį vertinimą: kokie asmens duomenys iš tiesų yra reikalingi atitinkamiems duomenų tvarkymo tikslams pasiekti; ar gebėsiu argumentuoti kam to reikia? (BDAR 5 straipsnio 2 dalis). Iš esmės, praktinis patarimas būtų kiekvieną asmens duomenų kategoriją įsivertinti: ar ji tikrai yra būtina.

Trečia, teisėti interesai yra viršesni už duomenų subjekto pagrindines teises ir laisves. Kaip žinia, teisė į asmens duomenų apsaugą nėra absoliuti (BDAR preambulės 4 punktas). Siekiant patikrinti šį santykį svarbu nustatyti, ar pats duomenų subjektas, asmens duomenų rinkimo kontekste, gali pagrįstai tikėtis, kad atitinkami duomenys galimai bus tvarkomi vienokiu ar kitokiu tikslu (BDAR preambulės 47 punktas). Tarp šalių yra pakankamas santykis, jog būtų įmanoma remtis šiuo teisiniu pagrindu. Darbuotojas dirbantis pagal darbo sutartį bendrovėje, gali pagrįstai tikėtis, kad atitinkami asmens duomenys apie jį neišvengiamai bus tvarkomi. Asist. dr. J. Zaleskis pastebi, kad siekiant suderinti darbdavio ir darbuotojo interesus, reikšmę turi teigiami duomenų tvarkymo rezultatai ir neigiami tokio asmens duomenų tvarkymo padariniai (Zaleskis, 2019, p. 162). Šiame kontekste yra svarbi Europos Žmogaus Teisių Teismo byla, kuri detalizuoja dviejų šalių interesų priešpriešą. Darbuotojo teisę į asmens duomenų apsaugą ir darbdavio teisę vykdyti darbuotojo priežiūrą.

Teismas šioje byloje įvertino, kad turi būti atsižvelgta į darbdavio kontrolės apimtį: asmens duomenų kategorijas, priemones, intensyvumą. Taip pat darbdavio gebėjimą pagrįsti savo teisėtus interesus, asmens duomenų tvarkymo būtinumą, t. y. ar nėra kitų alternatyvių priemonių, kurios mažiau ribotų asmens teises. Visgi teismas sutiko, kad darbdavys turėjo teisėtą interesą užtikrinti gerą bendrovės veikimą, bei pasirinkti tam tikslui reikalingas priemones. Tačiau pažymėjo, kad darbdavys neįspėjo iš anksto (prieš pradėdamas asmens duomenų tvarkymą) darbuotojo apie galimą darbuotojo stebėseną (*Bărbulescu* prieš Rumuniją ..., 2017). Todėl, asmens duomenų

tvarkymo skaidrumas yra ypač reikšmingas darbo santykiuose. Šalys turi bendradarbiauti, keistis tarpusavyje darbo santykiams reikalinga informacija (Darbo kodekso 24 straipsnis). Nepakanka turėti tik teisėtą interesą ir gebėti pagrįsti asmens duomenų tvarkymo būtinumą. Svarbu atsižvelgti į visas faktines aplinkybes susijusias su asmens duomenų tvarkymu.

Šiame kontekste yra svarbu ir tai, kad bendrovė pradėdama naujas asmens duomenų tvarkymo operacijas, diegdama naujas technologijas vadovautųsi pritaikytosios duomenų apsaugos ir standartizuotosios duomenų apsaugos principais (BDAR 25 straipsnis). Šių principų įgyvendinimas duomenų valdytojams padėtų pagrįsti savo asmens duomenų tvarkymo būtinumą ir pasirinktas proporcingas priemones. Todėl sutiktina su prof. Davulio nuomone, kad kuo daugiau yra siekiama surinkti informacijos apie darbuotoją, tuo labiau turi būti siekiama pagrįsti teisėtą interesą, bei pasirinkti tinkamas technines ir organizacines priemones, kurios būtų proporcingos (Davulis, 2018, p. 119). Prof. Ball, pažymi, kad bendrovės valdymo interesai apima ir pačių duomenų saugumą, t. y. užtikrinti duomenų atkūrimą, praradimo prevenciją ir pan. (Ball, 2021, p. 71). Atsižvelgiant į tai, tvarkant darbuotojų asmens duomenis svarbu pasirinkti apsaugą užtikrinančias saugumo priemones.

Apibendrinant, galima pagrįstai teigti, kad tiek darbdavys, tiek darbuotojas gali turėti skirtingus interesus, bet svarbu juos derinti. Asmens duomenų tvarkymą grindžiant sutikimo pagrindu: i) darbuotojas privalo turėti teisę pasirinkti, turėti galimybę nesutikti su asmens duomenų tvarkymu ir neturėti neigiamų pasekmių; ii) darbdavys turi teisę tvarkyti darbuotojo asmens duomenis, įskaitant specialiųjų kategorijų asmens duomenis, jeigu yra įgyvendinamos sutikimo sąlygos. Asmens duomenų tvarkymą grindžiant teisėtų interesų pagrindu: i) darbdavys remdamasis savo arba trečiųjų šalių interesais turi teisę tvarkyti darbuotojo asmens duomenis; ii) darbuotojo teisė į asmens duomenų apsaugą gali būti ribojama, bet nepaisant to, turi teisę būti informuotas apie asmens duomenų tvarkymą.

Užtikrinant darbo santykių šalių interesų pusiausvyrą svarbu iš anksto apibrėžti duomenų tvarkymo tikslus, tokių duomenų būtinumą, bei pasirinkti tinkamas technines ir organizacines priemones, kurios užtikrintų asmens duomenų apsaugą.

1.2. Darbuotojo asmens duomenų tvarkymas skaidrumo aspektu

Darbuotojo asmens duomenys turi būti tvarkomi skaidriu būdu, ypač, kai darbdavys pasirenka naudoti vis labiau intensyvesnes stebėsenos priemones. Darbuotojas turi teisę būti informuotas apie tai, kokiais tikslais, kokia apimtimi, kokiu būdu yra tvarkomi jo asmens duomenys (BDAR 13 straipsnis). Informacija apie darbuotojo asmens duomenų tvarkymą turi būti pateikta lengvai prieinama ir suprantama, aiškia ir paprasta kalba. Negana to, darbuotojas turėtų būti supažindintas su galimomis asmens duomenų saugumo rizikomis, bei galimybėmis pasinaudoti savo kaip duomenų subjekto teisėmis (BDAR preambulės 39 punktas). Darbo santykiuose neturėtų būti pateisinamas joks slaptas asmens duomenų tvarkymas. Tuo atveju, kai asmens duomenų tvarkymas yra grindžiamas darbuotojo sutikimo teisiniu pagrindu, skaidrumo reikšmė tik išauga (Europos duomenų apsaugos teisės vadovas, 2018, p. 122-123). Pasirinkus tvarkyti darbuotojo vaizdo ir (ar) garso asmens duomenis, darbdavys privalo pasirašytinai ar kitu įrodančiu būdu supažindinti darbuotojus (Lietuvos Respublikos asmens duomenų ... įstatymas, 1996). Taigi, skaidrumo principas reiškia, kad darbuotojas turėtų gebėti aiškiai suprasti, kaip yra tvarkomi jo asmens duomenys.

Darbuotojams turi būti suteikta teisė žinoti apie asmens duomenų tvarkymo operacijas tam, kad jie galėtų jas kontroliuoti. Prof. Ball pažymi, jog skaidrumo principo įgyvendinimas yra būtinas darbo santykiuose, kitu atveju, būtų paneigta darbuotojų teisė reikalauti ištaisyti, ištrinti asmens duomenis ar apriboti jų tvarkymą (Ball, 2021, p. 71-72). Darbuotojas, kuris nežino, kokie asmens duomenys yra tvarkomi, negali pasinaudoti savo teisėmis. Tinkamas darbuotojo informavimas yra būtinas. Stanev akcentuoja, jog informavimas neturėtų apsiriboti tik, kai jau yra vykdomas asmens duomenų tvarkymas. Atvirkščiai, supažindinimo pareiga turėtų būti įgyvendinta dar prieš pradedant rinkti asmens duomenis. Tokiu būdu suteikiant galimybę darbuotojui atlikti prevencinius veiksmus (Stanev, 2019, p. 103). Darbuotojas žinodamas apie savo asmens duomenų tvarkymą turės galimybę užginčyti neteisėtą tvarkymą.

Skaidrumo principo įgyvendinimas turi atsispindėti ir technologinėje pažangoje. Įprasti skaidrumo tikslai paseno ir nebeatitinka pirminių tikslų. Asmens duomenų tvarkymas skaidrumo aspektu atsinaujino kartu su naudojamomis informacinėmis ir komunikacinėmis sistemomis. Naujos technologijos asmens duomenų tvarkymo amžiuje gali sudaryti galimybes, kai darbdavys darbuotojo asmens duomenys rinks ir tvarkys slaptai, o informacijos kiekiai perkops visas įmanomas ribas (ES 29 straipsnio duomenų apsaugos darbo grupė, 2017, p. 8). Atsižvelgiant į

technologijų pažangą, asmens duomenų tvarkymas tampa vis labiau intensyvesnis. Darbdavys gali rinkti ne tik įprastai suprantamus tiesioginius asmens duomenis, bet taip pat išgauti informaciją apie jo naudojimosi patirtį, elgesį susijusį su tam tikra darbo priemone. Darbuotojo privataus ir profesinio gyvenimo atskyrimas pamažu nyksta. Darbuotojo asmens gyvenimas tampa neatsiejamai susijęs su darbu ir jo sukurtais duomenimis, ypač dirbant nuotoliniu būdu iš asmens gyvenamosios vietos. Skaidrumas negali apsiriboti tik informacijos pateikimu darbuotojui. Skaidrumas turi apimti ir pritaikytosios duomenų apsaugos principo įgyvendinimą. Reiškia tinkamą techninių ir organizacinių priemonių diegimą, piktogramų panaudojimą informacijos įsisavinimui.

Dirbtinio intelekto panaudojimas darbo santykiuose įgauna pagreitį. Dirbtinį intelektą siekiama panaudoti įdarbinimo procese. Užtikrinant greitesnį ir efektyvesnį darbuotojo įdarbinimo procesą. Taip pat surinkti gausybę asmens duomenų apie kandidatą, bei parduoti įdarbinimo agentūroms (Broecke, 2022). Tačiau dirbtinis intelektas gali apimti ne tik įdarbinimą, bet ir darbo santykių nutraukimą, kuris būtų automatizuotas. Tinkamas skaidrumo įgyvendinimas gali padėti jį suvaldyti. Dirbtinio intelekto algoritmai gali pasiekti ribą, kai jie bus tokie veiksmingi, jog taps nekontroliuojami. Todėl skaidrumo trūkumas gali pažeisti darbuotojų teises ir laisves (Aloisi *et al.,* 2019, p. 106). Algoritmai, kurie yra neoptimalūs ir nenaudingi darbuotojams silpnina darbuotojo padėtį. Tokių algoritmų panaudojimas gali sukurti atvirkščią situaciją – nesąžiningą ir neskaidrų asmens duomenų tvarkymą (Mandl, 2021, p. 17). Dirbtinio intelekto panaudojimas gali kelti grėsmę. Taikant tokius algoritmus darbo santykiuose yra svarbu išgryninti jų loginį pagrindimą ir apie tai supažindinti darbuotojus. Nustatyti standartinius nustatymus taip, kad būtų tvarkoma, kuo mažiau darbuotojo asmens duomenų.

Pasitelkiant vaizdo stebėjimą skaidrumo reikalavimas neišnyksta. Filmuojamose patalpose turi būti perspėjimo pranešimai, kurie būtų informatyvūs (Europos duomenų apsaugos valdyba, 2020a, p. 27). Informacija įtvirtinta BDAR 13-14 straipsniuose turėtų būti pateikta ne tik kaip lipdukai vietose, kurios patenka į filmavimo erdvę, bet taip pat ir vidinėse darbovietės tvarkose (Ball, 2021, p. 27). Siekiant įgyvendinti skaidrumo ir atskaitomybės principą geriausia dokumentuoti asmens duomenų tvarkymo operacijas (Petkevičienė *et al.,* 2020, p. 334). Viena iš priežasčių, kodėl įvyksta asmens duomenų tvarkymo pažeidimai yra ne dėl to, kad asmens duomenys *per se* tvarkomi neteisėtai, o todėl, kad darbuotojai nebuvo tinkamai informuoti apie asmens duomenų tvarkymą (ES 29 straipsnio duomenų apsaugos darbo grupė, 2001, p. 20).

Darbuotojo asmens duomenų apsaugos srityje siekiant skaidrumo turėtų būti įgyvendintos informavimo ir konsultavimo procedūros su darbuotojų atstovais (ES 29 straipsnio duomenų apsaugos darbo grupė, 2002, p. 15). Darbuotojų atstovai gali veikti asmens duomenų apsaugos srityje, teikti savo rekomendacijas, siūlymus ir reikalauti informacijos.

Darbuotojo asmens duomenų apsaugos politikos turi aiškiai deklaruoti skaidrumą, kokie duomenys, kokiais tikslais generuojami ir panaudojami (Mandl, 2021, p. 23). Politika gali būti parengta vadovaujantis šiais elementais: i) aiškumu; ii) prieinamumu; iii) tinkamumu; iv) universalumu; v) suprantamumu; vi) informacijos dalijimusi įvairiais kanalais ir panašiai (Europos duomenų apsaugos valdyba, 2020d, p. 15). Politika ir kiti vidiniai dokumentai reguliuojantys asmens duomenų apsaugą turi būti reguliariai peržiūrėti ir atnaujinti. Atsakingos priežiūros institucijos turi galimybę paskirti baudas.

Neskaidrus asmens duomenų tvarkymas kelia riziką darbuotojo asmens duomenų saugumui. Pavyzdžiui, darbuotojo konkreti buvimo vieta ir veikla tampa gana lengvai atsekama ir gali būti neteisėtai ar per klaidą atskleista tretiesiems asmenims. Taigi, darbuotojas turi teisę būti informuotam apie asmens duomenų tvarkymą. Todėl, pirmiausiai duomenų valdytojas privalo žinoti visas asmens duomenų tvarkymo operacijas: kokius asmens duomenis renka, kas turi prieigą prie jų. Antra, darbdavys turi pareigą suteikti reikalingą informaciją darbuotojui apie asmens duomenų tvarkymą, įskaitant automatizuotą atskirų sprendimų priėmimą ir asmens duomenų tvarkymą. Ši informacija turi būti pateikiama įvairiais kanalais, įskaitant ir patvirtinta vidine tvarka. Tokio pobūdžio informacija gali būti iš anksto pateikiama darbo sutartyje arba atskirais dokumentais pasirašant darbo sutartį. Trečia, darbdavys turi teisę pasirinkti tinkamas technines ir organizacines priemones asmens duomenų apsaugai užtikrinti.

2. Pagrindiniai darbuotojo asmens duomenų tvarkymo iššūkiai

Reglamentas neįtvirtina papildomų, specialių reikalavimų, kai duomenų valdytojas savo veikloje tvarko darbuotojo asmens duomenis. Reiškia darbuotojo asmens duomenų tvarkymo operacijoms galioja bendrieji BDAR reikalavimai. Tačiau kaip ir anksčiau aptartais teisėtumo ir skaidrumo aspektais, reikėtų atkreipti dėmesį, kad darbo santykiuose yra galios disbalansas. Darbuotojas yra silpnesnioji darbo santykių šalis. Todėl yra svarbu derinti abiejų šalių interesus ir pasiekti pusiausvyros.

Darbdavys turi galimybes nustatyti asmens duomenų tvarkymo tikslus, jų apimtį ir pasirinkti tinkamas technines ir organizacines priemones. Pavyzdžiui, i) vidinių dokumentų (prašymų, įsakymų, tvarkų, taisyklių ir kt.) administravimui gali būti pasitelktos kitų paslaugų teikėjų informacinės sistemos; ii) turto apsaugos ir asmenų saugumui galimai įdiegtos vaizdo kameros; iii) darbuotojo darbo efektyvumui ir kontrolės tikslais – vidinės IT sistemos; iv) saugių darbo sąlygų užtikrinimui gali būti pasitelkiami įvairūs įrenginiai, sveikatos prietaisai.

Darbuotojo asmens duomenis tvarkant minėtais tikslais ir būdais gali kilti rizika darbuotojo teisėms ir laisvėms, grėsmė pažeisti įtvirtintus BDAR reikalavimus, susimokėti priežiūros institucijos paskirtą baudą. Bendrovė rizikuoja savo dalykine reputacija, o tuo pačiu klientų ir darbuotojų, įskaitant pelno, praradimu. Taigi, yra plona riba tarp neteisėto darbuotojo asmens duomenų tvarkymo darbo santykiuose. Verslo subjektams duomenų apsauga turi tapti prioritetu. Toliau aptariamos gyvenimiškos situacijos identifikuos, kur kyla daugiausiai iššūkių ir pateiks praktinius patarimus, kaip jas išspręsti.

