Vilniaus Universiteto Teisės fakulteto
Privatinės teisės katedra

Emilijos Rimanaitės
V kurso, darbo ir socialinės teisės
studijų šakos studentės

Magistro darbas

Modernios technologijos ir darbuotojų privatumo apsauga
Modern Technologies and Protection of Employee Privacy

Vadovas: vyr. lekt. dr. Arnas Paliukėnas

Recenzentas: doc. dr. Justinas Usonis

Vilnius
2025

ANOTACIJA IR PAGRINDINIAI ŽODŽIAI

Šiame darbe analizuojamas modernių technologijų poveikis darbuotojų teisei į privatumą, darbo santykių subjektų teisių ir interesų balanso problematika. Mokslinės literatūros, norminių aktų ir teismų praktikos pagrindu analizuojami iššūkiai, kurie kyla darbuotojų teisei į privatumą, kai darbdavys vykdo kontrolę panaudodamas modernias technologijas stebėsenai, taip pat technologijų naudojimo atvejai, kai yra siekiama darbdavio teisėtų interesų užtikrinimo. Darbe apžvelgiamas pasirinktų Europos Sąjungos valstybių nacionalinis reguliavimas, aptariama geroji praktika ir siūlomi būdai, kaip galima tobulinti galiojančius įstatymus nacionalinėje teisėje, kad jie atitiktų šiuolaikines tendencijas darbo vietoje.

Pagrindiniai žodžiai: Šiuolaikinės technologijos, asmens duomenys, privatumas, duomenų valdytojas, duomenų tvarkytojas, duomenų subjektas, stebėsena.

This paper analyses the impact of modern technologies on the right to privacy of employees and the balance between the rights and interests of the subjects of employment relations. On the basis of scientific literature, normative acts and case law, it analyses the challenges that arise for the right to privacy of employees when the employer exercises control by using modern technologies for monitoring, as well as the cases of using technologies when the employer's legitimate interests are sought to be ensured. The paper reviews the national regulation in selected European Union countries, discusses good practices and suggests ways in which existing laws can be improved to reflect modern trends in the workplace.

Keywords: Modern technologies, personal data, privacy, data controller, data processor, data subject, monitoring.

TURINYS

ĮŽANGA

Temos aktualumas: Šiuolaikiniame pasaulyje sparčiai didėja modernių technologijų įtaka visoms gyvenimo sritims. Technologijų naudojimas darbo santykiuose suteikia asmenims prieigą prie didesnio kiekio duomenų, tad darbdaviams atsiranda vis daugiau galimybių kontroliuoti darbuotojus, siekiant padidinti darbo efektyvumą. Tačiau, turint prieigą prie tokių duomenų, kyla problema užtikrinant darbuotojų teisę į privatumą. Lietuvos Respublikos Konstitucija numato, kad žmogaus privatumas yra neliečiamas, o 2018 metais įsigaliojęs Bendrasis duomenų apsaugos reglamentas, kuriuo siekiama asmens duomenų apsaugos taisykles pritaikyti prie skaitmeninio amžiaus, apima ir šios Konstitucinės teisės užtikrinimą. Darbo santykių kontekste taip pat iškyla problema, kad darbuotojams atsiranda galimybė piktnaudžiauti šia teise ir darbo vietoje vykdyti veiklas, kurios nėra susijusios su jų darbo funkcijų įgyvendinimu, tuo tarpu darbdaviai susiduria su iššūkiais nustatydami teisėtas, proporcingas priemones darbuotojų kontrolei vykdyti, nes egzistuojantis teisinis reguliavimas riboja jų galimybes vykdyti darbuotojų stebėseną darbo metu. Tad būtina rasti balansą tarp efektyvaus modernių technologijų naudojimo darbo teisiniuose santykiuose ir darbuotojų teisės į privatumą užtikrinimo, taip pat įvertinti, ar teisinis reguliavimas spėja vytis technologinę pažangą.

Darbo tikslas: Šio darbo tikslas yra literatūros, norminių aktų ir teismų praktikos pagrindu atskleisti, kokią įtaką modernios technologijos daro šiuolaikiniams darbo santykiams bei teisiniam reguliavimui ir ar yra galimybė, remiantis šiuo metu egzistuojančiu teisiniu reguliavimu, užtikrinti darbuotojų teisių ir darbdavio teisėtų interesų balansą.

Darbo uždaviniai: 1) atskleisti, kokios yra sąsajos tarp teisės į asmens duomenų apsaugą ir teisės į privatumo apsaugą; 2) nustatyti kokią įtaką darbo santykių subjektams daro šiuolaikinės darbo organizavimo formos ir darbo santykiuose naudojamos modernios technologijos; 3) aptarti, kaip turi būti tvarkomi duomenys susiję su darbuotojais, kad būtų užtikrinti darbdavio poreikiai ir darbuotojų teisė į privatų gyvenimą; 4) išanalizuoti kokia atsakomybė gali kilti darbo santykių šalims už teisės aktų pažeidimą, kai yra naudojamos modernios technologijos; 5) įvertinti, ar pakanka šiuo metu egzistuojančių teisės aktų, siekiant apsaugoti darbuotojų privatumą ir užtikrinti darbdavio teisėtus interesus, modernių technologijų kontekste.

Tyrimo objektas: Modernių technologijų naudojimas darbo santykių kontekste, užtikrinant darbuotojų privatumo apsaugą ir darbdavio teisėtus interesus.

Tyrimo metodai: 1) Lyginamasis – Bendrojo duomenų apsaugos reglamento nuostatos ir nacionaliniai teisės aktai, aktualūs magistro darbo temai, lyginami su tam tikrų Europos Sąjungos valstybių nacionalinėmis nuostatomis, teismų formuojama praktika; 2) aprašomasis – siekiama išsamiai atskleisti esamą teisinį reguliavimą, egzistuojančią teismų praktiką, susijusią su darbuotojų privatumo apsauga; 3) teleologinis – taikytas, tiriant modernių technologijų naudojimo darbo vietoje teisinio reguliavimo tikslingumą; 4) sisteminis – naudojamas siekiant išanalizuoti Lietuvos Respublikos, kitų Europos Sąjungos valstybių teisės aktų nuostatas, susijusias su privatumo apsauga ir analizuojant privatumo apsaugą kaip dalį platesnės duomenų apsaugos sistemos, nagrinėjant jos sąveiką su darbo teise, asmens duomenų apsaugos teise ir kitomis teisės šakomis; 5) lingvistinis – darbe yra detaliai analizuojama darbo vietos, privatumo, teisės į privatumą samprata, kiti apibrėžimai, taip pat aiškinamas teisės aktų turinys.

Darbo originalumas: Modernios technologijos keičia darbo santykių turinį, atsiranda vis naujų būdų, kuriais galima vykdyti darbuotojų stebėjimą, tačiau aktyvus technologijų panaudojimas kelia iššūkius darbuotojų privatumui. Šis magistro darbas lyginant su A. Anisimenkos, R. Grigonienės, A. Komanovisc, I. Breskienės ir kitais rašto darbais, išsiskiria tuo, kad jame yra plačiai analizuojama sąsaja tarp teisės į privatumą ir teisės į asmens duomenų apsaugą, išskiriamos konkrečios modernių technologijų rūšys ir pateikiami naujausi teismų praktikos pavyzdžiai, susiję su privatumo apsauga modernių technologijų kontekste. Taip pat darbe aptariami naujausi teisės aktai ir teisės aktų projektai, kurie ateityje gali teigiamai paveikti darbo santykių šalis ir apginti darbuotojų teises, o būtent – teisę į privatumą.

Svarbiausi šaltiniai: Magistro darbui parengti analizuojami nacionaliniai teisės šaltiniai, tokie kaip Lietuvos Respublikos darbo kodeksas, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas, Lietuvos Respublikos Konstitucinio Teismo doktrina, taip pat tarptautiniai teisės šaltiniai – Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija, Bendrasis duomenų apsaugos reglamentas, Europos Žmogaus Teisių Teismo sprendimai. Taip pat remtasi I. Petraitytės, G. Tamašauskaitės-Janickės, R. Grigonienės, T. Bagdanskio, P. Sartatavičiaus ir kitų autorių darbais.

1. PRIVATUMO SAMPRATA IR JO RIBOS

1.1. Teisės į privatų gyvenimą sąvoka

Apibūdinant privatumą yra vartojamos skirtingos apibrėžtys, tad aktualu atkreipti dėmesį į tai, jog nacionalinės ir tarptautinės teisės terminijose yra sinonimiškai vartojamos skirtingos sąvokos apibrėžiančios asmens privatumą. Galima aptikti tokių apibrėžčių, kaip teisė į privatų gyvenimą, teisė į privatumą, teisė į privataus gyvenimo gerbimą, teisė į privatumo gerbimą, teisė į privataus ir šeimos gyvenimo gerbimą ir taip toliau (Tamašauskaitė-Janickė, 2016, p. 71), todėl yra būtina išnagrinėti privatumo teisės sampratą plačiau.