2.1. Darbuotojo vaizdo ir garso duomenų tvarkymas darbo vietoje

Darbuotojo vaizdo ir (ar) garso asmens duomenų tvarkymas darbo vietoje tampa intensyvesnis ir rizikingesnis. Prof. Ball pažymi, kad toks darbuotojo asmens duomenų tvarkymas nuo šiol gali apimti keturias kategorijas: i) darbuotojo mintis, jausmus; ii) judėjimą ir lokaciją; iii) užduočių atlikimą (efektyvumą); iv) santykius tarp kitų kolegų ir reputaciją (Ball, 2021, p. 23). Vaizdo stebėjimas kelia iššūkius ir todėl, nes vaizdo kameros filmuoja aukštesnės raiškos vaizdus; diktofonai įrašo geresnės kokybės pokalbius. Tuo pačiu pasitelkiamos veido atpažinimo sistemos, kurių netinkamas naudojimas ar veikimas kelia riziką darbuotojo teisėms ir laisvėms. Manytina, kad veido atpažinimo sistemos diegimas gali daryti įtaką seksualinio priekabiavimo apraiškoms

darbovietėje, bet tam yra reikalingas išsamesnis tyrimas. Taigi, veido atpažinimo sistemų naudojimas turėtų būti apsvarstytas ir pagrįstas.

Darbuotojo stebėjimas pasitelkiant vaizdo kameras, pokalbių įrašymas yra įmanomas, bet tam reikia atlikti keletą papildomų žingsnių. Pirma, reikia nusistatyti asmens duomenų tvarkymo tikslą ir aiškiai žinoti, kokių duomenų tikrai reikia tikslui pasiekti. Antra, pasirinkti tinkamą teisinį pagrindą. Įprastai praktikoje, bendrovės vaizdo stebėjimą grindžia turto ir fizinių asmenų apsaugai užtikrinti. Sutikimo teisinis pagrindas darbuotojo asmens duomenis rinkti vaizdo stebėjimu ar garso įrašymu dažnu atveju yra netinkamas. Pirmiausiai, todėl, kad tai yra specialiųjų kategorijų asmens duomenys, kurie gali būti renkami išimtiniais atvejais (BDAR 9 straipsnio 2 dalis). Antra, dėl galios disbalanso darbuotojui nebus užtikrintas sutikimo laisvanoriškumas. Todėl įprastai asmens duomenis tvarkyti šioje situacijoje reikia teisėtų interesų teisiniu pagrindu ir tik tuo atveju, kai atliktas balanso testas (Europos duomenų apsaugos valdyba, 2020a, p. 9-10). Taigi, svarbu identifikuoti tikslą, bei pasirinkti teisinį pagrindą ir tvarkyti tik tuos duomenis, kurie yra būtini tikslui pasiekti.

Bendrovė atlikdama vaizdo stebėjimą turėtų derinti technines ir organizacines priemones. Turto ir fizinių asmenų apsaugos tikslams neturėtų būti naudojama tik vaizdo stebėjimo kamera. Todėl, kad įranga yra pasyvaus naudojimo: i) įranga nesulaikys pažeidėjo nuo žalos atsiradimo; ii) įranga nebūtinai užfiksuos pažeidėją. Turi būti pasitelkiama alternatyvių priemonių, kurios būtų aktyvaus naudojimo, pavyzdžiui, įdiegti signalizaciją, geresnį apšvietimą, samdyti saugos paslaugų teikėją, rakinti patalpas (Europos duomenų apsaugos valdyba, 2020a, p. 9-10). Vaizdo stebėjimas turėtų būti logiškai nukreiptas į tą erdvę, į tą vietą, kurioje yra realiausia, kad gali kilti žala (pavyzdžiui, parduotuvės kasos aparatas vagystės atveju; įėjimas į biurą pro duris, langus ar pan. įsilaužimo atveju). Vaizdo stebėjimas neturi apimti erdvių, kuriose darbuotojas gali pagrįstai tikėtis privatumo (pavyzdžiui, persirengimo, poilsio kambariuose, buities, sanitarinės ir higienos patalpose).

Bendrovė atlikdama darbuotojo pokalbių įrašymą turi pasirūpinti techninėmis priemonėmis. Darbuotojas teikdamas konsultaciją telefonu nepraranda teisės susipažinti su telefoninio pokalbio įrašu (BDAR 15 straipsnis). Ši situacija kelia iššūkį, todėl, kad i) asmens (kliento) asmens duomenys neturėtų būti atskleisti darbuotojui, nes gali būti atskleista jautri, konfidenciali informacija; ii) reiškia asmens duomenis surinktus pokalbio metu reikia techniškai atskirti pagal subjektus. Priežiūros institucija rekomenduoja, kad darbuotojui būtų pateiktas garso įrašas su

„iškirptais“ kito asmens kalbėjimo epizodais arba pateikiant dialogo stenogramą (Valstybinė duomenų apsaugos inspekcija, 2021). Šie sprendimai gali pareikalauti didelių žmogiškųjų išteklių. Todėl svarbu iš anksto tinkamai pasirūpinti duomenų apsauga.

Darbdavys turi supažindinti darbuotoją, kai tvarko darbuotojo vaizdo, balso asmens duomenis pasirašytinai ar kitu būdu (Lietuvos Respublikos asmens duomenų ... įstatymas, 1996). Šiuo aspektu, rekomenduojama darbovietėje turėti atskirą vaizdo stebėjimo ir pokalbių įrašymo (jeigu tai yra atliekama) tvarką. Ši tvarka turėtų būti prieinama visiems darbuotojams bet kuriuo metu. Pavyzdžiui, būtų atsiųsta kiekvienam individualiai el. paštu arba įkelta vidinėje sistemoje tarp kitų bendrovės dokumentų. Tvarka turėtų aiškiai numatyti momentus, kada vyksta atitinkamas darbuotojo asmens duomenų tvarkymas, kokiais tikslais, kokia apimtimi. Turėtų būti laikomasi duomenų kiekio mažinimo principo (BDAR 5 straipsnio 1 dalies c punktas). Reiškia, kad tokie asmens duomenys neturėtų būti saugomi neribotą laiką. Vaizdo kameros, garso įrašai negali saugoti šimtus valandų įrašų. Griežtai neturėtų būti pritaikomas techninis sprendimas, kad vaizdo, garso įrašai išsitrina, kai nebelieka vietos saugomame kietajame diske arba, kai šie vaizdo, garso įrašai perrašo (angl. *override*) ankstesnius vaizdo, garso įrašais surinktus duomenis.

Kitos su vaizdo stebėjimu ir balso įrašymu kylančios grėsmės gali būti, kai pasitelkiamas dirbtinis intelektas ar kitos informacinės technologijos. Pavyzdžiui, vaizdo (veido išraiškų) ir garso (balso) įrašymas, bei šių duomenų analizė, kai vyksta pokalbis su kandidatu į darbą gali pagreitinti įdarbinimo procesą, bet tikėtina, kad tai bus neteisėtas asmens duomenų tvarkymas (Ball, 2021, p. 12). Kandidato veido išraiškos, emocijos gali atskleisti apie ką galvoja kandidatas. Keletas papildomų perteklinių klausimų ir darbdavys, kaip verslo subjektas gali įgauti pranašumą rinkoje (Lietuvos Respublikos konkurencijos įstatymo 15 straipsnis, 1999). Kita vertus, vaizdo stebėjimas pasitelkiant veido atpažinimo sistemas kaip priemonė prieš seksualinį priekabiavimą gali būti tinkamas ir efektyvus. Tačiau, tuo pačiu tai sustiprina susirūpinimą dėl pačios duomenų apsaugos (Anthony *et al.*, 2017 cituotas Stark *et al.*, 2020, p. 1084). Visgi, tuos pačius surinktus duomenis galima panaudoti tiek mobingo prevencijai, tiek jo užkardymui, bet tuo pačiu ir paties seksualinio priekabiavimo apraiškoms. Taigi, darbdavys naudodamasis technologijomis gali lengviau ir pigiau rinkti didelius darbuotojo asmens duomenų kiekius, o surinktus duomenis panaudoti skirtingiems tikslams (Bodie, 2021, p. 36). Dažnu atveju darbuotojams to nežinant. Bendrovė turi išlikti skaidri. Tinkamai aprašyti asmens duomenų tvarkymo operacijas ir parengti aiškias duomenų tvarkymo procedūras. Apibrėžti tikslus ir priemones, kuriomis siekia tikslų įgyvendinimo. Pasirinkti

mažiausiai darbuotojo teises ir laisves ribojančias priemones. Supažindinti darbuotojus su įgyvendinama duomenų apsaugos politika darbovietėje.

Europos Žmogaus Teisių Teismo nagrinėjo situaciją, kai mokymosi įstaigoje buvo įrengtos vaizdo kameros, kuriomis nors ir siekta užtikrinti turto ir žmonių saugumą, pažeidė teisę į privataus asmens gerbimą. Apie vaizdo kameras dėstytojai buvo iš anksto informuoti (*Antović ir Mirković* prieš Juodkalniją ..., 2017). Tačiau akivaizdu, kad nepakanka įgyvendinti reikalavimų formaliai: aiškiai apibrėžti duomenų tvarkymo tikslą ir informuoti duomenų subjektus. Teisėjai Vučinič ir Lemens pateikė savo atskirąją nuomonę, kuria sustiprino teismo argumentus, jog tarp dėstytojų ir studentų susiformuoja artimas tarpusavio santykis auditorijose. Dėstytojai gali sau leisti elgtis taip, kaip galbūt niekada nepasielgtų už auditorijos ribų. Darbuotojai auditorijoje gali pagrįstai tikėtis, kad tai, kas įvyksta auditorijoje bus prieinama tik joje esantiems asmenims (*Antović ir Mirković* prieš Juodkalniją ..., 2017). Vaizdo stebėjimas konkrečiose darbuotojų darbo vietose turėtų būti vengtinas arba turi būti gerai argumentuotos to priežastys ir nustatytos galimos kilti grėsmės. Darbdavys siekdamas įrodyti, kad laikosi BDAR reikalavimų turėtų atlikti poveikio duomenų apsaugai vertinimą (Valstybinės duomenų apsaugos inspekcijos direktoriaus įsakymas ..., 2019) (BDAR 84 preambulės punktas). Taip duomenų valdytojas įsivertintų ar to negalima pasiekti kitomis saugumą užtikrinančiomis ir mažiau teises ir laisves ribojančiomis priemonėmis.

Kitoje Europos Žmogaus Teisių Teismo byloje buvo atleisti darbuotojai, nes užsiiminėjo vagystėmis darbo vietoje. Darbuotojai ginčijo atleidimus ir siekė pripažinti, kad vaizdo kameromis surinkti duomenys yra neteisėti, nes apie vaizdo stebėjimą jie nebuvo informuoti (*López Ribalda* ir kt. prieš Ispaniją ..., 2019). Gali atrodyti, kad toks asmens duomenų tvarkymas bus laikomas neskaidriu. Tačiau tiek nacionaliniai teismai, tiek Europos Žmogaus Teisių Teismas konstatavo, jog vaizdo stebėjimo ir įrašų darbdavys nenaudojo jokiais kitais tikslais, kaip tik siekdamas susekti asmenis, atsakingus už užfiksuotus prekių praradimus ir imtis drausminių priemonių jų atžvilgiu. Teismai pripažino, kad buvo pasiekta šalių interesų pusiausvyra ir atleidimai, bei asmens duomenų tvarkymas buvo teisėti ir proporcingi (*López Ribalda* ir kt. prieš Ispaniją ..., 2019). Šis sprendimas ypatingas tuo, kad darbdaviai turėtų aiškiai atriboti, kokios darbo erdvės yra filmuojamos ir kokios rizikos kyla kiekvienoje iš jų.

Duomenų valdytojai privalo tinkamai informuoti apie vaizdo stebėjimą ir garso įrašymą. Darbuotojai turi teisę būti informuoti apie vaizdo ir (ar) garso duomenų rinkimą (BDAR 13 straipsnis). Pavyzdžiui, darbdavys Ispanijoje gavo įspėjimą nepaisant to, kad buvo iškabinęs vaizdo kamerų lipdukus. Tam, kad lipdukai būtų pakankami, juose turi būti pateikta ši informacija: i) duomenų valdytojo tapatybė; ii) duomenų tvarkymo tikslas, ir iii) informacija, kuri nurodytų kaip asmuo gali susipažinti su duomenų tvarkymu, bei įgyvendinti savo kitas duomenų subjekto teises (Ispanijos duomenų apsaugos agentūros 2021 m. spalio 18 d. sprendimas). Ši nurodyta informacija yra būtina pateikti. Liuksemburge bendrovė gavo 12,500 EUR baudą, nes taip pat turėjo neišsamius lipdukus. Pažymėtina, kad dalis informacijos privalo būti pateikta (angl. *first layer*), tuo tarpu informacija į kitą dalį gali būti pateikta pasitelkiant URL nuorodas, QR kodus ir kt. (angl. *second layer*) (Liuksemburgo duomenų apsaugos komisijos 2021 m. liepos 13 d. sprendimas). Lipdukuose turi būti pateikta informacija, kuri leistų suprasti, kas ir kokia apimti tvarko asmens duomenis. Taip pat sudaryta teisė susipažinti ir galėti įgyvendinti kitas teises. Pavyzdžiui, ant lipdukų galima pateikti duomenų apsaugos pareigūno ar kito atsakingo asmens kontaktinius duomenis ar nuorodą į privatumo politiką.

Duomenų valdytojai turi atsakingai įvertinti filmuojamas erdves darbo vietoje. Nacionalinė teisė leidžia numatyti papildomų reikalavimų. Todėl Ispanijoje duomenų apsaugos teisės aktas numato draudimą filmuoti darbuotojų poilsio kambarius. Nagrinėjamoje situacijoje darbdavys gavo 19,600 EUR baudą už perteklinį asmens duomenų tvarkymą, nes vaizdo kamera buvo nukreipta į poilsio kambario duris, o pro jas matėsi dalis paties poilsio kambario (Ispanijos duomenų apsaugos agentūros 2021 m. birželio 7 d. sprendimas). Bendrovė situacijas turi vertinti kompleksiškai ir logiškai. Tuo tarpu Liuksemburge bendrovės vaizdo kameros nepertraukiamai fiksavo registratūros stalą ir poilsiui skirtas erdves (Liuksemburgo duomenų apsaugos komisijos 2022 m. sausio 17 d. sprendimas). Duomenų valdytojas Rumunijoje pažeidė duomenų kiekio mažinimo principą filmuodamas darbuotojams skirtas rūbines ir valgymo zonas (Rumunijos nacionalinė asmens duomenų tvarkymo priežiūros institucijos 2021 m. balandžio 15 d. sprendimas). Taigi, naudojant vaizdo kameras ar atliekant garso įrašus, svarbu aiškiai nustatyti, o kas gali būti užfiksuota tvarkant asmens duomenis pasirinktu būdu. Darbdaviai privalo žinoti ir gebėti valdyti informacijos srautus.

Pagrįstai galima daryti išvadą, kad vaizdo ir (ar) garso asmens duomenų tvarkymas kelia papildomų iššūkių. Bet kuriame žingsnyje egzistuoja plona riba tarp neteisėto asmens duomenų tvarkymo. Siekiant suvaldyti rizikas, duomenų valdytojas turėtų atlikti poveikio duomenų apsaugai vertinimą. Tinkamai ir iš anksto informuoti duomenų subjektus, pavyzdžiui, pasitelkiant informacinius lipdukus, aprašant vidaus dokumentuose. Bendrovė turėtų tvarkyti tik tiek duomenų, kiek yra būtina atitinkamiems tikslams pasiekti. Atsisakyti nepertraukiamo vaizdo stebėjimo. Nefiksuoti erdvių, kurios keltų diskomfortą ar žemintų darbuotojų garbę ir orumą.