Lietuvių kalbos žodyne yra pateikiamos kelios žodžio "privatus" reikšmės: priklausantis atskiram asmeniui, nuosavas, netarnybinis, neoficialus (Lietuvių kalbos išteklių informacinė sistema, 2025). Sąvoka privatus kildinama iš lotyniško žodžio *privatus,* reiškiančio atskiras, priklausantis sau pačiam (ne valstybei), asmeninis ir vartojamas kaip visuomeninis, bendras *(publicus, communis)* antonimas **(**Online Etymology Dictionary). "Privatumas" įvardija asmens teisės objektą, o būtent gėrį, kurį saugo teisė. Teisė į privatumą reiškia asmens subjektyvią teisę tą gėrį apsaugoti ir šios teisės turinį (Zaleskis, 2019, p. 38).

Svarbu aptarti ir tai, kokią privatumo sampratą formuoja nacionaliniai ir tarptautiniai teismai. Lietuvos Respublikos Konstitucinis Teismas (toliau – Konstitucinis Teismas) sieja tai su asmeninio, šeimos, namų gyvenimo, asmens fizinės ir psichinės neliečiamybės, garbės ir reputacijos, asmeninių faktų slaptumo, draudimo skelbti gautą ar surinktą konfidencialią informaciją, apsauga (Lietuvos Respublikos Konstitucinio Teismo 2000 m. gegužės 8 d. nutarimas). Konstitucinio Teismo 2004 metų nutarime teigiama, jog privatus žmogaus gyvenimas – tai individo asmeninis gyvenimas: gyvenimo būdas, šeimyninė padėtis, gyvenamoji aplinka, santykiai su kitais žmonėmis, individo pažiūros, įsitikinimai, įpročiai, jo fizinė bei psichinė būklė, sveikata, garbė, orumas ir kita (Lietuvos Respublikos Konstitucinio Teismo 2004 m. gruodžio 29 d. nutarimas).

Šiam darbui aktuali yra ir Europos Žmogaus Teisių Teismo (toliau – Žmogaus Teisių Teismas) byla Niemetz prieš Vokietiją, kurioje buvo sprendžiama ar krata advokato kontoroje patenka į "privataus gyvenimo" ir "namų" apsaugos sritį, kurią garantuoja Europos Žmogaus teisių ir pagrindinių laisvių konvencijos (toliau – Žmogaus teisių konvencija) 8 straipsnis. Teismas pabrėžė, jog "privatus gyvenimas" yra plati sąvoka

apimanti ir teisę užmegzti, plėtoti santykius su kitais asmenimis, taip pat buvo pasisakyta, jog nėra priežasties plačiai suvokiant privataus gyvenimo sąvoką atmesti profesinio ar verslo pobūdžio veiklą (Niemetz v. Germany, 1992). Plačiau apie teisės į privatumą apsaugą profesinės veiklos kontekste bus kalbama kitose šio darbo dalyse.

T. Davulio teigimu teisė į privatų gyvenimą – pasyvioji teisė, nes asmuo negali jos įgyvendinti savo paties elgesiu, tačiau turi teisę reikalauti, kad kiti asmenys veiktų atitinkamu būdu (Davulis, 2018, p. 115). L. Meškauskaitės nuomone, naudojimasis teise į privatų gyvenimą yra siejamas su konkretaus asmens asmenine nuožiūra, tai reiškia, jog tik nuo asmens priklauso jo privataus gyvenimo apsaugos ribos, tiksliau tai, kokiose ribose jis pageidauja būti paliktas vienas, todėl yra sunku apibrėžti vieną bendrą ir visiems tinkamą privatumo sąvoką (Meškauskaitė, 2004, p. 235). Literatūroje taip pat galima aptikti mintį, kad teisė į asmens privataus gyvenimo gerbimą teisės aktuose įvardijama gana abstrakčiai, lakoniškai, todėl jos turinio plėtojimas turi būti paliekamas teismų praktikai **(**Čilinskas, Jočienė, 2004, p. 71).

Tad galima daryti išvadą, jog visiems priimtinos privatumo sąvokos neegzistuoja, ji yra gana subjektyvi, todėl turi būti aiškinama skirtingai, atsižvelgiant į kiekvieną konkretų atvejį (Meškauskaitė, Lankauskas, 2016, p. 73). Svarbiausia yra tai, kad asmens privatus gyvenimas yra ginamas teisės normomis.

1.2. Teisės į privatų gyvenimą raida

Teisė į privatumą yra viena iš pamatinių žmogaus teisių, kylanti iš senovės laikų. Graikų mąstytojas Platonas manė, jog įstatymas turėtų apimti ne tik viešą, bet ir privatų gyvenimą, nes be sutvarkyto privataus gyvenimo visuomenės santvarka nėra įmanoma (Leonas, 2005, p. 143.). Tačiau vyrauja nuomonė, jog teisės į privatumą doktrina buvo suformuluota 19 amžiaus pabaigoje, teisininkų S. Warren ir L. D. Brandeis paskelbtame darbe, kurį parašyti juos paskatino tų laikų technologinė pažanga. Mokslininkai privatumą suvokė kaip teisę būti paliktam vienu ir apsaugotam nuo individo asmeninio gyvenimo detalių atskleidimo be jo sutikimo (Žiobienė, 2002, p. 34.). Teisė į privatų gyvenimą buvo pripažinta asmenine neturtine teise 19 amžiaus pabaigoje – 20 amžiaus pradžioje, o tam tikrose valstybėse dar vėliau (Mikelėnas, 2001, p. 54.).

Svarbu aptarti teisės į privatumą istorines ištakas. 1948 metais priimtos Visuotinės žmogaus teisių deklaracijos (toliau – Žmogaus teisių deklaracija) 12 straipsnyje numatyta, kad niekas neturi patirti savavališko kišimosi į jo privatumą, šeimos gyvenimą, buitį ar

susirašinėjimą arba kėsinimosi į garbę ir reputaciją (Visuotinė žmogaus teisių deklaracija, 1948). 1950 metais buvo pasirašyta Žmogaus teisių konvencija, kurios 8 straipsnyje įtvirtinta, jog kiekvienas turi teisę į jo asmeninio ir šeimos gyvenimo gerbimą, buto neliečiamybę ir susirašinėjimo slaptumą ir kištis į naudojimąsi šia teise galima tik tada, kai tai numatyta įstatyme ir yra būtina demokratinėje visuomenėje apsaugant vertybes, kurios gali būti pažeistos (Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija, 1950). Teisė į privatumą yra saugoma ir 1966 metų Jungtinių Tautų tarptautiniu pilietinių ir politinių teisių paktu (Tarptautinis pilietinių ir politinių teisių paktas, 1966).

Nacionalinėje teisėje reguliavimas, apimantis asmens teisę į privatumą, yra įtvirtintas tiek privatinės, tiek ir viešosios teisės normose. 1990 metais priimtame Lietuvos Respublikos Laikinajame Pagrindiniame įstatyme – 35 straipsnyje, buvo numatyta, jog piliečių asmeninį gyvenimą saugo įstatymas (Petraitytė, 2011, p.126), o vėliau įsigaliojusios Lietuvos Respublikos Konstitucijos (toliau – Konstitucija) 22 straipsnyje yra numatyta, jog žmogaus privatus gyvenimas yra neliečiamas, asmens susirašinėjimas, pokalbiai telefonu, telegrafo pranešimai ir kitoks susižinojimas neliečiami, o informacija apie asmens privatų gyvenimą gali būti renkama tik teismo sprendimu ir tik pagal įstatymą. Yra saugoma, kad niekas nepatirtų savavališko ar neteisėto kišimosi į jo asmeninį ir šeimyninį gyvenimą, kėsinimosi į jo garbę ir orumą (Lietuvos Respublikos Konstitucija, 1992). 1999 metų liepos mėnesį Europos Vadovų Taryba nutarė, kad Europos Sąjungos lygmeniu taikomos pagrindinės teisės turėtų būti įtvirtintos chartijoje. Europos Sąjungos pagrindinių teisių chartija (toliau – Chartija) (Europos Sąjungos pagrindinių teisių chartija, 2009) 2000 metais buvo paskelbta, o 2009 metais, įsigaliojus Lisabonos sutarčiai, tapo teisiškai privaloma ir lygi Europos Sąjungos sutartims. Chartijos 7 straipsnyje yra numatyta teisė į privatų ir šeimos gyvenimą.

Privataus gyvenimo apsauga taip pat yra įtvirtinta Lietuvos Respublikos civiliniame kodekse (toliau – Civilinis kodeksas) (Lietuvos Respublikos civilinis kodeksas, 2000), Lietuvos Respublikos darbo kodekse (toliau – Darbo kodeksas) (Lietuvos Respublikos darbo kodeksas, 2016), atsakomybė už pažeidimus numatyta Lietuvos Respublikos baudžiamajame kodekse (toliau – Baudžiamasis kodeksas) (Lietuvos Respublikos baudžiamasis kodeksas, 2000), Lietuvos Respublikos administracinių nusižengimų kodekse (toliau – Administracinių nusižengimų kodeksas) (Lietuvos Respublikos administracinių nusižengimų kodeksas, 2015) ir kituose teisės aktuose.

Teisė į privatų gyvenimą yra fundamentali žmogaus teisė, kuri nuolat evoliucionavo ir buvo įtvirtinta skirtinguose teisės aktuose. Šios teisės apsauga yra numatyta ir

Konstitucijoje, o tai leidžia teigti, jog teisė į privatumą yra viena iš esminių demokratinės visuomenės vertybių.

1.3. Teisės į privatų gyvenimą ir teisės į asmens duomenų apsaugą santykis

Apibrėžti asmens teisę į privatumą yra pakankamai sunku. I. Petraitytė išsako poziciją, jog informacija apie asmenį ir tokios informacijos apsauga yra sudedamoji teisės į asmens privatų gyvenimą dalis (Petraitytė, 2011, p.74), tačiau svarbu išsiaiškinti, ar toks požiūris, kuriuo privatumas suvokiamas kaip asmeninės informacijos valdymas, per daug nesutapatina šios vienos iš pagrindinių žmogaus teisių su teise į asmens duomenų apsaugą, tad svarbu aptarti šių dviejų institutų santykį.

Teisė į privatumą ir teisė į asmens duomenų apsaugą yra glaudžiai susijusios, tačiau skirtingos teisės. Kaip jau buvo minėta šiame darbe, teisė į privatumą, tarptautinėje žmogaus teisių teisėje, kaip viena iš pagrindinių saugomų vertybių, atsirado priėmus Žmogaus teisių deklaraciją, o vėliau patvirtinus Žmogaus teisių konvenciją. Tuo tarpu, pasaulyje vyko pokyčiai susiję su modernių technologijų atsiradimu ir tai pradėjo kelti pavojų teisei į privatų gyvenimą, tad atsirado nauja privatumo koncepcija, kuri lėmė tai, jog buvo sukurti specialūs teisiniai reglamentai. 1970 metais Vokietijos Heseno žemė priėmė pirmąjį įstatymą dėl duomenų apsaugos, 1973 metais Švedija priėmė pirmąjį pasaulyje nacionalinį duomenų apsaugos įstatymą, 20 amžiaus 9–ojo dešimtmečio pabaigoje keletas Europos valstybių taip pat priėmė įstatymus nustatančius asmens duomenų apsaugą. 1981 metais buvo priimta Europos Tarybos Konvencija „Dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu" (toliau – 108–oji Konvencija), o ilgainiui susiformavo atskiras institutas, nepriskiriamas teisei į privatumą (Europos duomenų apsaugos teisės vadovas, 2018, p. 20-21). Pažymėtina, kad Chartijos 8 straipsnyje yra įtvirtinta teisė į asmens duomenų apsaugą, o Žmogaus teisių konvencijoje teisė į asmens duomenų apsaugą apima teisę į šeimos ir privataus gyvenimo gerbimą (Europos Sąjungos pagrindinių teisių chartijos..., 2019, p. 217). Santykį tarp šių dviejų teisių gerai apibūdina E. Sharpston, kuri pateikia mintį, jog privatumo apsauga pagal Žmogaus teisių konvencijos 8 straipsnį yra klasikinė teisė, o duomenų apsauga pagal 108–ąją Konvenciją – modernesnė teisė, tad šios teisės yra skirtingos, tačiau Teisingumo Teismas yra nurodęs, jog tarp jų yra glaudus ryšys (Opinion of Advocate General Sharpston…, 2010).

20 amžiaus pabaigoje, Lietuvos Respublikoje, buvo pradėtas kurti teisinis reguliavimas, kuris buvo skirtas informacijos apie fizinius asmenis tvarkymui, o būtent 1996 metais įsigaliojo Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas (toliau – Asmens duomenų teisinės apsaugos įstatymas) (Lietuvos Respublikos asmens duomenų teisinės…, 1996 m. redakcija), kurio tikslas buvo nustatyti duomenų subjektų teises ir šių teisių apsaugos tvarką, teisių į duomenis bei duomenų apsaugos garantijas tvarkant asmens duomenis informacinėse sistemose. Pagal šį įstatymą buvo reikalingas asmens sutikimas, kad informacija būtų tvarkoma ir platinama, o jos sunaikinimas buvo galimas tik gavus Lietuvos archyvų departamento ir Valstybinės duomenų apsaugos inspekcijos (toliau – Duomenų apsaugos inspekcija) leidimą. Modernių technologijų sklaida lėmė tai, jog buvo pradėta tvarkyti vis gausesnė ir įvairesnė informacija ir informaciją apie fizinius asmenis informacinėse sistemose pradėjo tvarkyti ne tik valstybė, bet ir privatūs asmenys. Turimų taisyklių nepakako, tad 1998 metais įsiteisėjo minėto įstatymo pataisos, kuriomis buvo išplėsta įstatymo taikymo sritis – jis tapo taikomas ne tik valstybės, bet ir kitose informacinėse sistemose tvarkomai fizinių asmenų informacijai, taip pat buvo supaprastintos duomenų tvarkymo sąlygos, o būtent, nustatyti atvejai, kai informacija gali būti platinama be asmens sutikimo ir išplėstas informacijos tvarkymo pagrindų sąrašas. 2001 metais įsigaliojo nauja Asmens duomenų teisinės apsaugos įstatymo redakcija. Šio teisės akto naujoje redakcijoje nacionalinis teisinis reguliavimas buvo suderintas su 1995 metų spalio 24 dienos Europos Parlamento ir Tarybos direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo. Įstatymo apsaugos sritis buvo išplėsta, priskiriant kiekvieną su fiziniu asmeniu, kurio tapatybė yra žinoma ar gali būti nustatyta, susijusią informaciją, apimant duomenis, kurie tvarkomi automatiniu būdu arba kurių susistemintos rinkmenos tvarkomos neautomatiniu būdu, taip pat įstatyme buvo numatyti teisėti asmens duomenų tvarkymo pagrindai, duomenų subjektų – asmenų, kurių duomenys yra tvarkomi teisės ir duomenų valdytojų – fizinio arba juridinio asmens, valdžios institucijos, agentūros ar kitos įstaigos, kuris vienas ar drauge su kitais nustato duomenų tvarkymo tikslus ir priemones, pareigos (Petraitytė, 2011, p.128-129). Svarbu paminėti, kad egzistuoja ir kitas asmuo, kuris gali užsiimti veikla duomenų valdytojo vardu, toks asmuo yra vadinamas duomenų tvarkytoju (Kas yra duomenų valdytojas ir…). Šios naujos redakcijos įstatymo tikslas – ginti žmogaus privataus gyvenimo neliečiamumo teisę ryšium su asmens duomenų tvarkymu ir sudaryti sąlygas laisvam asmens duomenų judėjimui (Lietuvos Respublikos asmens duomenų teisinės…, 2001 m. redakcija).

Asmens duomenys yra bet kokia informacija, susijusi su asmeniu, kurio tapatybė nustatyta ar gali būti nustatyta. Asmuo, kurio tapatybė gali būti nustatyta, yra bet kuris asmuo, kuris gali būti tiesiogiai ar netiesiogiai identifikuojamas. Asmens duomenimis gali būti laikoma ir įvairi informacija, kurią sudėjus būtų galima nustatyti konkretaus asmens tapatybę (Europos duomenų apsaugos valdyba, 2024). Asmens duomenų apibrėžimas akcentuoja du kriterijus – tiesioginį ir netiesioginį asmens tapatybės nustatymą, o tai leidžia apimti daug duomenų, kurie, *prima facie,* turi labai menką ryšį su konkrečiu asmeniu, tačiau apjungus duomenis su pagalbiniais, asmuo gali būti identifikuotas, todėl tokie duomenys gali būti laikomi asmeniniais (Civilka, 2002). Pabrėžtina, kad sąvoka „informacija“ apima garso, vaizdo, biometrinius, genetinius duomenis ir gali būti pateikiama raidėmis, skaičiais, garsu, grafiniu, fotografiniu vaizdu ir kitomis formomis (Gairės viešojo sektoriaus institucijoms..., 2023, p. 22). Taisyklės, susijusios su fizinių asmenų apsauga tvarkant jų duomenis ir su laisvu tokių duomenų judėjimu yra apibrėžtos Europos Parlamento ir Tarybos reglamente (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, kuriuo panaikinama Direktyva 95/46/EB (toliau – Bendrasis duomenų apsaugos reglamentas). Ketvirtoje šio Reglamento konstatuojamojoje dalyje numatyta, jog juo yra paisoma visų Chartijoje pripažintų ir Sutartyse įtvirtintų pagrindinių teisių ir laisvių bei principų, tarp jų – teisės į privatų ir šeimos gyvenimą.