2.2. Darbuotojo stebėsena elektroninėmis priemonėmis

Darbuotojo stebėsena yra kasdienis, aktyvus asmens duomenų tvarkymo procesas. Dr. Tamašauskaitės-Janickės vertinimu darbuotojo stebėsena yra darbdavio prevencinių priemonių ir veiksmų sistema, skirta užtikrinti darbo saugą ir drausmę, bei sumažinti arba panaikinti bet kokią galimą riziką nuo neigiamų padarinių, įskaitant žalos atsiradimo (Tamašauskaitė-Janickė, 2016, p. 83). Tačiau praktikoje gausu pavyzdžių, kai darbuotojo stebėsena peržengia šiuos tikslus. Asmens duomenų gavimo šaltiniai apima tik mažą dalį gautų tiesiogiai iš darbuotojo. Didelė dalis duomenų gali būti gaunami iš darbdavio suteiktų darbo priemonių, aplikacijų, programų ar kitų darbuotojo asmeninių įrenginių, jutiklių, įtaisų (Europos Sąjungos pagrindinių teisių agentūra ..., 2018, p. 362). Pavyzdžiui, darbuotojų sveikatingumo skatinimo tikslais gali būti siūloma, o kai kada ir reikalaujama, sekti save naudojant ant kūno dėvimus, nešiojamus prietaisus (Ball, 2021, p. 23). Toks platus informacijos rinkimas yra asmens duomenų tvarkymas. Europos Sąjungos Teisingumo Teismas yra išaiškinęs, kad net ir dažnai besikeičiantis dinaminis interneto protokolo (IP) adresas yra laikomas asmens duomenimis, nes išlieka galimybė identifikuoti konkretų fizinį asmenį (*Patrick Breyer* ..., 2016). Kartais iš pirmo žvilgsnio negalime aiškiai pasakyti, kas yra asmens duomenys, o kas ne. Todėl, darbdaviams yra svarbu savo veikloje pirmiausiai gebėti nustatyti ir aiškiai atsakyti, kokius asmens duomenis jie renka apie darbuotojus.

Išsamus darbuotojo asmens duomenų rinkimas ir tvarkymas gali būti pateisinamas dėl įvairių priežasčių. Darbdaviai yra skatinami ieškoti technologinių sprendimų siekiant didinti darbo našumą ir efektyvumą, mažinti veiklos kaštus. Kita vertus, darbdaviai ieško priemonių kaip įsitikinti, kad darbuotojai laikosi prisiimtų įsipareigojimų ir darbo priemones naudoja pagal tikslinę jų paskirtį (Tamašauskaitė-Janickė, 2016, p. 81-82). Toks poreikis ypač išaugo, kai pasaulį apėmė pandemija dėl koronaviruso (COVID-19 ligos). Darbas persikėlė nuotoliniu būdu.

Darbuotojų stebėjimo programinės įrangos paklausa pasiekė aukštumas. Paslaugų teikėjai pranešė apie milžiniškus pardavimus: „Time Doctor“ padidėjo 202 proc., „Teramind“ padidėjo 169 proc., „Desk Time“ padidėjo 333 proc., „KickIdler“ padidėjo 139 proc. (Ball, 2021, p. 12). Ši statistika rodo kaip duomenų rinkimo srautai susiję su darbo santykiais išaugo. Tokie didieji duomenys (angl. *big data*) kelia naujus iššūkius. Darbuotojai tapo vis labiau sekami. Išsiplėtė stebėjimo metodai, kurie apima nuo šiol veidų atpažinimą, elektroninių ryšių analizę, internetines kameras, kompiuterio ekrano veiklos ar balso įrašymą. Kilo grėsmė darbuotojų nediskriminavimui, seksualiniam priekabiavimui, automatiniam sprendimų priėmimui (Ball, 2021, p. 73). Duomenų valdytojai turi įsipareigoti netvarkyti darbuotojo asmens duomenų toliau nesuderinamais tikslais, ypač darbuotojų sekimui ir vertinimui (Ogriseg, 2017, p. 19). Bendrovės turėtų ieškoti būdų kaip gebėti valdyti tokius išaugusius duomenų srautus; kaip gebėti užtikrinti surinktų ir tvarkomų asmens duomenų apsaugą.

Darbuotojo kontrolė atliekama nebe tik konkrečioje darbo vietoje, bet taip pat ir darbo funkcijų atlikimo vietoje, kuri pasirenkama paties darbuotojo. Darbdavys nuo šiol kontrolę gali atlikti ne vien tik įrengdamas vaizdo kameras savo buveinėje, bet stebėsena atlikti nuotoliniu būdu pasitelkdamas elektroninėmis priemonėmis. Tokios stebėsenos objektas tampa pats darbuotojas, jo darbo procesas, informaciniai ir komunikaciniai srautai, įskaitant darbuotojo asmeninius susirašinėjimus, bei veikla internetinėje erdvėje (Tamašauskaitė-Janickė, 2016, p. 48). Iš esmės darbuotojas ir jo elgsena kuria naujus asmens duomenis, naujo pobūdžio informaciją, kuri tampa pertekline ir nebūtina darbdaviui žinoti. Tiesa, ne visais atvejais. Informacija gali būti pagalba darbdaviui užtikrinti, kad darbuotojas nepiktnaudžiaus darbo procese suteiktomis priemonėmis. Duomenų valdytojas naudodamas naujas technologijas, automatizuotas priemones turėtų užtikrinti, kad pasitelkiami algoritmai ir dirbtinis intelektas iš anksto nenulems darbuotojų pasirinkimų (Europos Komisija, 2022). Pavyzdžiui, jog nesudarys sąlygų rinkti dar daugiau asmens duomenų elektroninėje erdvėje arba kitų pasirinkimų susijusių su darbo sutarties vykdymu. Asmens duomenų tvarkymas turi būti skaidrus ir darbuotojui privalo būti sudarytos galimybės sprendimus priimti savarankiškai.

Darbdavys gali fiksuoti darbuotojo darbą automobilyje, pavyzdžiui, įmontuojant GPS. Tačiau būtina išlikti skaidriam. Lietuvos vyriausiasis administracinis teismas pripažino, kad automobilio judėjimo trajektorija, laikas, važiavimo greitis ir kt. yra asmens duomenys. GPS įrenginio pagalba asmens duomenys surenkami tiesiogiai iš darbuotojo (Lietuvos vyriausiojo

administracinio teismo 2016 m. gruodžio 7 d. nutartis administracinėje byloje Nr. eA-2333-525/2016). Todėl, būtina informuoti darbuotojus apie tokių asmens duomenų tvarkymą. Portugalijos teismas atkreipė dėmesį, kad sekimo įrankiai turėtų būti naudojami tik aiškiai apibrėžtam tikslui. Taip pat, kad darbuotojai gautų instrukcijas, kaip naudotis tokiais įrankiais ir kokią informaciją apie juos yra renkama (Gimarainso apeliacinio teismo 2016 m. kovo 3 d. sprendimas byloje Nr. 20/14.7T8VRL.G1). Nukentėjęs darbuotojas turi teisę reikalauti neturtinės žalos atlyginimo, jeigu GPS įrenginiu nėra užtikrinama jo teisė į privataus asmens gerbimą (Austrijos Aukščiausiojo Teismo 2020 m. sausio 22 d. sprendimas byloje Nr. 9 ObA 120/19s). Tokiu būdu suteikiama reali galimybė kompensuoti darbuotojo patirtus išgyvenimus.

Automobiliu renkami vietos nustatymo duomenys negali būti renkami nepertraukiamai. Liuksemburgo priežiūros institucija nustatė, kad bendrovė rinko darbuotojo asmens duomenis ir tada, kai darbuotojas naudojosi automobiliu iš namų į darbą ir atvirkščiai. Taip pat saugojo tokius duomenis 28 mėn. tokiu būdu pažeisdamas saugojimo trukmės apribojimo principą (Liuksemburgo duomenų apsaugos komisijos 2021 m. birželio 7 d. sprendimas). Kitoje byloje nustatė, kad automobiliuose buvo įrengtos ir vaizdo kameros. Nepagrindžiant tokio asmens duomenų tvarkymo, pripažino duomenų kiekio mažinimo principo pažeidimą (Liuksemburgo duomenų apsaugos komisijos 2021 m. lapkričio 2 d. sprendimas). Tuo tarpu Suomijoje buvo paskirta 16,000 EUR bauda, nes bendrovė prieš pradedama tvarkyti geolokacijos duomenis neatliko poveikio duomenų apsaugai vertinimo ir neįvertino galimų rizikų (Suomijos duomenų apsaugos ombudsmeno tarnybos 2020 m. gegužės 18 d. sprendimas). Taigi, prieš pradedant tvarkyti tokio pobūdžio duomenis svarbu įvertinti galimas rizikas, aprašyti procesą, supažindinti darbuotojus su automobilio naudojimo tvarka. Automobilio sekimas turi būti savalaikis, ypač, kai automobiliu darbuotojas gali naudotis ne darbo reikalais. Duomenų apimtis ir jų saugojimo trukmė turi būti pasirinkta pagrįstai ir argumentuotai.

Darbdavys turi teisę patikrinti darbuotojo darbo kompiuterį, o darbuotojas manydamas, kad jo teisės pažeistos gali jas ginti. Teismas pripažino, kad bendrovė atlikdama veiklos tyrimą gali paimti darbuotojo darbo kompiuterį ir patikrinti darbinį el. paštą. Teismas aiškino, kad bendrovė turi teisėtą interesą apsaugoti konfidencialią informaciją (Lietuvos vyriausiojo administracinio teismo 2018 m. balandžio 20 d. nutartis administracinėje byloje Nr. A-622-525/2018). Teismui pavyko užtikrinti interesų balansą. Darbuotojas turi prisiimti riziką, jeigu nusprendžia saugoti asmeninio pobūdžio informaciją darbo kompiuteryje. Asmuo turi teisę ginčyti priežiūros

institucijos sprendimą, kai šis yra susijęs tik su paties duomenų subjekto teisėmis, o ne trečiųjų asmenų (Lietuvos vyriausiojo administracinio teismo 2020 m. vasario 5 d. nutartis administracinėje byloje Nr. eA-37-629/2020). Vokietijoje buvo išaiškinta, kad neteisėtai dėl darbuotojo stebėsenos gauti duomenys negali būti įrodymais teismo procese. Stebėsena apėmė ne tik naršymo istoriją, bet ir patį naršytą turinį, o tai buvo įvertinta kaip pertekliniai duomenys (Vokietijos Federalinio darbo teismo 2017 m. liepos 27 d. sprendimas byloje Nr. 2 AZR 681/16). Apibendrinant, galima teigti, kad tvarkant duomenis reikalingas teisėtas interesas. Informaciją galima suteikti darbo sutartyje ar kituose dokumentuose. Siūlytina stebėseną vykdyti reguliariai arba kilus abejonėms, o ne nepertraukiamu būdu. Asmens duomenų tvarkymą ir kontrolės veiksmus dokumentuoti.

Platformų darbuotojams (angl. *platform workers*) galimai neužtikrinama teisė į duomenų apsaugą. Paslaugų teikėjo „Uber“ vairuotojai naudojasi išmaniąja programėle. Ši aplikacija renka geolokacijos duomenis padedančius nustatyti asmens tikslią buvimo vietą, t. y. artimiausią vairuotoją klientui ir duomenis susijusius su ekonominiu vairavimu (Ball, 2021, p. 28). Lietuvos Respublikos teisėje yra vietos nustatymo duomenų sąvoka ir bendrosios duomenų teikimo tretiesiems asmenims taisyklės (Lietuvos Respublikos elektroninių ryšių įstatymo 3 straipsnio 98 dalis ir 80 straipsnis, 2004). Teisė reguliuoja duomenų teikimą tarp viešosios valdžios institucijų, bet ne privačiuose santykiuose. Tokiam duomenų tvarkymui ir teikimui galioja bendrieji BDAR reikalavimai. Platformų darbuotojai, nepaisant jų užimtumo statuso, būdo ar trukmės, turi teisę į sąžiningą ir tinkamą apsaugą skaitmeninėje erdvėje (Europos Komisija ..., 2022). Taigi, duomenų valdytojai teikdami universalias paslaugas vartotojams, sukuria skaitmeninę dalijimosi ekonomiką (angl. *digital sharing economy*), kurioje gausiai renka savo platformų darbuotojų asmens duomenis.

Neskaidrus ir neteisėtas asmens duomenų tvarkymas gali pasireikšti kaip diskriminacinis. Italijos priežiūros institucija paskyrė 2,6 mln. EUR baudą paslaugų teikėjui „Foodinho“.[2] Bendrovėje veikė algoritmu paremta kurjerių vertinimo sistema. Priežiūros institucija nustatė, kad bendrovė neįdiegė tinkamų saugumo priemonių, kurios užtikrintų tinkamą ir teisingą kurjerių reitingavimo sistemą. Nebuvo sudaryta galimybė žmogui užginčyti algoritmu paremtos sistemos. Šių priemonių trūkumu pasireiškė diskriminacinis kurjerių vertinimas, o to pasekmė paskyros

[2] „Foodinho” yra skaitmeninė platforma teikianti maisto pristatymo paslaugas Milane. Darbuotojai įprastai pristato maisto užsakymus dviračiu.

išjungimas (darbo netekimas) aplikacijoje. Be viso to, paslaugų teikėjas neatliko poveikio duomenų apsaugai vertinimo, nepaskyrė duomenų apsaugos pareigūno, neįgyvendino tinkamų techninių ir organizacinių priemonių (Italijos nacionalinės priežiūros institucijos 2021 m. birželio 10 d. sprendimas). Tai vienas pirmųjų atvejų, kuriuo yra nustatomi platformų darbuotojų teisių ir laisvių pažeidimai. Darbo santykiai suteikia vienokią ar kitokią apsaugą darbuotojams, taip pat suteikia teisinį aiškumą. Nors platformų darbuotojų statuso suvienodinimui apraiškų matyti. Visgi, jų statusas kol kas nėra iki galo išspręstas. Platformų darbuotojų teisei į duomenų apsaugą reikalingas atskiras išsamesnis tyrimas. Šis magistro darbas pristatė problemą, bet toliau šio santykio nenagrinės.

Apibendrinant, darbuotojo stebėsena nėra būtina, o atvirkščiai turėtų būti pasitelkiama tik esant aiškiai apibrėžtiems tikslams ir turint teisėtą interesą. Pareiga pradėti darbuotojo stebėsena nekyla tik todėl, kad darbas yra organizuojamas nuotoliniu būdu (Valstybinė duomenų apsaugos inspekcija, 2020a, p. 2). Darbdaviai turėtų vengti nepertraukiamo asmens duomenų tvarkymo, surinkti asmens duomenis nuotoliniu būdu. Pasitelkiant naujas darbuotojo fiksavimo priemones kyla naujų iššūkių. Tokia asmens duomenų rinkimo praktika įprastai tampa neproporcinga ir neteisėta (ES 29 straipsnio duomenų apsaugos darbo grupė, 2017, p. 21). Siekiant užtikrinti teisingą šalių interesų pusiausvyrą, siūloma naudotis priemonėmis, kurios apribotų perteklinį asmens duomenų tvarkymą (Ogriseg, 2017, p. 19). Šiomis priemonėmis gali būti saugos sistemų įdiegimas, apribojimas naudotis mobiliais įrenginiais automobilyje, asmeninio el. pašto išjungimas, prieigos prie interneto puslapių ribojimas. Skaidrus asmens duomenų tvarkymas gali būti įgyvendinamas parengiant vidines tvarkas, pasirašant darbo sutartis, kolektyvines sutartis (Torres, 2021, p. 55). Taigi, įvairių tinkamų techninių ir organizacinių priemonių derinimas gali padėti sustabdyti perteklinį asmens duomenų tvarkymą, užtikrinti darbuotojo asmens duomenų apsaugą ir atspindėti geriausius darbdavio interesus.

2.3. Darbuotojo sveikatos asmens duomenų tvarkymo ypatumai

Duomenų valdytojas savo veikloje gali susidurti su situacijomis, kai reikės tvarkyti darbuotojo sveikatos asmens duomenis. Pirmiausiai, galioja bendra darbdavio pareiga užtikrinti darbuotojams saugias ir sveikatai nekenksmingas darbo sąlygas visų darbo santykių metu (Darbo kodekso 158 straipsnis). Reiškia darbdavys turi imtis visų būtinų priemonių tinkamos, saugios darbo aplinkos sukūrimui. Pavyzdžiui, darbuotojo atsisakymas privalomai tikrintis savo sveikatą gali būti

pripažintas šiurkščiu darbo pareigų pažeidimu (Darbo kodekso 58 straipsnio 2 dalies 3 punktas). Tvarkyti darbuotojo sveikatos duomenis yra tiek pareiga, bet tuo pačiu ir darbdavio teisėtas interesas, nes siekiama apsaugoti savo darbuotojų sveikatą, užtikrinti nenutrūkstamą darbo procesą.

2020 m. pasaulyje išplito koronavirusas (COVID-19 liga), o to pasekmė tapo būtinumas tvarkyti darbuotojo sveikatos asmens duomenis. Sveikatos asmens duomenys yra priskiriami specialiųjų kategorijų asmens duomenims, kurių tvarkymas galimas tik išimtiniais atvejais (BDAR 9 straipsnio 1-2 dalys). Tačiau, tai nereiškia, kad toks asmens duomenų tvarkymas yra absoliučiai uždraustas ir negalimas. Kaip jau minėta anksčiau, asmens duomenų tvarkymas turi pasitarnauti žmonijai (BDAR preambulės 4 punktas). Be jokios abejonės, kad išplitus COVID-19 ligai asmens duomenų tvarkymas yra pateisinamas. Sveikatos asmens duomenims yra taikoma didesnė apsauga. Sveikatos asmens duomenų tvarkymo tikslais, o šiuo atveju COVID-19 ligos prevencijos ir plitimo valdymo tikslais gali būti tvarkomi darbuotojo sveikatos asmens duomenys (BDAR 9 straipsnio 2 dalies i punktas). Visgi, tokių jautrių asmens duomenų tvarkymas turi būti aiškiai, skaidriai ir tinkamai vykdomas. Asmens duomenų susijusių su darbuotojo sveikata tvarkymo apimtys ir jų tvarkymo būtinumas privalo būti aiškiai pagrįstas.