Teisės doktrinoje įprastai privatumas analizuojamas kaip plati kategorija, apimanti keturis tarpusavyje susijusius elementus:

1. kūno privatumas – asmens fizinė apsauga;
2. teritorinis privatumas – asmens namų, darbo ir kitų erdvių apsauga;
3. informacinis privatumas – informacijos apie asmenį apsauga;
4. komunikacinis privatumas – asmens pašto, telefono, elektroninio pašto ir kitokių komunikacijos priemonių apsauga (Zaleskis, 2019, p. 40-41).

Taip pat yra pateikiamos privatumo apibrėžtys informacinių ir ryšių technologijų kontekste. Literatūroje galime rasti tokių apibūdinimų: privatumas yra asmeninės informacijos apsauga nuo nesąžiningų subjektų piktnaudžiavimo ir leidimas tam tikriems įgaliotiems subjektams naudotis ta asmenine informacija, privatumas – privatumo politikų rinkinys, verčiantis sistemą saugoti privačią informaciją. Kalbant apie privatumą informacinių ryšių ir technologijų kontekste, taip pat yra sutinkama su jau anksčiau šiame darbe pateikta mintimi, jog vieningos privatumo apibrėžties nėra, tačiau labiau jis yra siejamas su informaciniu privatumu (Aldhafferi, Watson, Sajeev, 2013, p. 2).

Ilona Petraitytė, kaip ir daugelis užsienio mokslininkų teigia, jog šios dvi teisės yra glaudžiai susijusios. Jos manymu asmens duomenų apsaugos teisinės nuostatos turinio prasme skirtos asmens privatumui užtikrinti, remiantis teisės į privatų gyvenimą garantija, asmens duomenų teisinė apsauga gali būti reguliuojama tik tokia apimtimi, kiek tai reikalinga asmens informaciniam privatumui apsaugoti (Petraitytė, 2013, p.). Terminą „duomenų apsauga“ reikėtų suvokti taip, jog juo yra siekiama apsaugoti žmones ir, kad duomenys gali tiesiogiai ir netiesiogiai atskleisti asmens privataus gyvenimo aspektus, kurie suteiks pagrindą diskriminacijai ir būtent teisė į privatumą suteikia apsaugą nuo duomenų atskleidimo ir užkerta kelią bet kokiai diskriminacijai (Wachter, Mittelstadt, 2019, p. 82).

1.4. Asmens duomenų apsaugos teisiniai pagrindai

Didelis kiekis duomenų gali neturėti tiesioginės sąsajos su konkrečiu asmeniu, tačiau sujungus turimus duomenis su papildoma informacija, gali būti nustatyta asmens tapatybė (Europos duomenų apsaugos valdyba, 2024), todėl Bendrajame duomenų apsaugos reglamente yra numatytas mechanizmas, kuriuo užkertamas kelias neteisėtam duomenų tvarkymui, taip garantuojant asmenų, su kuriais yra susiję duomenys, teises, tarp jų ir teisę į privatumą.

Bendruoju duomenų apsaugos reglamentu yra paisoma visų Chartijoje pripažintų ir Sutartyse įtvirtintų pagrindinių teisių ir laisvių bei principų, tad duomenų tvarkymas turi vykti užtikrinant teisę į privatų gyvenimą, duomenų saugumą. Bendrojo duomenų apsaugos reglamento 6 straipsnyje yra numatyti teisiniai pagrindai, kurių laikantis yra užtikrinamas duomenų tvarkymo teisėtumas. Jeigu taikomas bent vienas iš jų, ir tik tokiu mastu, kokiu jis yra taikomas, asmens duomenų tvarkymas yra teisėtas.

Pirmasis pagrindas – sutikimas. Duomenų subjektas turi duoti sutikimą, kad jo asmeniniai duomenys būtų tvarkomi vienu ar keliais konkrečiais tikslais. 29 straipsnio darbo grupės darbiniame dokumente yra pastebima, jog kalbant apie sutikimą darbo santykių kontekste yra sunku nustatyti ar jis yra duotas laisva valia, nes tokiam duomenų subjekto sprendimui įtakos gali turėti tai, jog jis yra silpnesnioji darbo santykių šalis, todėl vertinant sutikimo galiojimą reikia atsižvelgti į aplinkybių visumą – ar sutikimas buvo duotas laisva valia, ar darbuotojas buvo tikras, kad jei jis neduos sutikimo, nebus patirtos neigiamos pasekmės, sutikimas turi būti konkretus, pagrįstas informacija, o valios išreiškimas – nedviprasmiškas, tik tada galima spręsti ar sutikimas yra tinkamas teisinis

pagrindas (Gairės 05/2020 dėl sutikimo pagal...2020, p. 7). Dažniausiai sutikimu galima remtis tais atvejais, kai siekiama tvarkyti duomenis apie asmenį, susijusius ne su jo funkcijų vykdymu, pavyzdžiui, fiksuojant darbuotojo atvaizdą vidiniuose renginiuose, informuojant šeimos narį apie darbo metu įvykusį incidentą (Gairės smulkiajam ir vidutiniam verslui, 2023, p. 9). Europos duomenų apsaugos valdyba gairėse 05/2020 dėl sutikimo pagal Reglamentą 2016/679, yra nurodžiusi, kad prašymas duoti sutikimą turi būti pateiktas suprantama kalba ir lengvai prieinama forma, kad kiekvienas duomenų subjektas, suprastų duomenų tvarkymo tikslus (Gairės 05/2020 dėl sutikimo pagal..., 2020, p. 16).

Antrasis pagrindas yra sutartis. Šis pagrindas gali būti pritaikytas tik tada, kai tenkinama bent viena iš dviejų sąlygų – yra būtina tvarkyti duomenis siekiant įvykdyti sutartį, kurios šalis yra duomenų subjektas, arba siekiant atlikti veiksmus, kurių duomenų subjektas prašo, prieš sudarant sutartį. Kiti teisiniai pagrindai aptariami straipsnyje – teisinė prievolė, viešojo intereso labui vykdoma užduotis arba pavestų viešųjų valdžios funkcijų vykdymas, šios dvi sąlygos yra panašios, nes abi jos kyla iš teisės aktų. Siekiant remtis teisine prievole, konkrečiame teisės akte turi būti aiškiai nustatyta pareiga tvarkyti asmens duomenis, tuo tarpu Bendrojo duomenų apsaugos reglamento 6 straipsnio 1 dalies e punkte numatytas pagrindas yra taikomas tada, kai teisės aktai nustato ne aiškią pareigą tvarkyti asmens duomenis, bet tik tam tikras funkcijas, įgaliojimus, paliekant teisę duomenų valdytojui nuspręsti, ar asmens duomenys būtini kiekvienu atskiru atveju (Gairės viešojo sektoriaus institucijoms ir…, 2023, p. 10). Asmens duomenų tvarkymas turėtų būti laikomas teisėtu, kai jis būtinas norint apsaugoti gyvybinius duomenų subjekto ar kito fizinio asmens interesus. Duomenų tvarkymas remiantis kito fizinio asmens gyvybiniu interesu turėtų būti vykdomas tik tada, kai tvarkymas akivaizdžiai negali būti grindžiamas kitu teisiniu pagrindu (Bendrasis duomenų apsaugos reglamentas, 46 konstatuojamoji dalis). Paskutinis teisinis pagrindas, numatytas Bendrojo duomenų apsaugos reglamento 6 straipsnyje, yra teisėtas interesas. Šio straipsnio f punkte – rašoma, jog tvarkyti duomenis būtina siekiant teisėtų duomenų valdytojo arba trečiosios šalies interesų, išskyrus atvejus, kai tokie duomenų subjekto interesai arba pagrindinės teisės ir laisvės, dėl kurių būtina užtikrinti asmens duomenų apsaugą, yra už juos viršesni. Atkreiptinas dėmesys, kad šiame straipsnyje nurodytas teisinių pagrindų eiliškumas neturi įtakos jų svarbai. Europos ir nacionalinės priežiūros institucijos nurodė, kad kiekvienas duomenų tvarkymo atvejis turi būti grindžiamas tuo teisiniu pagrindu, kuris konkrečiu atveju yra tinkamiausias, atsižvelgiant į aplinkybes (Data Protection Comission, 2019, p. 2).

Tad galima teigti, jog teisė į asmens duomenų apsaugą atsirado vystantis asmens teisės į privatų gyvenimą doktrinos raidai, kai teisės į privatumą nebepakako apginti asmenų teisių, vykstant technologinei evoliucijai, ši teisė tapo savarankiška, tačiau vis dar glaudžiai susijusi su teise į privatumą. Kaip teigia Ilona Petraitytė – visa privati informacija yra laikoma asmens duomenimis, tačiau ne visi asmens duomenys laikytini privačia informacija (Petraitytė, 2013, p. 57). Ši mintis tik patvirtina šių dviejų institutų sunkų atskiriamumą ir būtinumą kiekvienu atveju užtikrinti teisėtą bet kokių duomenų tvarkymą, kad būtų užkirstas kelias asmens teisės į privatumą pažeidimui.

1.5. Elektroninių ryšių privatumo reguliavimas: direktyvos vaidmuo

Europos Sąjungos teisė turi apsaugoti pagrindinę teisę į privatumą ir ryšių konfidencialumą, tai yra numatyta Chartijos 7 straipsnyje, o Bendruoju duomenų apsaugos reglamentu yra įgyvendinamas Chartijos 8 straipsnis, nustatomos taisyklės, kuriomis siekiama užtikrinti teisėtą, sąžiningą ir skaidrų duomenų tvarkymą, tačiau minėto reglamento tikslas nėra apsaugoti teisę į ryšių konfidencialumą, todėl teisės į privatumo apsaugą įgyvendinimas nėra detalizuotas (Markevičius, 2019, p. 143). Reikšminga yra aptarti teisės aktą, kurio nuostatos laikytinos papildančiomis Bendrojo duomenų apsaugos reglamento reguliavimą ir nustatančios papildomą elektroninių ryšių paslaugų naudotojų apsaugą.

Šiam darbui yra svarbi Europos Parlamento ir Tarybos 2002 metų liepos 12 dienos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (toliau – Direktyva dėl privatumo ir elektroninių ryšių). Direktyva nustatomos taisyklės, kuriomis užtikrinamas asmens duomenų tvarkymo saugumas, pranešimas apie pažeidimus susijusius su asmens duomenų saugumu ir pranešimų konfidencialumas, ja taip pat draudžiami neužsakyti pranešimai, kai naudotojas neduoda savo sutikimo (Duomenų apsauga elektroninių ryšių sektoriuje, 2020). Direktyvos 1 straipsnio 2 dalyje yra numatyta, kad šio teisės akto nuostatos detaliau išaiškina ir papildo Direktyvą dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, kurią pakeitė šiuo metu galiojantis Bendrasis duomenų apsaugos reglamentas, šio straipsnio 1 dalyje nurodytais tikslais, o būtent valstybių narių nuostatų, užtikrinančių vienodo lygio pagrindinių teisių ir laisvių, ypač teisės į privatumą ir konfidencialumą apsaugą susijusių su asmens duomenų tvarkymu elektroninių ryšių sektoriuje, ir užtikrinančių laisvą tokių duomenų judėjimą ir laisvą elektroninių ryšių įrangos ir paslaugų

judėjimą Bendrijoje, suderinimu. Šios direktyvos 5 straipsnio 3 dalyje rašoma, kad valstybės narės užtikrina, kad saugoti informaciją arba suteikti galimybę naudotis jau saugoma informacija abonento ar naudotojo galiniame įrenginyje būtų leidžiama tik su sąlyga, jei atitinkamam abonentui ar naudotojui sutikus pagal Direktyvą dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo pateikiama aiški ir išsami informacija, *inter alia*, apie tokio duomenų tvarkymo tikslus. Šios nuostatos laikytinos papildančiomis Bendrojo duomenų apsaugos reglamento reguliavimą ir nustatančios papildomą elektroninių ryšių paslaugų naudotojų apsaugą, palyginti su Bendruoju duomenų apsaugos reglamentu (Markevičius, 2019, p. 143).

Šiuo metu galiojančioje direktyvoje nėra atsižvelgiama į technologinę plėtrą, nes teisės aktas neapima internetinių asmenų tarpusavio ryšio paslaugų (pavyzdžiui, interneto telefonijos, tikralaikių pokalbių ir internetinių elektroninio pašto paslaugų) (Markevičius, 2019, p. 141), todėl 2017 metais Europos Komisija priėmė pasiūlymą dėl E. privatumo reglamento. Pagrindiniai pasiūlymo aspektai yra šie:

1. Privatumo taisyklių taikymas naujiems teikėjams, tokiems kaip „WhatsApp“, „Facebook Messenger“, tai užtikrins, kad populiariosios šiuolaikinės platformos garantuotų tokį patį ryšių konfidencialumo lygį kaip ir tradiciniai telekomunikacijų operatoriai.
2. Tiesiogiai taikomu reglamentu numatomos griežtesnės taisyklės, visiems Europos Sąjungos piliečiams ir įmonėms bus taikoma vienoda jų elektroninių ryšių apsauga, naudingas bendras taisyklių rinkinys visoje Europos Sąjungoje.
3. Garantuojamas ryšių turinio ir metaduomenų privatumas. Metaduomenys – duomenys, apibūdinantys kitus duomenis, pavyzdžiui, autorius, sukurta data ir vieta – turi aukštą privatumo komponentą ir turėtų būti nuasmeninti arba ištrinti, jeigu nėra duotas naudotojų sutikimas.
4. Naujos verslo galimybės.
5. Paprastesnės taisyklės dėl slapukų.
6. Apsauga nuo brukalų, draudžiami nepageidaujami elektroniniai ryšiai elektroninių paštu, žinutėmis ir automatinėmis skambinimo mašinomis.
7. Už Reglamente nustatytų konfidencialumo taisyklių vykdymą bus atsakingos institucijos, jau atsakingos už Bendrojo duomenų apsaugos reglamento nustatytas taisykles (Proposal for an ePrivacy regulation, 2017).

Apibendrinant galima teigti, kad Direktyva dėl privatumo ir elektroninių ryšių nustato pagrindinius principus, kurie yra taikomi elektroninių ryšių privatumo

užtikrinimui, kartu su Bendruoju duomenų apsaugos reglamentu. Darbo santykių kontekste, tai apima darbuotojų stebėseną, komunikacijos apsaugą, teisėtą ir skaidrų asmens duomenų tvarkymą, užtikrinant pagrindinių teisių apsaugą, tačiau galiojanti Direktyva nėra pakankama, atsižvelgiant į naujų technologijų panaudojimą darbo santykiuose, todėl sukūrus atskirą reglamentą dėl privatumo ir elektroninių ryšių, būtų užtikrintas teisinis aiškumas ir nuoseklumas, o tokio reglamento tiesioginis taikymas kartu su Bendruoju duomenų apsaugos reglamentu sustiprintų darbuotojų teisės į privatumą apsaugą.

2. DARBO VIETOS SAMPRATA MODERNIŲ TECHNOLOGIJŲ ASPEKTU

Šiuolaikinės technologijos ir jų taikymas darbo santykiuose transformuoja ne tik įprastą darbo teisės subjektų komunikaciją, bet ir daro įtaką darbo funkcijų atlikimui. Modernių technologijų naudojimas darbo vietoje didina darbo efektyvumą, tačiau vis labiau panaikina ribas tarp profesinio ir privataus gyvenimo. Iškyla daug klausimų susijusių tiek su pačia darbo vietos samprata, tiek ir su darbuotojų teisių užtikrinimu vykdant jų stebėseną ir sekimą pasitelkiant naujausias technologijas, tad šioje dalyje bus kalbama apie darbo vietos sampratą, dažniausiai darbo santykiuose naudojamas technologijas bei egzistuojantį teisinį reguliavimą.

2.1. Darbo vietos samprata

Darbuotojas yra silpnesnioji darbo santykių šalis, kadangi darbo santykių įforminimas, darbo sutarčių sudarymas, taisyklių nustatymas ir kitų procesų organizavimas priklauso darbdavio diskrecijai (Grigonienė, 2020, p. 347). Tačiau nepriklausomai nuo to, kaip darbo santykiuose yra vertinamas darbuotojo statusas, darbdavys privalo užtikrinti, kad darbo vietoje nebūtų pažeidžiama darbuotojo, kaip fizinio asmens, teisė į privatumą.

Bendrajame duomenų apsaugos reglamente numatomos kelios pavienės su darbuotojų duomenų apsauga susijusios nuostatos. Europos Sąjungos valstybėms narėms leidžiama numatyti specialias taisykles nacionalinėje teisėje. Lietuvos teisiniame reguliavime, siekiant darbuotojų privatumo ir duomenų apsaugos sustiprinimo, atsirado specialiųjų darbuotojų duomenų apsaugos reikalavimų, kurių tikslą atspindi Darbo kodekso 27 straipsnyje numatyta nuostata, kad darbdavys privalo gerbti darbuotojų teises į privatų gyvenimą, asmens duomenų apsaugą, darbdaviui įgyvendinant nuosavybės ar valdymo teises į darbo vietoje naudojamas informacines ir elektroninių ryšių technologijas, negali būti pažeidžiamas darbuotojų asmeninio susižinojimo slaptumas (Zaleskis, 2019, p. 254). Prieš tęsiant taisyklių, susijusių su darbuotojų teisės į privatumą apsauga, aptarimą ir konkrečių technologijų, naudojamų darbo teisiniuose santykiuose, analizę, reikėtų apibrėžti, kaip šiame darbe yra suvokiama sąvoka „darbo vieta“.