Darbuotojo sveikatos asmens duomenis galima tvarkyti esant teisinei prievolei. COVID-19 liga savaime nesuteikia pareigos ar teisės tvarkyti darbuotojo sveikatos asmens duomenų. Todėl įprastai tinkamiausias teisinis pagrindas tokio pobūdžio kontekste yra teisinė prievolė, kuri įtvirtinta nacionalinėje teisėje (BDAR 6 straipsnio 1 dalies c punktas). BDAR aiškiai deklaruoja, kad epidemijos kontrolės tikslais gali būti tvarkomi sveikatos asmens duomenys (BDAR preambulės 46 punktas). Teisinio reguliavimo taikymą ir aiškinimą patvirtina Europos duomenų apsaugos valdyba, nurodydama, jog darbdaviui darbo santykiuose sveikatos asmens duomenų tvarkymas yra būtinas, kai tai nustatyta nacionalinėje teisėje (Europos duomenų apsaugos valdyba, 2020b). Lietuvos Respublikos Vyriausybės nutarimu yra įtvirtinta darbuotojų pareiga pateikti su sveikatos patikrinimu susijusius dokumentus (Lietuvos Respublikos Vyriausybės nutarimas ... darbuotojų sveikatos tikrinimosi tvarkos, 1995). Reiškia tuo pačiu, tai yra darbdavio teisė reikalauti iš darbuotojo pateikti reikalingus dokumentus, bei kartu sistemiškai vadovaujantis ir kitais teisės aktais, pareiga tokius duomenis tvarkyti. Apibendrintai, galime teigti, kad darbuotojo sveikatos asmens duomenų tvarkymas yra leistinas, kai yra įtvirtinama teisinė prievolė.

Duomenų valdytojas turėtų imtis visų reikalingų priemonių siekiant apsaugoti darbuotojo sveikatos asmens duomenis. Sveikatos asmens duomenys dėl savo pobūdžio yra jautri informacija susijusi su konkrečiu duomenų subjektu. Tokių neskelbtinų duomenų atskleidimas gali turėti neigiamų pasekmių darbuotojams. Ši aplinkybė ypač aktuali COVID-19 ligos kontekste, nes surinkti sveikatos duomenys bus naudojami moksliniams tyrimams (Petkevičienė *et al.*, 2020, p. 335-336). Kartu kyla ir kitų grėsmių. Pavyzdžiui, darbo santykiuose iš darbuotojo gali būti reikalaujama įsidiegti vietos sekimo aplikacijas ar naudoti kitus dėvimus nešiojamus įrenginius, kurie rinktų informaciją apie darbuotojo sveikatą ne tik darbo vietoje (Ogriseg, 2017, p. 17). Taigi, darbdavys negali nepagrįstai rinkti ir kurti naujus duomenų gavimo šaltinius apie darbuotojų sveikatą, o renkant, užtikrinti tinkamą apsaugą.

Duomenų valdytojas privalo gerai įvertinti duomenų tvarkymo operacijas, apimtis ir rizikas. Prof. Ball tyrinėdama kitų mokslininkų vertinimus atkreipė dėmesį, kad darbdaviai diegė įvairias sveikatingumą skatinančias programas. Kryptingos tendencijos įžvelgiamos darbo santykiams persikėlus į nuotolinį darbą. Tokio pobūdžio aplikacijos rinko milžiniškus kiekius duomenų apie darbuotoją, to pasekmė virto, kad darbdaviai analizavo pačius duomenis, o ne teikiamas programos naudas (Ball, 2021, p. 24-26). Lietuvos atveju, tokia situacija galėjo susiformuoti įvedus karantino režimą visoje teritorijoje. Siekiant užimti darbuotojus, išlaikyti aktyvią, efektyvią komandą, už žmogiškuosius išteklius atsakingi darbuotojai kūrė panašaus pobūdžio iniciatyvas. Tačiau atkreiptinas dėmesys, kad karantino režimas ar COVID-19 liga savaime nesudaro galimybės tvarkyti tokio pobūdžio duomenų (Valstybinė duomenų apsaugos inspekcija, 2020b). Duomenų valdytojai iš principo turėtų susilaikyti nuo bet kokių perteklinių asmens duomenų tvarkymo, kai tai susiję su sveikatos duomenimis. Pavyzdžiui, darbuotojų temperatūros rodmenų, medicininių pažymų, sveikatos patikrinimo rezultatų ar kt. rinkimo (Petkevičienė *et al.*, 2020, p. 340). Darbdaviai turėtų imtis aktyvių priemonių, kurios padėtų užtikrinti darbuotojo sveikatą savarankiškai pačiam. Prašyti tik susipažinti su sveikatos patikrinimo rezultatais, jų nerinkti ir nesaugoti.

Darbo santykių šalys privalo tarpusavyje bendradarbiauti, ypač, kai tai susiję su epidemijos kontrolę. Svarbu, kad darbuotojai būtų parengti, apmokyti, instruktuoti ir žinotų kaip elgtis įvykus COVID-19 ligos protrūkiui darbovietėje ar patiems pajautus ligos simptomus. Supažindinti su darbuotojų pareiga informuoti apie patvirtintą COVID-19 ligą, jaučiamus ligos simptomus. Nereikalauti pildyti dokumentų, anketų, apklausų, kurios padėtų surinkti ir saugoti duomenis iš

darbuotojų (Valstybinė duomenų apsaugos inspekcija, 2020b). Bendrovė gali investuoti ne į sistemų kūrimą, kurios surinktų duomenis apie darbuotojus, bet į priemonių sudarymą, kurios padėtų individualiai darbuotojams pasitikrinti savo sveikatą.

Darbuotojui susirgus COVID-19 liga informuoti tik ribotą skaičių darbuotojų. Rekomenduojama tik išimtiniais atvejais informuoti, kas susirgo COVID-19 liga, pavyzdžiui, tuo atveju, kai siekiama nustatyti sąlytį turėjusius asmenis (Petkevičienė *et al.*, 2020, p. 343). Tiesa, siekiant pasitikėjimo ir skaidrumo prieš darbuotojus – informuoti reikia apie COVID-19 ligos atvejus darbovietėje reikia. Tačiau bet kokio pobūdžio informaciją riboti, įsivertinti, kas yra tikrai būtina atskleisti (Europos duomenų apsaugos valdyba, 2020b). Pavyzdžiui, informuoti visą komandą bendru el. laišku apie COVID-19 ligos atvejį ir pranešti, kad su sąlytį turėjusiais asmenimis bus asmeniškai susisiekta. Šio laiško turinys būti ribotas.

Darbdavio teisėtas interesas tvarkyti darbuotojo sveikatos duomenis prieš jį įdarbinant ar paaukštinant. Darbo kodeksas leidžia iš darbuotojo reikalauti informacijos, kuri yra susijusi su darbuotojo sveikatos būkle (Darbo kodekso 41 straipsnio 1 dalis). Darbdavys gali turėti interesą, kad darbuotojo sveikata leis atlikti darbo funkcijas, o darbuotojui susidaryti lūkestį ir žinoti, ko gali tikėtis darbo pradžioje. Visgi, tokio pobūdžio informacijos rinkimas nėra absoliutus. Europos Žmogaus Teisių Teismas padarė išvadą, kad yra pažeidžiama asmens teisė į privataus gyvenimo gerbimą, kai dėl darbuotojo psichikos sveikatos duomenų saugojimo ir atskleidimo bei jų panaudojimo sprendžiami darbuotojų prašymai paaukštinti pareigose. Nagrinėjamoje byloje nustatyta, kad Ukrainos nacionalinė teisė leido ilgą laiką saugoti su sveikata susijusius duomenis ir juos atskleisti bei naudoti su pradiniu rinkimo tikslu nesusijusiais tikslais (*Surikov* prieš Ukrainą ..., 2017). Kandidatui turi būti užtikrinta asmens duomenų apsauga. Darbdavys negali surinkti duomenis apie kandidato sveikatą, o juos vėliau ilgą laiką saugoti ir (ar) perleisti tretiesiems asmenims, pavyzdžiui, įdarbinimo agentūrai.

Duomenų valdytojo pasirinktos COVID-19 ligos valdymo priemonės tvarkančios darbuotojo asmens duomenis. Bendrovė turėjo internetinį registrą, kuriame kaupė darbuotojų vardus, pavardes, adresus, el. p. adresus, soc. draudimo numerius, neatvykimo į darbą priežastis (ligų pavadinimus, simptomus, kt. požymius). Ši informacija atitiko sveikatos duomenis (BDAR 4 straipsnio 15 punktas). Tyrimu buvo nustatyta, jog tokių duomenų tvarkymas yra nebūtinas darbuotojų reintegracijai (sugrįžimui į darbą) (Nyderlandų duomenų apsaugos tarnybos 2020 m. kovo 24 d. sprendimas). Bendrovė neturėtų sveikatos asmens duomenų tvarkyti per soc. tinklus.

Danijoje darbuotojai keitėsi sveikatos duomenų informacija naudodamiesi „WhatsApp“ programėle. Pripažinta, kad tokiu būdu duomenų valdytojas neužtikrino tinkamų techninių ir organizacinių priemonių (Danijos duomenų apsaugos agentūros 2021 m. liepos 9 d. sprendimas).

Apibendrinant, darytina išvada, kad darbuotojo sveikatos asmens duomenų tvarkymas gali būti teisėtas, bet atsižvelgiant į šių duomenų jautrumą turi būti imamasi visų atsargumo priemonių. Siekiant valdyti rizikas, apibrėžti duomenų tvarkymo tikslus konkrečiai ir nedviprasmiškai. Instruktuoti darbuotojus kaip tvarkyti sveikatos duomenis. Riboti prieigas prie sveikatos duomenų. Darbo santykių šalys turi bendradarbiauti, dalintis viena su kita reikalinga informacija, ypač, kai siekiama naudos visuomenės, epidemijos kontrolės valdymo. Pasirinkti tinkamas ir saugumą užtikrinančias technines priemones. Atlikti poveikio duomenų apsaugai vertinimą. Įvertinti rizikas ir pasirengti planus, procedūras šioms rizikoms valdyti.

2.4. Darbuotojo asmens duomenų tvarkymas vykdant darbuotojų atstovavimą

Darbuotojų atstovų iššūkis yra susijęs tiek su pačių galimybėmis tvarkyti darbuotojo asmens duomenis, tiek su aktyviu įsitraukimu atstovaujant darbuotojų teisę į duomenų apsaugą. Šis iššūkis pirmiausiai yra susijęs su galiojančia bendrąja taisykle, kad, pavyzdžiui, specialiųjų kategorijų asmens duomenų tvarkymas atskleidžiantis narystę profesinėse sąjungose yra draudžiamas, išskyrus įtvirtintas išimtis (BDAR 9 straipsnio 1 dalis). Antra, sunkumai kyla su atstovų nepasiruošimu būti aktyviems teisių gynėjams, kai tai susiję su teise į duomenų apsaugą (Vargas, 2017 cituota Ball, 2021, p. 27). Toks kylantys dvilypiškumas gali signalizuoti tik vieną – darbuotojų teisės gali likti neapgintos. Natūralu, kad kai problemos kyla organizacijos viduje (tvarkant asmens duomenis), jos kils ir išorėje (atstovaujant asmenų interesus ir ginant teises). Todėl, šiuo aspektu yra reikalingas kompleksinis BDAR reikalavimų ir darbuotojų atstovavimo įgyvendinimo vertinimas. Svarbu aiškiai atskirti dvi galinčias kilti problemas, bei joms pasiūlyti sprendimų būdus.

Galimybė tvarkyti darbuotojo asmens duomenis vykdant darbuotojų atstovavimą. Lietuvoje darbuotojų atstovais yra įvardijamas darbuotojų patikėtinis, darbo taryba ir profesinė sąjunga (Darbo kodekso 165 straipsnio 2 dalis). Šie konkretūs subjektai susiduria su iššūkiais tvarkydami darbuotojo asmens duomenis. Pavyzdžiui, Vokietijoje darbdavys tvarkė darbuotojų darbo užmokesčio apskaitą elektroniniu būdu. Darbo taryba prašė susipažinti su neanoniminiais duomenimis (teisės aktai nenumatė ribojimo) argumentuodami, kad tik tokiu būdu bus įmanoma

užtikrinti lyčių lygybės ir nediskriminavimo kitais pagrindais principus. Teismas patvirtino darbo tarybos argumentus išaiškindamas, kad darbo tarybai reikalinga konkreti informacija apie darbuotojams mokamą atlyginimą, jog galėtų įgyvendinti savo pareigas (Vokietijos Federalinio darbo teismo 2019 m. gegužės 7 d. sprendimas byloje Nr. 1 ABR 53/17). Tuo tarpu Lietuvoje įtvirtinta, kad tik nuasmenintus duomenis apie vidutinį darbo užmokestį pagal darbuotojų grupes galima atskleisti darbo tarybai ar profesinei sąjungai (Darbo kodekso 23 straipsnio 2 dalies 1 punktas). BDAR prasme darbo tarybos teisinis statusas nėra aiškus ir reikalingas tolimesnis tyrimas. Tačiau autoriaus nuomone manytina, kad tokių nenuasmenintų duomenų atskleidimas duomenų apsaugos teisės srityje galėtų būti pagrįstas ir pateisinamas. Darbo taryba turi teisę būti sprendimų priėmėja, gauti informaciją ir teikti siūlymus (Darbo kodekso 174 straipsnio 1 dalis). Darbuotojo asmens duomenų tvarkymas bus laikomas teisėtu, jeigu darbo taryba gebės įrodyti tokių duomenų tvarkymo proporcingumą ir būtinumą, siejant su reikalingų pareigų įgyvendinimu.

Darbuotojo asmens duomenų apsaugos teisės srityje galimos susiformuojančios šalių praktikos dėl duomenų tvarkymo darbovietėje. Vienoje iš Belgijos ligoninių susiformavo praktika, kai iš darbuotojų darbo užmokesčio buvo išskaitomas narystės mokestis profesinėje sąjungoje. Ši praktika buvo pagrįsta tik žodiniu susitarimu su ligoninėje esančia darbo taryba ir rašytiniais darbuotojų sutikimais. Problema kilo po to, kai darbovietėje neliko ankstesnės profesinės sąjungos ir ją pakeitė kita, o tokia darbuotojo asmens duomenų tvarkymo praktika nepakito (Belgijos duomenų apsaugos institucijos 2020 m. lapkričio 9 d. sprendimas). Profesinė sąjunga gali tvarkyti specialiųjų kategorijų asmens duomenis esant šioms sąlygoms: i) tvarko profesinės sąjungos tikslais, kurių siekia asociacija; ii) taiko tinkamas saugumo priemones; iii) tvarko tik savo esamų ar buvusių narių duomenis; iv) duomenų neatskleidžia tretiesiems asmenims be duomenų subjekto sutikimo (BDAR 9 straipsnio 2 dalies d punktas). Taigi, profesinių sąjungų tikslas tvarkyti savo narių (darbuotojų) asmens duomenis turi būti aiškiai suformuotas. Profesinė sąjunga gali tvarkyti tik tų narių, kurie palaiko ryšį su asociacija. Pavyzdžiui, narys yra šalinamas iš profesinės sąjungos, jeigu nesumokėjo kartą per metus nesumoka nario mokesčio. Reiškia, tokioje situacijoje pagrįstai kiltų klausimas: ar vis dar būtina tvarkyti darbuotojo asmens duomenis? Nepagrindžiant būtinumo – toks tvarkymas nebūtų pateisinamas.

Darytina išvada, jog darbuotojų atstovai gali tvarkyti darbuotojo asmens duomenis. Remiantis tikslo apribojimo principu darbuotojo asmens duomenų tvarkymas turėtų būti būtinas tik tiek, kiek yra tai iš tiesų yra reikalinga atstovauti darbuotojų interesams arba vykdyti prisiimtus įsipareigojimus pagal atskirus tarp šalių sudarytus susitarimus (Europos Sąjungos pagrindinių teisių agentūra, 2018, p. 346). Vertinant teisėtumo aspektu, pažymėtina, kad ne kaip kitose darbo santykiams įprastose situacijose, sutikimas šiame kontekste galėtų būti laikomas teisėtu pagrindu. Kitoks aiškinimas būtų nelogiškas. Nepagrįsta teigti, kad tarp darbuotojo ir jį atstovaujančių asmenų yra galios disbalansas. Priešingai, abiejų šalių interesai yra suderinti ir negali prieštarauti. Darbuotojų atstovai turi gerai įsivertinti, kokia informacija yra reikalinga tinkamam atstovavimui. Darbdavys tuo tarpu turi išlikti aktyvus ir naudotis galimybe apriboti perteklinį asmens duomenų tvarkymą. Darbovietė ir darbuotojų atstovai gali sudaryti susitarimus (Darbo kodekso 175 straipsnis) arba kolektyvines sutartis (Darbo kodekso 190 sutartis), kuriose galėtų aptarti darbuotojo (asociacijos narių) duomenų tvarkymo apimtis ir šalių besiformuojančią praktiką.