Žodynuose yra pateikiamos kelios darbo vietos sąvokos: Vieta, kurioje yra būtinos darbo priemonės ir kurioje gali dirbti darbuotojas ar jų grupė (Raupelienė, 2024, p. 15), nustatyta vieta arba vietos, kuriose vykdoma darbinė veikla (Ekspozicija darbo vietoje. Terminija, 2022). Lietuvos Respublikos darbuotojų saugos ir sveikatos įstatymo 2 straipsnio 8 dalyje yra nurodyta, jog darbo vieta – vieta, kurioje asmuo dirba darbo sutartyje sulygtą darbą arba atlieka viešojo administravimo funkcijas (Lietuvos Respublikos darbuotojų saugos ir sveikatos įstatymas, 2003), o Darbo kodeksas nenumato tikslaus darbo vietos apibrėžimo, tačiau analizuojant 30 straipsnio turinį, galima suprasti, jog įstatymų leidėjas darbo vietą suvokia kaip tiek viešą, tiek ir privačią vietą, kai darbuotojas yra darbdavio žinioje ar atlieka pareigas pagal darbo sutartį. Lietuvos Aukščiausiasis Teismas pasisakė, jog „darbo funkcijų atlikimo vieta“ priklausomai nuo darbo pobūdžio ir darbo organizavimo tvarkos, gali būti nenuolatinė ir tam tikru laikotarpiu skirtis tos pačios vietovės ribose. Sąvokos „darbo vieta“, „darbo funkcijų atlikimo vieta“ yra siejamos su adresu, kuriuo darbuotojas, vykdydamas darbovietės nurodymus, konkrečiu laikotarpiu atlieka pareigas ar vykdo funkcijas (Lietuvos Aukščiausiojo Teismo 2021 m. birželio 16 d. nutartis civilinėje byloje). Tad kalbant apie darbo vietą – kalbama apie tai, kur faktiškai darbuotojas atlieka savo darbo funkcijas.

Svarbu aptarti ir tokią darbo organizavimo formą, kaip nuotolinis darbas. Darbo kodekso 52 straipsnio 1 dalyje yra pateikiama nuotolinio darbo apibrėžtis: nuotolinis darbas – darbo organizavimo forma arba darbo atlikimo būdas, kai darbuotojas jam priskirtas darbo funkcijas ar jų dalį visą arba dalį darbo laiko su darbdaviu suderinta tvarka reguliariai atlieka nuotoliniu būdu, tai yra sulygtoje darbo sutarties šalims priimtinoje kitoje, negu yra darbovietė, vietoje, taip pat naudodamas informacines ir elektroninių ryšių technologijas (teledarbas). Šiame straipsnyje taip pat yra numatyta, jog asmenį skiriant dirbti nuotoliniu būdu, raštu turi būti nustatomi darbo vietos reikalavimai, tap pat darbui suteikiamos naudoti priemonės, aprūpinimo jomis tvarka, naudojimosi taisyklės, numatomas darbovietės padalinys, skyrius ar atsakingas asmuo, kuriam darbuotojas turi atsiskaityti už atliktus darbus, o savo darbo laiką darbuotojas gali skirstyti savo nuožiūra, nepažeidžiant maksimaliojo darbo laiko ir minimaliojo poilsio laiko reikalavimų. Paminėtina ir Lietuvos Aukščiausiojo Teismo byla, kurioje teisėjų kolegija išaiškino: Darbo kodekso 52 straipsnio 1, 3 – 5, 7 dalių nuostatos leidžia spręsti, kad nuotoliniam darbui būdingas ir kitas požymis, jog jis vyksta pagal nustatytą nuotolinio darbo tvarką. Nuotolinį darbą dirbantis darbuotojas nėra nuolatinėje darbdavio priežiūroje, todėl darbdaviui, pasirinkusiam taikyti tokią darbo organizavimo formą, tenka ir pareiga nustatyti tokio darbo organizavimo tvarką, kurioje,

be kita ko, turėtų būti aptariami visi tokio darbo organizavimo ypatumai, bendravimo su darbuotoju būdai ir (ar) taisyklės, darbo laiko apskaitos taisyklės, darbo vietai keliami reikalavimai, jeigu tokie būtini pagal darbo pobūdį, nustatoma suteikiamų darbo priemonių naudojimo tvarka, dėl tokio darbo patiriamų išlaidų kompensavimas ir panašiai (Lietuvos Aukščiausiojo Teismo 2024 m. spalio 8 d. nutartis civilinėje byloje).

Egzistuoja dar viena darbo organizavimo forma, kai darbas yra atliekamas tiek nuotoliniu būdu, tiek ir darbdavio suteiktose patalpose, tai yra vadinama mišriu darbu (Hybrid work: New opportunities and…, 2023, p. 1). Literatūroje galima aptikti darbo vietos pavyzdžių, kurie yra išskiriami kalbant apie mišraus darbo organizavimą, o būtent, darbuotojo gyvenamoji vieta, pagrindinė darbo vieta, tai yra, darbdavio suteikta darbo vieta, transporto priemonės, viešbučiai, kavinės, parkai (Vartiainen, 2007, p. 29), tačiau šis sąrašas nėra baigtinis, jis gali apimti ir kitas vietas. Pažymėtina, kad tokia darbo organizavimo forma kelia diskusijų, nes mišrus darbas apima darbo funkcijų atlikimą tiek darbdavio suteiktose patalpose, tiek ir nuotoliniu būdu, todėl esamo reguliavimo, kuris apima nuotolinio darbo organizavimą, nepakanka, o tai reiškia, jog turi būti nustatomos vidinės taisyklės darbovietėse, susitarimai tarp darbdavio ir darbuotojo, o efektyviausiai ir skaidriausiai veiktų teisinio reguliavimo nacionaliniu ar viršnacionaliniu lygmeniu sukūrimas, kuriame būtų atsižvelgta į darbo santykiams reikšmingus klausimus, įskaitant ir darbo bei asmeninio gyvenimo pusiausvyros užtikrinimą (Hybrid work in Europe: Concept…, 2023, p. 33).

Dirbti nuotoliniu būdu galima ir ne iš tos valstybės, kurioje yra įprasta darbo funkcijų atlikimo vieta, tačiau tai gali kelti tam tikrų iššūkių, o būtent, tais atvejais, kai yra dirbama nuotoliniu būdu būnant ne Europos ekonominės erdvės valstybėse, formaliai žiūrint, vyksta duomenų teikimas į trečiąsias šalis, kuris yra rizikingas, tad darbdavys turi įsitikinti, kad duomenų tvarkymas atitinka Bendrojo duomenų apsaugos reglamento nuostatas (Vasiliauskienė, 2022, p. 49), nes kartais informacija, kuri yra apdorojama darbuotojo, yra saugoma ne konkrečiame įrenginyje, o debesyse, todėl tokius duomenis galima pasiekti esant bet kurioje pasaulio vietoje, naudojant bet kokį įrenginį, turintį interneto ryšį (Kas yra debesies sauga, 2025). Ne visos pasaulio valstybės laikosi Bendrajame duomenų reglamente numatytų nuostatų, dėl to gali kilti pavojus duomenims, kurie gali apimti informaciją, susijusią su asmenų privačiu gyvenimu. Šiuo klausimu yra aktuali Europos Sąjungos Teisingumo Teismo (toliau – Teisingumo Teismas) byla C-311/18, kurioje buvo pasisakyta dėl fizinio asmens duomenų perdavimo iš Europos Sąjungos į Jungtines Amerikos Valstijas. Teisingumo Teismas pasisakė, jog Europos Sąjungos įmonės, kurios

perduoda duomenis apie asmenis už Europos Sąjungos ribų, privalo įsitikinti, jog priimančios valstybės aktai atitinka Bendrojo duomenų apsaugos reglamento nuostatas ir tuo atveju, jei ne – būtina taikyti papildomas apsaugos priemones arba sustabdyti duomenų perdavimą, taip pat pažymėjo, jog Nacionalinės priežiūros institucijos turi vykdyti aktyvią tokių duomenų perdavimo kontrolę (Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems, 2020).

Pažymėtina, kad egzistuoja sąlyginai naujas susitarimas tarp Europos Sąjungos ir Jungtinių Amerikos Valstijų, kuris yra vadinamas duomenų privatumo sistema (angl. *Data privacy framework*). Tai yra Jungtinių Amerikos Valstijų įmonių savarankiško sertifikavimo mechanizmas, kuriuo yra užtikrinamas tinkamas duomenų apsaugos lygis, kai duomenys yra perduodami iš Europos ekonominės erdvės. Ši sistema yra taikoma bet kokio tipo asmens duomenims, įskaitant duomenis, tvarkomus komerciniais ar sveikatos apsaugos tikslais, duomenis, susijusius su įdarbinimu (EU-U.S. Data privacy framework..., 2024, p. 3). Jungtinių Amerikos Valstijų įmonės, norinčios sertifikuotis, privalo laikytis visuotinai pripažintų 7 principų (apie kuriuos plačiau bus kalbama 3– ioje šio darbo dalyje), taip pat 16 šiuos principus papildančių ir vienodai privalomų principų (Participation Requirements Data Privacy...). Siekiant įsitikinti, jog įmonė, kuriai norima suteikti duomenis, turi teisę juos gauti, tvarkyti ir (ar) valdyti, duomenų eksportuotojas turi įsitikinti, kad įmonės atliktas sertifikavimas galioja, jis apima atitinkamus duomenis, taip pat turi būti užtikrinamas Bendrojo duomenų apsaugos reglamento nuostatų laikymasis (EU-U.S. Data privacy framework..., 2024, p. 4).

Kalbant apie darbo funkcijų atlikimą ir vietą, kurioje šios funkcijos yra atliekamos, reikia pripažinti, jog modernių technologijų panaudojimas tapo neišvengiamu darbo santykių elementu*,* o sparti technologinė pažanga darbdavį verčia imtis priemonių, siekiant realizuoti darbuotojų kontrolę, užtikrinančią sąžiningą ir tinkamą darbuotojų funkcijų atlikimą, tuo pat metu užtikrinant darbuotojų teisę į privatumą darbo vietoje. 2020 metais, prasidėjus pandemijai COVID-19 ir karantinui, tokia darbo organizavimo forma, kaip nuotolinis darbas, iki tol buvęs kaip galimybė ir laisvas pasirinkimas, tapo būtina sąlyga tęsti veiklą (The rise in telework: Impact…, 2022, p. 63). Nuotolinio darbo institutas suteikė ir iki šiol suteikia darbuotojams tam tikrų privalumų, pavyzdžiui, didesnį lankstumą, savarankiškumą, tačiau taip pat sukelia ir tam tikrų iššūkių – susiduriama su problema, jog naudojant skaitmenines priemones darbo funkcijų atlikimui, įsitvirtino kultūra, kai asmuo yra nuolat prisijungęs, visada pasiekiamas arba be perstojo dirbantis budėjimo režimu (Europos Parlamento rezoliucija su rekomendacijomis..., 2021). Šios aplinkybės lėmė

naujo darbuotojų apsaugos mechanizmo sukūrimo svarbą, tokiu mechanizmu galima pavadinti darbuotojų teisę atsijungti.

2.2. Darbuotojo teisė atsijungti

Šiuolaikinių technologijų naudojimas darbo santykiuose ir jau minėta įsitvirtinusi kultūra, kai darbuotojai yra nuolat prisijungę ir pasiekiami, sukūrė daugiau erdvės pažeisti pagrindines žmogaus teises, taip pat neužtikrinti tinkamų darbo sąlygų įskaitant teisingą darbo užmokestį, maksimalaus darbo ir minimalaus poilsio laiko laikymasi, saugą ir sveikatą darbe (Europos Parlamento rezoliucija su rekomendacijomis..., 2021). Teise atsijungti yra siekiama užtikrinti darbuotojų teisę į privatų gyvenimą ne darbo metu, nepatiriant neigiamų pasekmių iš darbdavio pusės.

Reikšminga šios darbuotojų teisės analizę pradėti nuo 2003 metų lapkričio 4 dienos Europos Parlamento ir tarybos direktyvos 2003/88/EB dėl tam tikrų darbo laiko organizavimo aspektų. Šio teisės akto pavadinimas suponuoja, jog jame yra numatomos tam tikros pareigos, susijusios su tinkamu darbo organizavimu, tad atkreiptinas dėmesys į tai, jog Direktyvoje yra išskiriamos tokios pareigos:

1. darbo valandų per savaitę limitas, kuris negali viršyti 48 valandų, įskaitant viršvalandžius;
2. pertrauka darbo metu, jei darbuotojas budi ilgiau nei 6 valandas;
3. minimalus kasdienio poilsio laikotarpis;
4. minimalus kassavaitinis poilsio laikas per kiekvieną septynių dienų laikotarpį;
5. kasmetinės mokamos atostogos, trunkančios ne mažiau kaip keturias savaites per metus.

Teisingumo Teismas byloje C-518/15, Ville de Nivelles prieš Rudy Matzak, priėmė sprendimą, kurį galima laikyti svarbiu argumentu už teisės atsijungti sukūrimą (Lerouge, Trujillo Pons, 2022, p. 453). Šioje byloje Teisingumo Teismas konstatavo, jog laikas, kurį darbuotojas praleidžia namuose turėdamas pareigą per 8 minutes sureaguoti į savo darbdavio iškvietimus, smarkiai ribojančią galimybes užsiimti kita veikla, laikytinas „darbo laiku“ (Ville de Nivelles v. Rudy Matzak, 2018). Taip pat Lietuvos Aukščiausiasis Teismas yra pasisakęs, jog budėjimo laikotarpį, kuriuo nustatyta, kad darbuotojas privalo vėl imtis darbo per vos kelias minutes, iš principo reikia laikyti darbo laiku, kaip tai suprantama pagal šią direktyvą, nes tokiu atveju darbuotojas praktiškai yra itin atgrasomas nuo bet kokios, net trumpalaikės, poilsio veiklos planavimo (Lietuvos Aukščiausiojo

Teismo 2023 m. gruodžio 20 d. nutartis civilinėje byloje). Tad tokia darbo organizavimo forma kaip nuotolinis darbas, darbo ir poilsio laikui keliami reikalavimai, taip pat ir pavyzdžiai pateikti analizuojant teismų praktiką įrodo, jog reikia reglamentuoti aiškų darbuotojų apsaugos mechanizmą, leidžiantį jiems išvengti nuolatinės darbo kultūros.

Teisė atsijungti nuo darbo Europos Sąjungos lygmeniu nėra įtvirtinta iki šiol, tačiau jau 2021 metais Europos Parlamentas pateikė svarstyti teisės akto projektą, kuris suteiktų galimybę nuotoliniu būdu dirbantiems asmenims pasibaigus darbo laikui atsijungti nuo bet kokių technologijų, kurios yra naudojamos darbo funkcijų atlikimo metu. Europos Parlamento ir Tarybos direktyva dėl teisės atsijungti apima reikalavimus, kad darbuotojai, darbo tikslais naudojantys skaitmenines priemones, įskaitant informacines ir ryšių technologijas, galėtų pasinaudoti savo teise atsijungti, taip pat užtikrina, kad darbdaviai gerbtų darbuotojų teisę atsijungti. Šis teisės aktas turėtų būti taikomas visiems viešiems ir privatiems sektoriams ir visiems darbuotojams, nepriklausomai nuo jų statuso ir darbo tvarkos. „Atsijungti“ pagal šią Direktyvą reiškia tiesiogiai ar netiesiogiai nedalyvauti su darbu susijusioje veikloje ar bendravime skaitmeninėmis priemonėmis ne darbo metu (Europos Parlamento rezoliucija su rekomendacijomis…, 2021). Naujausias siūlomos Direktyvos elementas – pareiga užtikrinti, kad būtų nustatyta išsami tvarka, leidžianti darbuotojams pasinaudoti teise atsijungti. Šiose priemonėse turėtų būti numatyta:

1. praktinė skaitmeninių priemonių išjungimo tvarka;
2. darbo laiko matavimo sistema;
3. sveikatos ir saugos vertinimai, įskaitant psichosocialinės rizikos vertinimus;
4. nukrypti leidžiančių nuostatų taikymo kriterijai ir visos susijusios kompensacijos už darbą neįprastu darbo laiku;
5. informuotumo didinimo priemonės ir mokymai darbo vietoje, kurių turi imtis darbdaviai (Bell *et al.*, 2021, p. 18).

Lietuvoje darbuotojų teisė atsijungti nėra įtvirtinta teisės aktais, tačiau buvo pateiktas įstatymo pakeitimo projektas dėl Darbo kodekso papildymo, kuriame numatyta pakeisti 52 straipsnio 5 dalį ir ją išdėstyti taip: 5. Nuotolinio darbo atveju darbuotojo dirbtas laikas apskaičiuojamas darbdavio nustatyta tvarka. Savo darbo laiką darbuotojas skirsto savo nuožiūra, nepažeisdamas maksimaliųjų darbo ir minimaliųjų poilsio laiko reikalavimų. Darbuotojas turi teisę atsijungti nuo skaitmeninių įrenginių ir būti darbdavio nepasiekiamas ne darbo laiku (Darbo kodekso 52 straipsnio pakeitimo…, 2022). Teisės Departamento išvadoje dėl siūlomo įstatymo pakeitimo projekto buvo numatyta, jog svarstytina, ar siūloma taisyklė yra darbo kodekso 52 straipsnio reguliavimo dalykas. Skaitmeniniai

įrenginiai gali būti naudojami ne tik dirbant nuotoliniu būdu, bet ir dirbant darbo vietoje (Teisės Departamento išvada dėl Darbo…, 2022).