Darbuotojai gali ginti savo teisę į duomenų apsaugą savarankiškai arba per darbuotojų atstovus. Šiuo metu teisės aktai nereglamentuoja kaip individualus darbuotojas galėtų teikti siūlymus darbdaviui asmens duomenų apsaugos teisės srityje (išskyrus tiek, kiek tai apima tarpusavio susitarimus, pavyzdžiui, darbo sutartyje, kt. susitarimuose). Teisiniai mechanizmai yra numatyti tik darbuotojų atstovams (Bodie, 2021, p. 63). Kiekviena valstybė narė teisinėje sistemoje gali reglamentuoti darbuotojo asmens duomenų tvarkymo ypatumus (BDAR 88 straipsnio 1 dalis). Anaiptol, valstybės iš tiesų šioje srityje nėra ryžtingos. Todėl, atsižvelgiant į darbinę technologinę pažangą, turėtų būti stiprinama apsauga nuo savavališko kišimosi į darbuotojų privatumą (Stanev, 2019, p. 102). Vienais atvejais, tai gali būti būtina, kitais atvejais reikalinga iniciatyva. Pavyzdžiui, siekiant aprašyti IT sistemų panaudojimo darbe ribas ir galimybes, nustatyti šių priemonių naudojimo tvarką, darbdaviui bus privalu suderinti ją su darbuotojų atstovais (Tamašauskaitė-Janickė, 2016, p. 226). Taigi, atstovavimo iniciatyvą galima išreikšti dvejopai: i) pasyviai, t. y. kai darbdavys inicijuoja ir vykdo informavimo ir konsultavimo procedūras, o darbuotojų atstovai prie to prisijungia (Darbo kodekso 206 straipsnio 1 dalis), arba ii) aktyviai, t. y. kai darbuotojų atstovai imasi aktyvių priemonių, teikia siūlymus, inicijuoja derybas ir pan.

Atkreiptinas dėmesys, kad teisė ginti interesus duomenų apsaugos teisės srityje yra suteikta ne konkrečiam darbuotojų atstovavimo subjektui, bet visiems. Sutiktina su Europos pažangiųjų studijų fondo (FEPS) patarėjo J. Nogarede pozicija, kuris teigia, kad tais atvejais, kai darbo tarybos lieka pasyvios, profesinės sąjungos gali įsitraukti, jog užtikrintų tinkamą paramą atstovaujamiems darbuotojams (Nogarede, 2021, p. 30). Neaišku, kiek tai būtų reali situacija Lietuvoje, bet sutiktina, kad darbuotojų atstovų subjektai turi bendradarbiauti ir dirbti drauge. Pavyzdžiui, steigti ir (ar) konsultuotis su duomenų apsaugos komitetu, specialistais, teisininkais (Ball, 2021, p. 77). Taip pat, darbuotojų atstovams nėra būtina siekti susitarimų su darbdaviu. Be abejonės, kad tais atvejais, kai kyla derybinių sunkumų dėl įvairių socialinių, ekonominių klausimų įgyvendinimo, ne ką mažiau tikėtina bus sunku pasiekti susitarimą duomenų apsaugos teisės srityje. Todėl, darbuotojų atstovai gali konsultuotis su bendrovėje paskirtu duomenų apsaugos pareigūnu, šviesti darbuotojus apie jų kaip duomenų subjektų teisių įgyvendinimo galimybes, padėti rengti skundus priežiūros institucijoms (Nogarede, 2021, p. 41). Susitarimus gali būti per sunku pasiekti ir jie gali likti formalūs arba sunkiai įgyvendinami. Tad, alternatyvių priemonių paieška, kurios galėtų turėti įtakos kiekvienam darbuotojui gali būti tapti ženkliai labiau efektyvesnėmis.

Taigi, darbuotojų atstovai gali ir turi įsitraukti į darbuotojų interesų gynimą asmens duomenų apsaugos srityje. Pavyzdžiui, duomenų valdytojas atlikdamas poveikio duomenų apsaugai vertinimą gali siekti išsiaiškinti darbuotojų ar jų atstovų nuomonę, apie numatytą asmens duomenų tvarkymą (BDAR 35 straipsnio 9 dalis). Konsultavimasis ypač svarbus prieš diegiant naujas informacines technologijas (Europos Sąjungos pagrindinių teisių agentūra, 2018, p. 343). Informavimas ir konsultavimasis apima visą su asmens duomenų tvarkymu susijusį procesą: i) tikslo apibrėžimą, ii) darbuotojų tinkamą informavimą, iii) pasirinktų saugumo priemonių diegimą, iv) tvarkymo operacijas, apimtis, v) saugojimą ir ištrynimą (Poquet Catalá, 2021 cituotas Torres, 2021, p. 55). Darbuotojų atstovai gali išlikti pasyvūs ir dalyvauti tik tiek, kiek yra įtraukiami darbdavių arba imtis aktyvių priemonių. Darbuotojų atstovai pirmiausiai turėtų didinti informuotumą apie duomenų subjektų teises ir rengti mokymus. Taip pat steigti nevyriausybines organizacijas arba bendradarbiauti su profesinėmis sąjungomis, jog galėtų teikti skundus priežiūros institucijai, atstovauti darbuotojų teisėms, kai kyla pažeidimų grėsmė (Nogarede, 2021, p. 18-19).

Apibendrinant, galima pagrįstai vertinti, kad darbuotojų atstovai gali tvarkyti darbuotojo asmens duomenis tokia apimtimi, kuri yra būtina jų pareigoms ir įsipareigojimams įgyvendinti. Kiekvienu atveju reikia kompleksiškai įsivertinti būtinumą tvarkyti asmens duomenis. Tais atvejais, kai kyla abejonių dėl tokio būtinumo, darbdavys turi išlikti aktyvus ir siekti apriboti neteisėtą asmens duomenų tvarkymą. Atsižvelgiant į tai, kad tarp santykyje tarp darbuotojo ir jo atstovų nėra galios disbalanso, asmens duomenų tvarkymas gali būti grindžiamas ir sutikimo teisiniu pagrindu. Darbuotojų atstovai turi imtis iniciatyvos siekdami tinkamai atstovauti darbuotojų interesams. Derinti įvairaus pobūdžio priemones, kurios leistų sėkmingai stiprinti apsaugą darbuotojų teisei į duomenų apsaugą ir darbdavio galimybei kištis į darbuotojo privatų gyvenimą.

2.5. Darbuotojo asmens duomenų saugumas ir saugojimas

Didelis iššūkis darbdaviui yra surinktų darbuotojo asmens duomenų saugumas ir jų pasirinkta saugojimo trukmė. Reglamentas įtvirtina, kad siekiant užtikrinti apsaugą, reikalingos tinkamos techninės ir organizacinės priemonės (BDAR preambulės 78 punktas). Todėl, duomenų valdytojas turi atsižvelgti į techninių galimybių išsivystymo lygį, įgyvendinimo sąnaudas, asmens duomenų tvarkymo operacijas ir įgyvendinti pasirinktas saugumo priemones (BDAR 25 straipsnio 1 dalis). Sąvoka „techninių galimybių išsivystymo lygis“ apima tiek technines, tiek organizacines priemones. Techninės priemonės gali užtikrinti tinkamą sistemų, įrankių, darbo priemonių veikimą ir sumažinti riziką. Organizacinės priemonės užtikrina skaidrumą, atsakingų asmenų kompetencijų ugdymą, bei apibrėžia aiškias asmens duomenų tvarkymo procedūras (Europos duomenų apsaugos valdyba, 2020d, p. 8). Sutiktina su C. Ogriseg nuomone, jog prieš diegiant turi būti atliktas poveikio duomenų apsaugai vertinimas ir pasirinktos tinkamos priemonės apsaugai užtikrinti (Ogriseg, 2017, p. 8). Aiškiai iš anksto atpažinus rizikas kils mažesnis pavojus duomenų apsaugos incidentui. Svarbu, jog kuo daugiau priemonių bus įdiegta, tai savaime nereikš, kad asmens duomenų tvarkymas bus teisėtas (Stanev, 2019, p. 101). Saugumo priemonės turi būti diegiamos ne tam, kad pagrįsti teisėtumą, o tam, kad apsaugoti asmens duomenis.

Duomenų valdytojas turi pasirinkti efektyvias saugumo priemones. Darbdaviui galioja pareiga, kad turi laikytis pritaikytosios ir standartizuotosios duomenų apsaugos principų (BDAR 25 straipsnis). Ši pareiga reiškia saugumo priemonių nustatymą, kuris gali apimti visą asmens duomenų tvarkymo surinkimą, tvarkymą ir saugojimą, t. y. visą techninį (programinis kodas,

išdėstymas, išvaizda) ir organizacinį (procedūros, tvarkos) sprendimą (Europos duomenų apsaugos valdyba, 2020d, p. 10). Pavyzdžiui, kaip tinkamas sprendimas gali būti pseudonimų duomenims suteikimas. Asmens duomenys yra užšifruojami, o jų šifras yra laikomas atskirai (Europos Sąjungos pagrindinių teisių agentūra, 2018, p. 136). Ši priemonė yra efektyvi ir mažai kaštų reikalaujanti. Taigi, kiekvienam darbdaviui prieinama. Be kita ko, efektyvių priemonių pasirinkimas pasireiškia per nuolatinį jų testavimą ir vertinimą (Ogriseg, 2017, p. 8). Efektyvios saugumo priemonės yra tos, kurios yra nuolat reguliariai peržiūrimos, suteikiančios tinkamą apsaugą.

Tik tinkamų techninių ir organizacinių priemonių pasirinkimas, bei jų tarpusavio derinimas užtikrins reikiamą duomenų apsaugą. Darbdavys šiuo aspektu turėtų ypač atkreipti dėmesį, nes netinkamų saugumo priemonių įgyvendinimas arba apskritai jų nebuvimas gali lemti nebūtinai konkretaus darbuotojo asmens duomenų neteisėtą atskleidimą tretiesiems asmenims, bet paties darbdavio ar jo klientų konfidencialios informacijos apsaugos pažeidimus (ES 29 straipsnio duomenų apsaugos darbo grupė, 2017, p. 18). Priežiūros institucijos įprastai teikia rekomendacijas, konsultacijas ir dalinasi gairėmis, kurių sąžiningas įgyvendinimas padės išvengti pažeidimų. Pavyzdžiui, Valstybinė duomenų apsaugos inspekcija rekomenduoja įdiegti prieigos kontrolę principu „būtina žinoti“ (Valstybinė duomenų apsaugos inspekcija, 2018, p. 3). Darbuotojams turi būti leista dirbti su tokia duomenų apimtimi, kuri yra būtina jų darbo funkcijoms atlikti.

Duomenų valdytojo atsakomybė už darbuotojo neteisėtus veiksmus. Jungtinėje Karalystėje darbuotojas tyčia atskleidė dalies savo bendradarbių duomenis apie jų darbo užmokestį. 10,000 bendradarbių pareiškė bendrovei grupės ieškinį dėl žalos atlyginimo. Teisme buvo ginčijamas atsakomybės klausimas: ar darbdavys atsakingas už darbuotojo neteisėtus veiksmus? Teismas pripažino, kad šioje situacijoje ne, nes darbuotojas atskleidė atlikdamas ne priskirtas darbo funkcijas, bei tai, jog darbdavys užtikrino adekvačią ir tinkamą saugumo kontrolę (Jungtinės Karalystės Aukščiausiojo Teismo 2020 m. balandžio 1 d. sprendimas byloje Nr. [2020] UKSC 12). Tačiau, tai vienas iš retų atvejų, kai duomenų valdytojas liko neatsakingas už tokių duomenų atskleidimą. Dažniausiai duomenų apsaugos incidentai įvyksta dėl darbuotojų žmogiškosios klaidos. Pavyzdžiui, todėl, kad darbuotojai negeba tinkamai atpažinti duomenų saugumo pažeidimų ir (ar) neturi aiškių procedūrų jam įvykus.

Duomenų valdytojas turi pasirengti įvairios kibernetinėms atakoms. Norvegijoje po kibernetinio įsilaužimo nutekėjo 160 GB dydžio duomenų į juodąjį internetą (angl. *dark web*). Priežiūros institucija pradėjo tyrimą ir nustatė IT sistemų ir procesų trūkumus: neapsaugojo atsarginių kopijų, netaikė dviejų veiksnių autentifikavimo (angl. *two-factor authentication*), netinkamai dokumentavo (Norvegijos duomenų apsaugos institucijos 2021 m. spalio 19 d. sprendimas). Taigi, duomenų valdytojai turi būti pasiruošę įvairioms kibernetinėms, duomenų vagystės (angl. *phishing*) atakoms. Tai nereiškia, kad bendrovė turėtų skirti neproporcingai daug finansinių ir žmogiškųjų išteklių. Atvirkščiai, kartais pigios, bet efektyvios priemonės gali būti daug veiksmingesnės (Europos duomenų apsaugos valdyba, 2020d, p. 9). Esminiu atakos suvaldymo veiksniu gali būti atsarginių kopijų darymas. Tokiu būdu yra užtikrinamas nepertraukiamas bendrovės darbų ir procesų tęstinumas (Valstybinė duomenų apsaugos inspekcija, 2018, p. 12). Tačiau svarbiausia yra derinti saugumo priemones kartu, kad kuo daugiau pasirinktų priemonių būtų realiai veiksmingos duomenų apsaugai užtikrinti. Turi būti paskirti atsakingi asmenys, numatytos vidinės procedūros kaip reaguoti įvykus incidentui. Taip pat visi veiksmai siekiant suvaldyti įvykusį incidentą turi būti dokumentuoti, jog vėliau bendrovė gebėtų pagrįsti, kad ėmėsi būtinų priemonių.

Duomenų valdytojas turi apibrėžti duomenų saugojimo laikotarpį. Jokie asmens duomenys negali būti saugomi neterminuotai. Pirmiausiai, turi būti aiškiai identifikuota, kokie konkrečiai tvarkomi darbuotojo asmens duomenys turi būti saugomi būtinam tikslui pasiekti. Bendrovė privalo gebėti pagrįsti sprendimo priežastis. Taip pat kaip minėta, atsarginės kopijos gali būti veiksminga priemonė duomenų saugumui, bet jos taip pat praėjus atitinkamam laikotarpiui privalo būti ištrintos (Europos duomenų apsaugos valdyba, 2020d, p. 26). Taigi, atkreiptinas dėmesys yra tai, jog pirmiausiai saugojimo laikotarpį gali pasirinkti pats darbdavys. Todėl, kad bendrovė geriausiai gali žinoti, kokie duomenys, kokiam laikotarpiui turi būti saugomi. Vis dėlto, teisės aktai taip pat numato tam tikrus saugojimo terminus. Šiuo aspektu reikšmingas dokumentas yra poįstatyminis teisės aktas nustatantis personalo valdymo dokumentų saugojimo trukmę. Darbdavys ar kiti atsakingi darbuotojai gali aiškiai susipažinti, kokie su darbuotojais susiję dokumentai privalo būti saugomi atitinkamą laikotarpį (pavyzdžiui, įsakymai dėl atostogų, komandiruočių saugomi 10 metų, o darbo sutartis net 50 metų) (Lietuvos vyriausiojo archyvaro įsakymas ..., 2011). Pastebėtina, kad būtent darbo sutarties saugojimo terminas yra dažnai kritikuotinas. Darbuotojas gali palikti darbą vos po dienos, o tokia jo darbo sutartis su visais

surinktais asmens duomenimis bus saugoma 50 metų. Taigi, darbdavys siekdamas įgyvendinti visus BDAR reikalavimus turėtų pagrįstai pasirinkti saugojimo laikotarpį ir netvarkyti darbuotojo asmens duomenų ilgiau, nei tai yra būtina.

Darbuotojo asmens duomenų ištrynimas praėjus saugojimo laikotarpiui. Darbdavys, atsižvelgęs į darbuotojo asmens duomenų tvarkymo ypatumus, gali priimti sprendimą panaikinti nereikalingus duomenis. Tuo atveju, jeigu dalis informacijos vis dėlto yra reikalinga, tokie duomenys gali būti anonimizuojami arba archyvuojami viešojo intereso, mokslo ar istorijos tikslais ar statistikos tikslais (Europos Sąjungos pagrindinių teisių agentūra, 2018, p. 134). Duomenys gali teikti naudą. Todėl dalis informacijos tokiu būdu bus išsaugota. Svarbu yra tai, kad įgyvendinant anonimizavimą neliktų galimybės nustatyti konkretų fizinį asmenį. Pasirinkus netaikyti anonimizavimo visi surinkti darbuotojo asmens duomenys turi būti negrįžtamai ištrinti. Pavyzdžiui, dokumentai, įvairūs popieriai sunaikinti su smulkintuvu, prieš pašalinant pačią saugojimo laikmeną (kietasis diskas, USB, CD, DVD ar kt.), joje saugoti duomenys pasitelkiant programinę įrangą privalo būti ištrinti. Tais atvejais, kai tai padaryti neįmanoma, gali būti pasirinktas fizinis duomenų laikmenos sunaikinimas be galimybės jos atstatyti (Valstybinė duomenų apsaugos inspekcija, 2018, p. 14). Tik negrįžtamas ir neatkuriamas asmens duomenų, įskaitant laikmenų, sunaikinimas yra tinkama priemonė asmens duomenų apsaugai užtikrinti ir BDAR reikalavimams įgyvendinti.

Tinkama darbuotojo asmens duomenų apsauga privalo būti užtikrinta ir po darbo santykių nutraukimo. Buvęs darbuotojas nepraranda savo teisės į privatumą. Bendrovė Italijoje po darbo santykių nutraukimo nedeaktyvavo buvusio darbuotojo darbinio el. pašto adreso. Darbuotojas teikė prašymus darbdaviui, bet šis į juos neatsakė. Priežiūros institucija nustatė duomenų kiekio mažinimo, duomenų sąžiningumo principų pažeidimus. Be to, nustatė, kad duomenų valdytojas laiku neatsakė į duomenų subjekto prašymą (Italijos nacionalinės priežiūros institucijos 2020 m. liepos 2 d. sprendimas). Taigi, darbdavys elgėsi neskaidriai, nesupažindino darbuotojų su tuo, kad po darbo santykių jų el. pašto dėžutės liks aktyvios. Tokiu būdu rinko ir saugojo perteklinius buvusio darbuotojo asmens duomenis.

Apibendrinant, galima prieiti prie išvados, kad tiek duomenų saugumo užtikrinimas, tiek tinkamas duomenų saugojimo trukmės pasirinkimas gali kelti iššūkius darbdaviui. Darbdavys turi atlikti rizikos vertinimą, įsivertinti savo duomenų tvarkymo operacijas. Bendrovėje turi būti įdiegiamos tinkamos techninės ir organizacinės priemonės, kurios būtų efektyvios ir veiksmingos apsaugant fizinių asmenų teises ir laisves. Darbdavys turi informuoti apie savo pasirinktas saugumo priemones. Pasibaigus būtinumui tvarkyti darbuotojo asmens duomenis ir praėjus atitinkam saugojimo laikotarpiui privaloma ištrinti asmens duomenis arba juos nuasmeninti taip, kad fizinio asmens tapatybė negalėtų būti nustatyta. Duomenų valdytojas turi gebėti pagrįsti duomenų saugojimo laikotarpio pasirinkimą ar kitus priimtus sprendimus susijusius su duomenų saugumu ir jų saugojimu.

3. Tolimesni asmens duomenų apsaugos iššūkiai darbo santykiuose

Susipažinus su esamais darbuotojo asmens duomenų apsaugos iššūkiais randasi poreikis toliau išsamiai pradėti nagrinėti ateityje galinčius kilti. Šis teiginys gali būti paaiškintas tuo, kad teisinis reguliavimas yra linkęs atsilikti nuo to, kas iš tiesų vyksta kasdieniame gyvenime. Sparti technologinė plėtra, išaugę duomenų rinkimo ir tvarkymo mastai leidžia privačioms bendrovėms ir valdžios institucijoms tvarkyti darbuotojo asmens duomenis beprecedenčiais kiekiais (BDAR preambulės 6 punktas). Todėl svarbu išlikti budriems ir iš anksto pasiruošti galimiems teisiniams ir praktiniams iššūkiams.

Svarbu atkreipti į tai, kad pamatiniai, fundamentalūs teisės principai, išaiškinimai ir (ar) argumentai gali likti nepakitę arba su gyvenime egzistuojančiais iššūkiais transformuotis kartu. Taigi, naujos technologijos ir nauji asmens duomenų apsaugos teisės srityje kylantys iššūkiai darbo santykiuose nepaneigia darbuotojo teisės į privatumą (ES pagrindinių teisių chartijos 7-8 straipsniai, Sutarties dėl ES veikimo 18 straipsnis, Lietuvos Respublikos Konstitucijos 22 straipsnis). Atvirkščiai, teisė į privatumą yra vis labiau aktualizuojama. Europos Komisija siekia sustiprinti šią apsaugą deklaruodama, kad kiekvieno asmens teisė į asmens duomenų apsaugą galioja ir internete (Europos Komisija, 2022, p. 5). Atsižvelgiant į tai, kuo anksčiau būtina atpažinti galimus sunkumus ir ieškoti priemonių jiems spręsti.

3.1. Darbuotojo asmens duomenų tvarkymas pasitelkiant dirbtinį intelektą

Dirbtinio intelekto (angl. *artificial intelligence*) naudojimas darbo santykiuose nėra visiškas naujadaras, bet panašu, kad vis daugiau duomenų valdytojų pasiryžta jį naudoti. Pirmiausiai, dirbtinis intelektas gali būti suprantamas kaip objektas, kuriam programinio kodo ir surinktų duomenų pagalba yra sukuriamas intelektas. Dirbtinis intelektas yra užpildomas algoritmais. Algoritmais gali būti atliekami šie veiksmai: automatizuotas duomenų tvarkymas, skaičiavimai, vertinimai, sprendimų priėmimas ir kt. (Europos Sąjungos pagrindinių teisių agentūra, 2018, p. 363). Programinį kodą parašo programuotojas. Tačiau reikšmingiausia dalis yra duomenys, kurie yra išgaunami iš duomenų subjekto. Skaitmeninės technologijos sukuria daug darbuotojo asmens duomenų, kuriuos gali panaudoti įvairiems tikslams, pavyzdžiui, įdarbinimo, atleidimo, užduočių paskirstymo, efektyvumo, veiklos vertinimo, stebėjimo procesuose (Mandl, 2021, p. 23).

Neapibrėžtas ir platus dirbtinio intelekto panaudojimas darbo santykiuose kelia reikšmingus duomenų apsaugos teisės iššūkius. Darbuotojas tampa sekamu.

Dirbtinis intelektas kelia įvairias rizikas. Dirbtinis intelektas perbraižo darbuotojo stebėsenos ribas ir galimybes. Nuo šiol stebėsena išreiškiama klavišų paspaudimais, soc. tinklų sąveika, ekrano kopijomis, paieškos rezultatais, veido atpažinimo sistema, išmaniųjų telefonų jutikliais ir kt. (Aloisi *et al.*, 2019, p. 105). Atsižvelgiant į tai, kad dirbtinis intelektas yra įrankis, kurio pagalba gali būti surinkti milžiniški duomenų kiekiai susiję su konkrečiu darbuotoju, formuojasi terpė pažeisti darbuotojo teises ir laisves. Pirma, kyla rizika, kad bus pažeistas asmens duomenų konfidencialumas (BDAR 32 straipsnio 2 dalis). Kuo daugiau asmens duomenų yra tvarkoma, tuo daugiau jų gali būti neteisėtai atskleisti tretiesiems asmenims. Antra, grėsmė yra susijusi su tvarkomų asmens duomenų panaudojimu neteisėtais tikslais. Pavyzdžiui, surinkta informacija galima manipuliuoti, šantažuoti, daryti įtaką, spaudimą, diskriminuoti ar netgi pavogti asmens tapatybę (Europos Sąjungos pagrindinių teisių agentūra, 2018, p. 366). Todėl, darbdavys turėtų gebėti identifikuoti grėsmes, susipažinti su dirbtinio intelekto loginiu pagrindimu ir valdyti rizikas. Duomenų saugumą užtikrinant pasirinkus tinkamas technines ir organizacines saugumo priemones, įgyvendinant pavojaus mažinimo priemones, pavyzdžiui, pseudonimizavimą, šifravimą, prieigų valdymą.

Duomenų valdytojas rizikuoja tvarkyti perteklinius darbuotojo asmens duomenis. Reglamentas įtvirtina duomenų kiekio mažinimo principą (BDAR 5 straipsnio 1 dalies c punktas). Šiame darbe jau ne kartą buvo minėta, kad darbdavys privalo įsivertinti, kokie asmens duomenys jam iš tiesų yra reikalingi. Todėl, tuo atveju, kai yra pasitelkiamas dirbtinis intelektas reikėtų sunerimti. Dirbtinis intelektas yra minėto principo priešingybė, nes jis kuria pridėtinę vertę tik apdorojęs milžiniškus duomenų kiekius (Europos Sąjungos pagrindinių teisių agentūra, 2018, p. 368). Bendrovė turėtų pasverti: ar turėti ir žinoti mažiau, bet atitikti BDAR įtvirtintus reikalavimus; ar pasiryžti prisiimti riziką ir naudoti dirbtinį intelektą. Prisiėmus riziką, būtina dirbtinio intelekto veikimo analizė. Įprastai sistemos yra sukalibruotos taip, kad automatiškai renka apie darbuotoją ypač detalius ir *per se* perteklinius duomenis (Aloisi *et al.*, 2019, p. 105-106). Taigi, darbdavys privalo suprasti duomenų srautus ir apimtis. Negali būti pateisinama situacija, kai duomenų valdytojas nežinojo rinksiąs duomenis. Tokio pobūdžio surinkti duomenys privalo būti tinkamai apsaugoti.

Skaidrumo problematika pasitelkiant dirbtinį intelektą. Darbuotojas nepraranda teisės būti informuotam (BDAR 12 straipsnis), kai darbovietėje ar jos sistemose yra įdiegtas ir naudojamas dirbtinis intelektas. Kaip tik, reikėtų skirti didesnį dėmesį siekiant užtikrinti atitikti tinkamo informavimo pareigą. Dirbtinis intelektas kaip priemonė yra susijusi su techninio pobūdžio aspektais. Ne kiekvienas teisininkas ar juolab darbuotojas galėtų aiškiai atsakyti ir suprasti, kaip yra tvarkomi jo asmens duomenys. Todėl informaciją būtina pateikti prieš pradedant rinkti duomenis, lengvai prieinamu ir suprantamu būdu, pateikiant aiškia ir paprasta kalba (BDAR preambulės 39 punktas). Šioje situacijoje negali likti jokių nutylėtų aspektų, nes bet koks informacijos nukrypimas gali lemti neskaidrų asmens duomenų tvarkymą. Tai ypač svarbu, kada dirbtinis intelektas realiai priima vienokius ar kitokius sprendimus turinčius ar galinčius turėti reikšmės darbuotojui (Europos Sąjungos pagrindinių teisių agentūra, 2018, p. 369). Skaidrumas neturėtų būti paneigtas mainais į nedidelį atlygį, paaukštinimą ar kitas naudas. Be to, ir tada, kai tuos duomenis iš esmės surenka ir pateikia pats darbuotojas dėvėdamas įrenginius (pavyzdžiui, išmaniuosius akinius) ar dalyvaudamas vidinėse darbovietės programose (Aloisi *et al.,* 2019, p. 106). Informacija turi būti pateikta laiku, ji turi būti suprantama. Neturi kilti abejonių, kad kažkas nutylima ar juolab užslepiama neaiškiomis tvarkomis, teisiniu žargonu. Darbuotojui turi būti aišku, kai naudojamas dirbtinis intelektas.

Darbuotojų atstovai turi būti aktyvesni, kai yra pasitelkiamas dirbtinis intelektas. Informavimas ir konsultavimas tvirtinant vidines tvarkas yra reikšmingas, nes yra įtraukiami darbuotojai ir jų atstovai (Darbo kodekso 206 straipsnis). Darbdavys neturėtų laikytis formalaus požiūrio ir (ar) neturėtų nepasitikėti savo paties darbuotojais, jog šie siekia jam pakenkti, apsunkinti teisinėmis procedūromis. Tinkamas informavimas ir konsultavimas gali leisti darbdaviui iš anksto pasitikrinti, kokios technologijos gali būti priimtinos, o kurios būtų sutiktos neigiamai. Socialiniai partneriai gali būti naudingi savo įžvalgomis, sprendimais ir pasiūlymais, kurie pabrėžtų teigiamą skaitmeninių technologijų panaudojimą gerbiant darbuotojo teises į privatumą (Mandl, 2021, p. 41). Tiesa, galima ir kita pozicija, kuri gali būti labiau radikalesnė, bet tuo pačiu rezultatyvi. Nogarede mano, kad darbo tarybos turi reikalauti reguliarių konsultacijų su darbdaviu ir siekti susitarimų, kurie leistų koreguoti naudojamas sistemas asmens duomenų tvarkymui (Nogarede, 2021, p. 29-30). Darbo tarybos kaip darbuotojų pasitikėjimo pagrindu išrinktas organas turėtų galėti aktyviai atstovauti darbuotojų interesams. Tačiau turi būti siekiama suderinti skirtingus šalių interesus, susipažinti su darbdavio argumentais, įvertinti kylančias rizikas

ir galimas naudas. Darbuotojų ir jų atstovų vaidmuo asmens duomenų apsaugos teisės srityje yra iš esminių priemonių ribojančių darbdavio neteisėtiems veiksmams.

Galimos teisių gynimo priemonės, kai pasitelkiamas dirbtinis intelektas. Be to, kad duomenų subjektai gali pasinaudoti Reglamente įtvirtintomis teisėmis į duomenų apsaugą. Galimos ir kitos alternatyvios priemonės. Autoriai pabrėžia, kad dirbtinio intelekto diegimas įdarbinimo, veiklos vertinimo ir kitų procesų metu turi tapti kolektyvinių derybų objektu (Roething *et al.,* 2021). Skaitmeninių technologijų diegimas apipintas tokiomis diskusijomis kainuotų daug brangaus laiko. Sutrikdytų galimus darbdavio ketinimus greitai ir efektyviai pakeisti darbo organizavimo procesus. Darbuotojai naudotųsi Europos Komisijos deklaruojamais tikslais užtikrinti skaidrų algoritmų ir dirbtinio intelekto panaudojimą (Europos Komisija, 2022, p. 4). Tai savaime reikštų darbuotojų teisėtus reikalavimus suteikti išsamią informaciją apie įdiegtas technologijas, jų loginį pagrindimą, veikimą, naudą, rizikas. Tokie reikalavimai įpareigotų darbdavį, kuo skubiau atlikti poveikio duomenų apsaugai vertinimą. Užsienio autoriai atkreipia dėmesį, kad darbuotojų teisė į privatumą gali būti apginta pasitelkiant streiką kaip priemonę (Roething *et al.,* 2021). Sutiktina su šia autorių pozicija, kad streikas galėtų būti viena iš alternatyvių priemonių siekiant apsaugoti savo teises ir laisves į privataus asmens gerbimą.

Apibendrinant, prieita prie išvados, kad dirbtinis intelektas ne tik, kad jau yra iššūkiu darbo santykių šalims, bet negana to, jo populiarumas tik augs. Dirbtinis intelektas yra viena iš darbdavio kaštų mažinimo priemonių. Uždrausti juo naudotis būtų neproporcinga. Tačiau darbdavys turi įsivertinti kylančią šio skaitmeninės technologijos riziką – perteklinį asmens duomenų tvarkymą milžinišku mastu. Turi įdiegti ne tik, kad tinkamas saugumo priemones, bet tuo pačiu ir duomenų kiekį mažinančias priemones, siekiant atsisakyti nebūtinų duomenų. Atsižvelgiant į sudėtingą ir neaiškų algoritmų ir dirbtinio intelekto veikimo metodus ir principus, darbdavys turi imtis papildomų priemonių skaidrumui ir tinkamam darbuotojo informavimui užtikrinti. Darbdavys turėtų atkreipti dėmesį, kad tuo atveju, kai yra peržengiamos asmens duomenų tvarkymo ribos, darbuotojų atstovų vaidmuo tampa reikšmingiausias ginant darbuotojų teises ir laisves. Darbuotojai ir jų atstovai išlikdami aktyvūs gali vesti kolektyvines derybas, derėtis, teikti siūlymus, sprendimus, kurie būtų naudingi abejoms šalims. Kaip vienas iš labiausiai nepalankiausių galimų iššūkių darbdaviui, yra tai, jog nepasisekus pasiekti susitarimų ar nesilaikant jų, galės būti taikoma *ultima ratio* priemonė – darbuotojų streikas.

3.2. Darbuotojo asmens duomenų tvarkymas virtualioje realybėje

Netolima ateitis ruošiasi dar labiau precedento neturintiems asmens duomenų rinkimo ir tvarkymo mastams. COVID-19 liga padarė įtakos į tai kaip suprantame darbo vietos sampratą. Nuotolinis darbas tapo nebe išimtis iš taisyklės, bet kitaip ir nesuprantama būtinybė. Bendrovės tapo drąsios besikišdamos į darbuotojų gyvenimą, pavyzdžiui, „Amazon“ šnipinėdama savo darbuotojus privačiose soc. tinklo „Facebook“ grupėse, ar net ir mažų darbdavių pastangos pasitelkiant veido atpažinimo sistemas stebėti darbuotojo darbą nuotoliniu būdu (Roething *et al.*, 2021). Hibridinis darbo modelis išpopuliarėjo. COVID-19 liga privertė persvarstyti, kaip atrodys ateities darbovietės. Manoma, kad nauji biurai bus lankstūs, apjungiantys skirtingas erdves, sudarant galimybes dirbti tiek darbovietėje, tiek nuotoliniu būdu (Pennel, 2021). Tačiau didžiosios korporacijos kaip „Facebook“, „Microsoft“ ar kt. svarsto apie jau visiškai kitokias darbui skirtas erdves – virtualios realybės (Blum, 2022). Ši mintis intriguoja, verčia svarstyti apie naujas galimybes ir kylančius iššūkius. Atsižvelgiant į tai, svarbu kuo anksčiau pradėti diskutuoti ir surasti atsakymus kaip apsaugoti nykstančią darbuotojo teisę į privatumą.

Virtuali realybė kaip nauja darbuotojo darbo vieta. J. Zaleskis vienas pirmųjų Lietuvoje pradėjo kelti diskusijas apie ribos tarp virtualiosios ir fizinės realybės ištrynimą (Zaleskis, 2019, p. 318). Šiandien mums jau yra žinoma, kad „Facebook“ kuria darbo kambarius metavisatoje (angl. *metaverse*). Šiuo tikslu bendrovė netgi pakeitė savo pavadinimą į „Meta“. Deklaruojama, kad virtualūs darbo kambariai panaikins fizinį atstumą tarp žmonių, pagerins komandinį darbą, leis bendradarbiauti ir bendrauti nuotoliniu būdu naudojant virtualios realybės (angl. *VR*) akinius (Meta, 2021). Darbuotojai jau dabar kelia klausimus: kodėl privalo vykti į darbą, sugaišti daug brangaus laiko ir sėdėti prie to paties kompiuterio, kai tai galima padaryti iš namų (Pennel, 2021). Taigi, neabejotina, kad vienu ar kitu būdu darbo vietos samprata keisis. Manytina, kad bendrovės siekdamos sutaupyti dar daugiau žmogiškųjų ir finansinių išteklių – perkels savo darbus į virtualios realybės darbo kambarius.

Metavisata kaip darbuotojo asmens duomenų rinkimo ir tvarkymo vieta. Įprasta, kad viena iš skaitmeninės technologijos funkcijų yra duomenų surinkimas ir tvarkymas. Virtuali realybė neišvengs asmens duomenų tvarkymo operacijų, netgi kaip tik manytina, kad duomenų apimtys tik išaugs. „Meta“ teigia, kad užtikrins privatumą, neapdoros vaizdo įrašų, aplinkos vaizdų, neperduos duomenų tretiesiems asmenims, sudarys galimybę pačiam naudotojui kontroliuoti ir valdyti duomenis (Meta, 2021). Visgi, autoriaus nuomone, ši deklaratyvi pozicija yra abejotina.

Lygiai taip pat kaip ir soc. tinklo „Facebook“ atveju, gali būti pagrįstai keliamas klausimas: kas generuos šio produkto pajamas? Metavisata ypač susitelks į biometrinių asmens duomenų tvarkymą, o tai savaime kels daugybę naujų iššūkių (Blum, 2022). Šiandien jau esami duomenų srautai nėra tinkamai suvaldomi. Kaip bus suvaldyti išaugę dar milžiniškesni duomenų kiekiai? Atsižvelgiant į tai, pirma, darbdaviai turėtų labai gerai apsvarstyti kaip užtikrins darbuotojo teisę į privatumą, prieš pradėdami naudoti virtualios realybės darbo kambarius (Beioley, 2022, p. 4). Taigi, darbdaviai turėtų tinkamai suvokti virtualios realybės veikimą, duomenų rinkimo ir tvarkymo apimtis, kylančias rizikas, bei ieškoti priemonių užtikrinančių darbuotojo asmens duomenų apsaugą.

Darbuotojo kūnas kaip duomenų rinkimo ir tvarkymo vienetas. Informacija renkama vos keliais paspaudimais, pavyzdžiui, mygtuku „Patinka“ soc. tinkluose, o tinkama duomenų analizė gali atskleisti neregėtus mastus informacijos (Zaleskis, 2019, p. 319). Jeigu dirbtinis intelektas rinko daug duomenų, ypač siekiant to, kad veiktų be klaidų. Virtualios realybės atveju jų bus dar daugiau. „Meta“ ketina rinkti duomenis nuo akių, nosies trūkčiojimo iki kūno judesių. Manoma, kad be galo asmeniškų asmens duomenų tvarkymas leis tikslingiau parduoti reklamas tretiesiems asmenims (Beioley, 2022, p. 3). Autoriaus nuomone, metavisatoje visas asmens kūnas bus nuskanuotas ir apdorojamas. Biometriniai duomenys bus renkami plačiausia įmanoma prasme: veidas, akies rainelė, balsas, pirštų antspaudai ir pan. Todėl, griežtas teisinis reguliavimas, masinis biometrinių asmens duomenų tvarkymo uždraudimas gali būti reikšminga priemonė siekiant apsaugoti darbuotojo teises (Roething *et al.*, 2021). Autorius mano, kad biometriniai duomenys bus naudojami asmens identifikavimui prisijungti prie virtualios realybės erdvės. Reiškia, tokios asmens duomenų tvarkymo apimties atsisakyti ar pasirinkti nei darbuotojui, nei darbdaviui nebus įmanoma.

Darbuotojo asmens duomenų tvarkymo teisinio reguliavimo stoka virtualioje realybėje. Paradoksalu, bet pakankamai naujo teisinio dokumento – BDAR – gali nebepakakti. Šiandien yra daugybę teisinių klausimų ir mažai teisinio reguliavimo susijusio su virtualia realybe, o ypač biometrinių asmens duomenų apsauga, kurių tvarkymas bus gausus (Blum, 2022). Teisė virtualioje realybėje kol kas nėra pakankamai akivaizdi. Nėra aiškūs neteisėto asmens duomenų tvarkymo atsakomybės aspektai. Autorius svarsto, kad nagrinėjant vaidmenų aspektą, duomenų tvarkytoju bus laikoma „Meta“, o duomenų valdytoju – darbdavys. Tačiau nėra aišku, kiek realiai duomenų

valdytojas turės galimybių nustatyti duomenų tvarkymo tikslus, pasirinkti saugumo priemones ir pan.

Atsižvelgiant į tai, kad virtuali realybė, daiktų internetas dar nėra plačiai naudojamas ekonomikoje, daugiausia dėl išlaidų ir įgūdžių reikalavimų. Atitinkamai skaitmeninės technologijos yra paplitusios tarp didžiųjų korporacijų (Mandl, 2021, p. 8). Taip pat atsižvelgiant į tai, kad įstatymų leidėjas yra linkęs atsilikti reguliuodamas naujųjų technologijų teisines problemas, autoriaus nuomone manytina, kad būtent didžiosios bendrovės brėš duomenų tvarkymo ribas. Žinoma su tuo kovoti turės darbuotojų atstovai, kurie privalės imtis iniciatyvų siūlydami platesnę teisių apsaugą suskaitmenintoje darbo vietoje (Nogarede, 2021, p. 18). Tiesa, autorius atkreipia dėmesį ir į visiškai kitą aspektą susijusį su BDAR, pavyzdžiui, BDAR įtvirtina teisę į duomenų perkeliamumą (BDAR 20 straipsnis). Pastebima, kad šia teise kol kas nėra dažnai naudojamasi. Tačiau būtent virtualios realybės dėka, galimai skirtingų virtualios realybės serverių dėka, tai taps įmanoma. Apibendrinant galima teigti, kad nors bendri principai ir liks galioti. Bendrovės turės galimybių nustatyti ribas. Tuo tarpu, socialiniai partneriai ir įstatymų leidėjai privalo išlikti aktyvūs. Taigi, kol kas lieka neaišku ar BDAR tikrai atlaikys šį išbandymą ir ar nereikės naujų teisinių instrumentų.

Apibendrinant, galima pagrįstai teigti, kad virtualios realybės darbo kambariai yra tolimesnis iššūkis darbo santykiuose. Koronavirusas (COVID-19 liga) ir nuotolinio darbo praktika paskatino diskusijas apie virtualios realybės kūrimą darbo santykiuose (angl. *metaverse*). Neabejotina, kad darbuotojo asmens duomenų rinkimo ir tvarkymo vieta taps virtualios realybės darbo kambariai prie kurių bus galimybė prisijungti tik mainais į daugybę biometrinių asmens duomenų. Manytina, kad darbdavys įpareigos darbuotojus perkelti savo kūnus į virtualią realybę. Nors ir galbūt siekdamas pozityvių tikslų, bet rizikuodamas savo paties darbuotojų saugumu. Virtualios realybės duomenų serveriai saugos milžiniškus darbuotojo biometrinius asmens duomenis, kurių atskleidimas tretiesiems asmenims galės kelti neregėtus pavojus, įskaitant, bet neapsiribojant tapatybės vagyste. Milžiniškas išbandymas laukia jau dabar griežtas asmens duomenų tvarkymo taisykles įtvirtinančiam teisiniam dokumentui – BDAR. Kol kas nėra aišku, ar Reglamentas bus pajėgus sureguliuoti virtualioje realybėje kylančius darbuotojo asmens duomenų apsaugos teisinius iššūkius.

IŠVADOS

1. Darbo santykiuose vyrauja galios disbalansas, todėl egzistuoja plona riba tarp teisėto ir neteisėto asmens duomenų tvarkymo. Atsižvelgiant į tai, kad sutikimo teisiniam pagrindui yra keliamos griežtos sutikimo sąlygos (įskaitant teisę bet kuriuo metu atšaukti), siūlytina, jog sutikimo teisinis pagrindas darbo santykiuose būtų *ultima ratio* priemonė. Neskaidrus asmens duomenų tvarkymas yra pavojingas darbuotojo teisėms ir laisvėms, todėl privaloma siekti suderinti skirtingus darbo santykių šalių interesus asmens duomenų apsaugos teisės srityje.

2. Duomenų valdytojo požiūris į duomenų apsaugą privalo keistis. Darbdavys tvarkydamas darbuotojo asmens duomenis gali susidurti su įvairiais duomenų apsaugos teisės probleminiais aspektais: nuo perteklinio vaizdo stebėjimo darbo vietoje iki informacijos saugojimo darbiniame el. pašte po darbo santykių nutraukimo ar tinkamo atsakingų darbuotojų instruktavimo kaip tvarkyti ir užtikrinti (ypač sveikatos) asmens duomenų konfidencialumą. Visi įvardinti duomenų apsaugos iššūkiai gali būti įveikti, jeigu darbdavys laikysis duomenų apsaugos teisės principų, įgyvendins tinkamas technines ir organizacines priemones visų asmens duomenų rinkimo ir tvarkymo procesų metu, bei bendradarbiaus su darbuotojais ir jų atstovais. Autorius taip pat atkreipia dėmesį, kad didelė rizika teisei į privatumą gali kilti platformų darbuotojams, tačiau šiuo aspektu yra reikalingas išsamesnis mokslinis tyrimas.

3. Teisė yra linkusi atsilikti nuo technologinės pažangos. Sparti technologinė plėtra ir naujų informacinių technologijų diegimas darbo santykiuose gali kelti naujus su duomenų apsaugą susijusius iššūkius. Darbuotojas gali nesuprasti algoritmų ir dirbtinio intelekto techninių subtilybių, todėl darbdavys turėtų imtis papildomų priemonių skaidrumui užtikrinti. Kartu autorius mano, kad koronavirusas (COVID-19 liga) paskatino didžiąsias korporacijas kurti virtualios realybės darbo kambarius, o tai lemia, jog visas darbuotojo kūnas taps duomenų rinkimo ir tvarkymo vienetu. Tampa akivaizdu, kad pakankamai naujas BDAR greitai besikeičiančioje aplinkoje jau spėjo pasenti ir tapti nepajėgus.

ŠALTINIŲ SĄRAŠAS

Teisės norminiai aktai:

Tarptautiniai ir Europos Sąjungos teisės aktai:

1. 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). OJ L 119, 4.5.2016.
2. Sutartis dėl Europos Sąjungos veikimo. OL 2012 C 326, p. 1-390.
3. Žmogaus teisių ir pagrindinių laisvių apsaugos konvencija, iš dalies pakeista protokolais Nr. 11 ir Nr. 14, *Valstybės žinios*, 2011-12-22, Nr. 156-7390.
4. 2000 m. gruodžio 7 d. Europos Sąjungos pagrindinių teisių chartija. OL 2012 C 326, p. 391–407.

Lietuvos Respublikos teisės aktai:

5. Lietuvos Respublikos Konstitucija (1992). *Valstybės žinios*, 33-1014.
6. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas (1996). *Valstybės žinios*, 63-1479.
7. Lietuvos Respublikos konkurencijos įstatymas (1999). *Valstybės žinios*, 30-856.
8. Lietuvos Respublikos elektroninių ryšių įstatymas (2004). *Valstybės žinios*, 69-2382.
9. Lietuvos Respublikos darbo kodeksas (2016). TAR, 23709.
10. Valstybinės duomenų apsaugos inspekcijos direktoriaus įsakymas dėl duomenų tvarkymo operacijų, kurioms taikomas reikalavimas atlikti poveikio duomenų apsaugai vertinimą, sąrašo patvirtinimo (2019). TAR, 4104.
11. Lietuvos Respublikos Vyriausybės nutarimas dėl Darbų ir veiklos sričių, kuriose leidžiama dirbti darbuotojams, tik iš anksto pasitikrinusiems ir vėliau periodiškai besitikrinantiems, ar neserga užkrečiamosiomis ligomis, sąrašo, Darbų ir veiklos sričių, kuriose leidžiama dirbti darbuotojams, pasitikrinusiems ir (ar) periodiškai besitikrinantiems, ar neserga užkrečiamąja liga, dėl kurios yra paskelbta valstybės lygio ekstremalioji situacija ir (ar)

karantinas, sąrašo ir šių darbuotojų sveikatos tikrinimosi tvarkos patvirtinimo (1999). *Valstybės žinios*, 41-1294.

12. Lietuvos vyriausiojo archyvaro įsakymas dėl bendrųjų dokumentų saugojimo terminų rodyklės patvirtinimo (2011). *Valstybės žinios*, 32-1534.

Specialioji literatūra:

13. Aloisi, A. and Gramano, E. (2019). Artificial Intelligence is Watching You at Work: Digital Surveillance, Employee Monitoring, and Regulatory Issues in the EU Context, *Comparative Labor Law & Policy Journal*, 41 (1), 101-127.
14. Ball, K. (2021). Electronic Monitoring and Surveillance in the Workplace. *Luxembourg: Publications Office of the European Union*, p. 1-104, https://doi:10.2760/5137.
15. Blum, S. (2022). *As workers enter the metaverse, how much privacy will they surrender at the virtual door?* [interaktyvus], HR Brew. Prieiga per internetą: https://www.morningbrew.com/hr/stories/2022/03/11/as-workers-enter-the-metaverse-how-much-privacy-will-they-surrender-at-the-virtual-door [žiūrėta 2022 m. kovo 30 d.].
16. Bodie T., M. (2021). The Law of Employee Data: Privacy, Property, Governance. *Indiana Law Journal*, 97, 1-68.
17. Broecke, S. (2022). *Artificial intelligence as a matchmaker in the job market* [interaktyvus]. Prieiga per internetą: https://www.oecd-forum.org/posts/artificial-intelligence-as-a-matchmaker-in-the-job-market-da864776-ebe1-42b6-a8ef-6edb9ff61b78 [žiūrėta 2022 m. kovo 30 d.].
18. Davulis, T. (2018). *Lietuvos Respublikos darbo kodekso komentaras*. Vilnius: Registrų centras.
19. Grigonienė, R. (2020). Darbuotojų asmens duomenų apsaugos užtikrinimo teisinio reguliavimo ypatumai, *Jurisprudencija*, 27 (2), 346-369, https://doi.org/10.13165/JUR-20-27-2-06.
20. Mandl, I. (2021). The digital age: Implications of automation, digitisation and platforms for work and employment. *Luxembourg: Publications Office of the European Union*, p. 1-34, https://doi:10.2806/288.
21. Nogarede, J. (2021). *No digitalisation without representation* [interaktyvus], Foundation for European Progressive Studies. Prieiga per internetą: https://www.feps-

europe.eu/attachments/publications/policy%20study_no%20digitalisation2.pdf [žiūrėta 2022 m. kovo 30 d.].

22. Ogriseg, C. (2017). *GDPR and Personal Data Protection in the Employment Contex* [interaktyvus], Milanas: Università degli Studi di Milano. Prieiga per internetą: https://labourlaw.unibo.it/article/download/7573/7276/22859 [žiūrėta 2022 m. kovo 30 d.].
23. Pennel, D. (2021). *What will the workplace of the future look like?* [interaktyvus]. Prieiga per internetą: http://englishbulletin.adapt.it/what-will-the-workplace-of-the-future-look-like/ [žiūrėta 2022 m. kovo 30 d.].
24. Petkevičienė, V. ir kt. (2020). Asmens duomenų tvarkymo iššūkiai COVID-19 pandemijos metu, *Jurisprudencija*, 27 (2), 330-345, https://doi.org/10.13165/JUR-20-27-2-05.
25. Roething, O. and Naranjo, D. (2021). *Workplace, public space: workers organising in the age of facial recognition*. Social Europe [interaktyvus]. Prieiga per internetą: https://socialeurope.eu/workplace-public-space-workers-organising-in-the-age-of-facial-recognition [žiūrėta 2022 m. kovo 30 d.].
26. Stanev, S. (2019). Monitoring of Employees' Personal Communications at Work. Practice of the ECtHR, *E-Journal of International and Comparative Labour Studies*, 8, 94-103.
27. Tamašauskaitė-Janickė, G. (2016). *Informacinių ir komunikacinių technologijų panaudojimas darbo vietoje darbo teisės požiūriu*. Daktaro disertacija, socialiniai mokslai, teisė (01 S), Vilniaus universitetas. Vilnius. Prieiga per internetą: http://epublications.vu.lt/object/elaba:16977251/16977251.pdf [žiūrėta 2022 m. kovo 30 d.].
28. Torres Garcia, B. (2021). Spain's Law No. 10/2021 on Teleworking: Strengths and Weaknesses. *E-Journal of International and Comparative Labour Studies*, 10, 41-61.
29. Zaleskis, J. (2019). *Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė: monografija*. Vilnius: Registrų centras.

Teismų praktika:

Tarptautinė ir Europos Sąjungos teismų praktika:

30. *Patrick Breyer* [ESTT], Nr. C-582/14, [2016-10-19]. ECLI:EU:C:2016:779.

31. *Surikov prieš Ukrainą* [EŽTT], Nr. 42788/06, [2017-01-26]. ECLI:CE:ECHR:2017:0126 JUD004278806.
32. *Rīgas satiksme* [ESTT], Nr. C-13/16, [2017-05-04]. ECLI:EU:C:2017:336.
33. *Bărbulescu prieš Rumuniją* [EŽTT], Nr. 61496/08, [2017-09-05]. ECLI:CE:ECHR:2016:0112 JUD006149608.
34. *Antović ir Mirković prieš Juodkalniją* [EŽTT], Nr. 70838/13, [2017-11-28]. ECLI:CE:ECHR:2017:1128 JUD007083813.
35. *López Ribalda ir kt. prieš Ispaniją* [EŽTT], Nr. 1874/13 ir Nr. 8567/13, [2019-10-17]. ECLI:CE:ECHR:2019:1017 JUD000187413.

Lietuvos vyriausiojo administracinio teismo praktika:

36. Lietuvos vyriausiojo administracinio teismo 2016 m. gruodžio 7 d. nutartis administracinėje byloje Nr. eA-2333-525/2016.
37. Lietuvos vyriausiojo administracinio teismo 2018 m. balandžio 20 d. nutartis administracinėje byloje Nr. A-622-525/2018.
38. Lietuvos vyriausiojo administracinio teismo 2020 m. vasario 5 d. nutartis administracinėje byloje Nr. eA-37-629/2020.
39. Lietuvos vyriausiojo administracinio teismo 2020 m. balandžio 2 d. sprendimas administracinėje byloje Nr. A-3345-822/2020.
40. Lietuvos vyriausiojo administracinio teismo 2022 m. vasario 9 d. nutartis administracinėje byloje Nr. eA-146-415/2022.

Užsienio valstybių teismų praktika:

41. Gimarainso apeliacinio teismo 2016 m. kovo 3 d. sprendimas byloje Nr. 20/14.7T8VRL.G1.
42. Vokietijos Federalinio darbo teismo 2017 m. liepos 27 d. sprendimas byloje Nr. 2 AZR 681/16.
43. Vokietijos Federalinio darbo teismo 2019 m. gegužės 7 d. sprendimas byloje Nr. 1 ABR 53/17.
44. Austrijos Aukščiausiojo Teismo 2020 m. sausio 22 d. sprendimas byloje Nr. 9 ObA 120/19s.

45. Jungtinės Karalystės Aukščiausiojo Teismo 2020 m. balandžio 1 d. sprendimas byloje Nr. [2020] UKSC 12.

Kita praktinė medžiaga:

46. Nyderlandų duomenų apsaugos tarnybos 2020 m. kovo 24 d. sprendimas byloje Nr. CP&A.
47. Nyderlandų duomenų apsaugos tarnybos 2020 m. balandžio 30 d. sprendimas byloje dėl darbuotojų biometrinių asmens duomenų tvarkymo.
48. Suomijos duomenų apsaugos ombudsmeno tarnybos 2020 m. gegužės 18 d. sprendimas byloje Nr. 531/161/20.
49. Italijos nacionalinės priežiūros institucijos 2020 m. liepos 2 d. sprendimas byloje Nr. 9445180.
50. Belgijos duomenų apsaugos institucijos 2020 m. lapkričio 9 d. sprendimas byloje Nr. 72/2020.
51. Rumunijos nacionalinė asmens duomenų tvarkymo priežiūros institucijos 2021 m. balandžio 15 d. sprendimas byloje Nr. S.C. Tip Top Food Industry S.R.L.
52. Liuksemburgo duomenų apsaugos komisijos 2021 m. birželio 7 d. sprendimas byloje Nr. 11FR/2021.
53. Ispanijos duomenų apsaugos agentūros 2021 m. birželio 7 d. sprendimas byloje Nr. PS/00261/2020.
54. Italijos nacionalinės priežiūros institucijos 2021 m. birželio 10 d. sprendimas byloje Nr. 9675440.
55. Danijos duomenų apsaugos agentūros 2021 m. liepos 9 d. sprendimas byloje Nr. Medicals Nordic.
56. Liuksemburgo duomenų apsaugos komisijos 2021 m. liepos 13 d. sprendimas byloje Nr. 24FR/2021.
57. Ispanijos duomenų apsaugos agentūros 2021 m. spalio 18 d. sprendimas byloje Nr. PS/00377/2021.
58. Norvegijos duomenų apsaugos institucijos 2021 m. spalio 19 d. sprendimas byloje Nr. DT-20/00480.
59. Liuksemburgo duomenų apsaugos komisijos 2021 m. lapkričio 2 d. sprendimas byloje Nr. 35FR/2021.

60. Liuksemburgo duomenų apsaugos komisijos 2022 m. sausio 17 d. sprendimas byloje Nr. 47FR/2021.

***Soft law* šaltiniai:**

61. ES 29 straipsnio duomenų apsaugos darbo grupė (2001). *2001 m. rugsėjo 13 d. Nuomonė dėl asmens duomenų tvarkymo darbo santykių kontekste* Nr. 5062/01/EN/Final WP 48 [interaktyvus]. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf [žiūrėta 2022 m. kovo 30 d.].
62. ES 29 straipsnio duomenų apsaugos darbo grupė (2002). *2002 m. gegužės 29 d. Nuomonė dėl elektroninės komunikacijos sekimo darbo vietoje* Nr. 5401/01/EN/Final WP 55 [interaktyvus]. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2002/wp55_en.pdf [žiūrėta 2022 m. kovo 30 d.].
63. ES 29 straipsnio duomenų apsaugos darbo grupė (2014). *2014 m. balandžio 9 d. Nuomonė Nr. 06/2014 dėl duomenų valdytojo teisėtų interesų sampratos pagal Direktyvos 95/46/EB 7 straipsnį* Nr. 844/14/LT WP 217 [interaktyvus]. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_lt.pdf [žiūrėta 2022 m. kovo 30 d.].
64. ES 29 straipsnio duomenų apsaugos darbo grupė (2017). *2017 m. birželio 8 d. Nuomonė Nr. 2/2017 dėl duomenų tvarkymo darbe* Nr. 17/LT WP 249 [interaktyvus]. Prieiga per internetą: https://ec.europa.eu/newsroom/article29/items/610169/en [žiūrėta 2022 m. kovo 30 d.].
65. Valstybinė duomenų apsaugos inspekcija (2018). 2018 m. spalio 31 d. *Tinkamų organizacinių ir techninių duomenų saugumo priemonių įgyvendinimo gairės asmens duomenų valdytojams ir tvarkytojams* [interaktyvus]. Prieiga per internetą: https://vdai.lrv.lt/uploads/vdai/documents/files/Rekomend_tech_priemones_gaires_2018.pdf [žiūrėta 2022 m. kovo 30 d.].
66. Europos duomenų apsaugos valdyba (2020a). *2020 m. sausio 29 d. Gairės 3/2019 dėl asmens duomenų tvarkymo naudojant vaizdo prietaisus* [interaktyvus]. Prieiga per internetą:

https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf [žiūrėta 2022 m. kovo 30 d.].

67. Europos duomenų apsaugos valdyba (2020b). *2020 m. kovo 19 d. Pareiškimas dėl asmens duomenų tvarkymo atsižvelgiant į COVID-19 protrūkį* [interaktyvus]. Prieiga per internetą: https://edpb.europa.eu/sites/default/files/files/file1/edpb_statement_art_23gdpr_20200602_lt_1.pdf [žiūrėta 2022 m. kovo 30 d.].
68. Valstybinė duomenų apsaugos inspekcija (2020a). *2020 m. balandžio 9 d. Rekomendacija dėl darbuotojų asmens duomenų tvarkymo, organizuojant darbą nuotoliniu būdu* [interaktyvus]. Prieiga per internetą: https://vdai.lrv.lt/uploads/vdai/documents/files/Rekomedacija%20del%20darbuotoju%20duomenu%20tvarkymo%20nuotolinio%20darbo%20metu%202020-04-09.pdf [žiūrėta 2022 m. kovo 30 d.].
69. Valstybinė duomenų apsaugos inspekcija (2020b). *2020 m. balandžio 14 d. Rekomendacija dėl darbuotojų sveikatos duomenų tvarkymo, įsigaliojus Darbo kodekso pataisoms dėl karantino* [interaktyvus]. Prieiga per internetą: https://vdai.lrv.lt/uploads/vdai/documents/files/DK%20pataisos%20del%20darbuotoju%20sveikatos%20duomenu%20tvarkymo%20%202020-04-14.pdf [žiūrėta 2022 m. kovo 30 d.].
70. Europos duomenų apsaugos valdyba (2020c). *2020 m. gegužės 4 d. Gairės 05/2020 dėl sutikimo pagal Reglamentą 2016/679* [interaktyvus]. Prieiga per internetą: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_lt_0.pdf [žiūrėta 2022 m. kovo 30 d.].
71. Europos duomenų apsaugos valdyba (2020d). *2020 m. spalio 20 d. Gairės 4/2019 dėl 25 straipsnio Pritaikytoji ir standartizuotoji duomenų apsauga* [interaktyvus]. Prieiga per internetą: https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_lt.pdf [žiūrėta 2022 m. kovo 30 d.].
72. Valstybinė duomenų apsaugos inspekcija (2021). *Duomenų subjekto teisė susipažinti su savo duomenimis: kaip duomenų valdytojui tinkamai įgyvendinti duomenų subjekto prašymą pateikti telefoninio pokalbio įrašo kopiją?* [interaktyvus]. Prieiga per internetą: https://vdai.lrv.lt/uploads/vdai/documents/files/30%20DUK%20D%C4%97l%20telefonin

io%20pokalbio%20iraso%20pateikimo%20kopijos%202021-09-29.pdf [žiūrėta 2022 m. kovo 30 d.].

Kiti šaltiniai:

73. Beioley, K. (2022). *Metaverse vs employment law: the reality of the virtual workplace* [interaktyvus], Financial Times. Prieiga per internetą: https://www.ft.com/content/9463ed05-c847-425d-9051-482bd3a1e4b1 [žiūrėta 2022 m. kovo 30 d.].
74. Europos Komisija (2022). European Declaration on Digital Rights and Principles for the Digital Decade, European Commission.
75. Europos Sąjungos pagrindinių teisių agentūra; Europos Taryba (2018). *Handbook on European Data Protection Law* [interaktyvus], Publications Office of the European Union. Prieiga per internetą: https://op.europa.eu/en/publication-detail/-/publication/5b0cfa83-63f3-11e8-ab9c-01aa75ed71a1 [žiūrėta 2022 m. kovo 30 d.].
76. Meta (2021). *Introducing Horizon Workrooms: Remote Collaboration Reimagined* [interaktyvus]. Prieiga per internetą: https://about.fb.com/news/2021/08/introducing-horizon-workrooms-remote-collaboration-reimagined/ [žiūrėta 2022 m. kovo 30 d.].

SANTRAUKA

Darbuotojo asmens duomenų apsaugos iššūkiai

Artūras Anisimenka

Magistro darbe yra analizuojama pagrindinių darbuotojo asmens duomenų apsaugos iššūkių tema, kuri yra atskleidžiama nagrinėjant BDAR reikalavimus, kitus asmens duomenų apsaugą reglamentuojančius teisės aktus, Lietuvos ir užsienio valstybių teisės mokslininkų doktrininius darbus, tiek Europos Sąjungos Teisingumo Teismo, tiek Europos Žmogaus Teisių Teismo ir Lietuvos vyriausiojo administracinio teismo praktiką, bei priežiūros institucijų duomenų apsaugos teisės srityje pateiktas nuomones, gaires ir rekomendacijas. Nagrinėjama tema geriausiai atskleidžiama per praktinius iššūkius kartu su teisinio reguliavimo analize.

Pagrindinė darbo problema yra plona riba tarp neteisėto darbuotojo asmens duomenų tvarkymo ir darbo santykių šalių interesų pusiausvyros užtikrinimo. Magistro darbe yra identifikuojami pagrindiniai darbo santykiuose vyraujantys darbuotojo asmens duomenų apsaugos iššūkiai. Darbe yra išsamiai išnagrinėjamas darbuotojo asmens duomenų tvarkymas pasitelkiant informacines technologijas: elektronines priemones, dirbtinį intelektą ir kt. Išanalizuojama sveikatos (ypač koronaviruso kontekste), biometrinių, kitų specialiųjų kategorijų asmens duomenų apsauga. Atskleidžiamas darbuotojų atstovų poreikis aktyviai atstovauti darbuotojų interesus asmens duomenų apsaugos teisės srityje. Aptariami kiti galintys kilti darbuotojo asmens duomenų apsaugos iššūkiai ateityje.

Darytina pagrįsta išvada, kad sutikimo teisinis pagrindas darbo santykiuose turi būti *ultima ratio* priemonė. Visi teisiniai ir praktiniai iššūkiai susiję su darbuotojo asmens duomenų apsauga gali būti įveikti. Darbdavys turi laikytis duomenų apsaugos teisės principų, derinti saugumo priemones tarpusavyje, bendradarbiauti su darbuotojais ir jų atstovais. Prieš pasitelkiant naujas skaitmenines technologijas atlikti rizikos vertinimą. Metavisatoje darbuotojo kūnas virs duomenų rinkimo ir tvarkymo vienetu.

SUMMARY

Employee Personal Data Protection Challenges

Artūras Anisimenka

The master's thesis analyses the main employee personal data protection challenges, which is revealed by examining the requirements of the GDPR, other legal acts regulating personal data protection, doctrinal works of Lithuanian and foreign legal scholars, the European Court of Justice, the European Court of Human Rights, and the Supreme Administrative Court of Lithuania, and the opinions, guidelines, and recommendations of the supervisory authorities in the field of data protection law. The topic is best revealed through practical challenges along with regulatory analysis.

The main problem thesis is the thin line between the unlawful processing of an employee's personal data and the balance of interests between the parties to the employment relationship. The main employee personal data protection challenges in the employment relationship are identified in the master's thesis. The work examines in detail the processing of an employee's personal data using information technology: electronic means, artificial intelligence, etc. The protection of health (especially in the context of coronavirus), biometrics, and other special categories of personal data is analysed. The need for employee representatives to actively represent the interests of employees in the field of personal data protection law is revealed. Other possible challenges to the protection of employee personal data in the future are discussed.

It is reasonable to conclude that the legal basis for consent in an employment relationship must be the *ultima ratio* measure. All legal and practical challenges related to the protection of employee personal data can be overcome. The employer must comply with the principles of data protection law, coordinate security measures with each other, and cooperate with employees and their representatives. Carry out a risk assessment before using new digital technologies. In metaverse, an employee's body will become a unit of data collection and processing.