Lietuvos Respublikos socialinės apsaugos ir darbo ministerija (toliau – Socialinės apsaugos ir darbo ministerija) nurodė, jog, nors terminas "teisė atsijungti" nėra tiesiogiai minimas Darbo kodekse, ši teisė jau yra įtvirtinta. Įstatymai skiria darbo ir poilsio laiką, suteikdami darbuotojams teisę nebūti pasiekiamiems po darbo valandų, teigiama, kad pakankama yra Darbo kodekse numatytų straispnių reguliuojančių darbo laiką, normą, režimą, nuotolinį darbą, viršvalandinį darbą ir budėjimą (Teisė atsijungti: Lietuvos darbuotojai turi…, 2024). Tačiau matoma, jog praktikoje vis dar kyla neaiškumų dėl darbuotojo teisės atsijungti, tai patvirtina tiek Lietuvos Aukščiausiojo Teismo, tiek ir Teisingumo Teismo sprendimai, kurie jau buvo aptarti šioje darbo dalyje.

2.3. Privatumo darbo santykiuose reguliavimas Europos Sąjungos valstybėse

Bendrajame duomenų apsaugos reglamente yra nustatomos taisyklės ir bendrieji principai susiję su asmens duomenų apsaugos sistema, šis Reglamentas yra tiesiogiai taikomas visoje Europos Sąjungoje, tačiau pravartu yra apžvelgti tam tikrų valstybių narių nacionalinius teisės aktus, kurie papildo taisykles, susijusias su privatumo darbo vietoje užtikrinimu, taip pat įtvirtina nacionalinėje teisėje jau minėtą darbuotojų teisę atsijungti nuo įrenginių ne darbo metu. Šioje dalyje bus aptariamos pasirinktos valstybės, kurių nacionalinės teisės nuostatos, autorės nuomone, gali būti pavyzdinėmis, lyginant su Lietuvoje egzistuojančiais teisės aktais.

Prancūzijos nacionalinis reguliavimas, kalbant apie darbuotojų privatumo apsaugą ir taisykles susijusias su darbuotojų kontrole darbo vietoje, naudojant modernias technologijas, nėra labai detalizuojamas, šiai temai yra aktualus Prancūzijos civilinis kodeksas (pranc. *Code civil*), kuriame yra garantuojama pagarba asmens privačiam gyvenimui, taip pat ir Prancūzijos darbo kodeksas (pranc. *Code du travali*) numatantis, kad niekas negali riboti asmenų teisių bei laisvių, kai tai nėra proporcinga siekiamam tikslui, tad nėra atskirų teisės aktų, kuriais būtų užtikrinamas privatumas šiuolaikinėje darbo vietoje, o tik iš kelių teisės aktų išplaukiančios taisyklės (Protection of privacy at work…, 2021). Tačiau, pažymėtina, kad Prancūzijoje įtvirtintos nuostatos, kurios detaliai reguliuoja darbuotojų teisę atsijungti.

Šiuo metu galiojančiame Prancūzijos darbo kodekso L2242-17 straipsnio 7 dalyje yra numatytos taisyklės, susijusios su darbuotojų teise atsijungti. Darbdaviai privalo derėtis su

socialiniais partneriais dėl darbuotojo teisės atsijungti įgyvendinimo būdų ir su įmonės skaitmeninių priemonių naudojimu susijusias taisykles, siekiant užtikrinti tinkamą darbuotojų poilsio laiką, atostogų suteikimą, taip pat tinkamą privataus ir profesinio gyvenimo pusiausvyrą. Darbo kodeksas nenumato sankcijų už nesėkmingas derybas, tačiau tai nereiškia, jog darbdaviai neturi laikytis įsipareigojimų, susijusių su darbuotojų teise atsijungti (Bell et. al., 2021, p. 20, 25). Darbdavys privalo parengti darbo tvarką, kurioje turi būti apibrėžtos naudojimosi teise atsijungti sąlygos (Right to disconnect: Implementation and…, 2023, p. 8). Teisės atsijungti svarba buvo patvirtinta ir viena naujausių Prancūzijos Kasacinio teismo nutarčių. Byloje buvo sprendžiamas klausimas dėl darbuotojo atleidimo iš darbo už šiurkštų darbo pareigų pažeidimą, o būtent, darbuotojas neatsiliepė į skambučius asmeniniu telefonu ne darbo metu, tačiau prieš tai jis buvo davęs sutikimą, kad su juo gali būti susisiekta laisvu nuo darbo laiku dėl su darbu susijusių priežasčių. Kasacinis teismas pasisakė, kad darbuotojas, net ir davęs sutikimą, neturėtų būti pasiekiamas savo asmeniniu telefonu ne darbo metu ir, kad tai negali būti laikoma pažeidimu (Berthereau, 2024). Panašų teisinį reguliavimą galima rasti ir tokiose Europos Sąjungos valstybėse, kaip Belgija, Graikija, Airija, Italija, Liuksenburgas, Slovakija, Ispanija, tačiau šioje dalyje plačiau nagrinėjamas Prancūzijos reguliavimas, nes būtent Prancūzija buvo pirmoji valstybė, kuri teisės aktuose įtvirtino darbuotojų teisę atsijungti (Right to disconnect: Implementation and…, 2023, p. 8-9).

Pirmasis teisės aktas, įtvitintas Europos Sąjungos valstybių, nacionaliniu lygmeniu reglamentuojantis privataus gyvenimo apsaugą darbo vietoje ir apimantis elektroninę darbo vietos stebėseną, informacijos apie darbuotojų sveikatą tvarkymą, buvo 2001 metais Suomijoje įsigaliojęs įstatymas dėl privataus gyvenimo apsaugos darbo vietoje (Hietanen, 2001). Šioje valstybėje ir šiuo metu yra nustatomos griežtos taisyklės susijusios su darbuotojų privatumo apsauga, Suomijoje galioja Duomenų apsaugos įstatymas 1050/2018 (suom. *Tietosuojalaki*), Elektroninių ryšių paslaugų įstatymas 917/2014 (suom. *Laki sähköisen viestinnän palveluista*), kuriuo, be kita ko, siekiama užtikrinti elektroninių ryšių konfidencialumą ir privatumo apsaugą, taip pat numatomos taisyklės susijusios su fizinio asmens buvimo vietos tvarkymu. Privatumo apsaugos darbo santykiuose įstatymas 759/2004 (suom. *Laki yksityisyyden suojasta työelämässä*) (Data protection laws of the…, 2023, p. 8) – būtent šiame įstatyme yra detaliai nustatytos taisyklės, susijusios su darbuotojų privatumo užtikrinimu, naudojant modernias technologijas darbo vietoje. 5 šio įstatymo skyriuje numatomos taisyklės, apimančios darbuotojų stebėjimą vaizdo kameromis ir tokios medžiagos tvarkymą. Kameros gali būti diegiamos, siekiant apsaugoti

teisėtą darbdavio interesą, tačiau stebėjimas negali būti vykdomas tam tikrose vietose ir stebint konkrečius darbuotojus, išskyrus atvejus, kai:

1. norima užkirsti kelią smurto grėsmei, žalai darbuotojų sveikatai ar saugumui, jiems atliekant darbo funkcijas;
2. galimų nusikaltimų nuosavybei prevencijai ar jų tyrimui, jeigu darbuotojo darbo funkcijos yra susijusios su didelės vertės turtu;
3. konkretaus darbuotojo interesų ir teisių apsaugai, kai stebėjimas vykdomas darbuotojo, kuris bus stebimas, prašymu.

Taip pat yra tiksliai įvardijama, kokius veiksmus turi atlikti darbdavys planuodamas ir įgyvendindamas tokio pobūdžio stebėjimą, o būtent:

1. prieš pradedant vykdyti stebėjimą vaizdo kameromis, darbdavys turi įsitikinti, kad nėra kitų priemonių, mažiau ribojančių darbuotojų privatumą;
2. į darbuotojų privatų gyvenimą turi būti kišamasi ne daugiau, nei tai yra būtina tikslui pasiekti;
3. įrašai turi būti naudojami tik tuo tikslu, dėl kurio buvo vykdomas stebėjimas;
4. darbuotojai turi būti informauojami apie vykdomą stebėjimą, toks informavimas turi apimti laiką, kada bus pradėtas toks stebėjimas, kaip jis bus vykdomas, supažindinami su įrašu naudojimo tikslais ir atvejais, taip pat apie vaizdo kamerų buvimo vietas, jei tokiu stebėjimu siekiama atskleisti nusikalstamos veikos vykdymą;
5. turi būti iškabinamos informacinės lentelės, kuriose pranešama apie vykdomą stebėjimą.

Taip pat, įstatyme nustatomi atvejai, kai darbdavys gali tvarkyti tokius duomenis, tikslus laikotarpis, kiek įrašas gali būti saugomas.

6 įstatymo skyriuje numatomos tasiyklės, sietinos su darbdavio vykdoma elektroninio pašto stebėsena. Darbdavys turi teisę vykdyti elektroninių laiškų kontrolę, jeigu jis pasirūpino darbuotojui būtinomis priemonėmis, kad būtų apsaugoti elektroniniai laiškai, siunčiami darbuotojo vardu, arba iš jo elektroninio pašto, ir šiuo tiklsu užtikrino, kad:

1. darbuotojas turi galimybę naudotis elektroninio pašto sistemos automatinio atsakymo funkcija, pranešti laiško siuntėjui apie savo nebuvimą darbo vietoje, nebuvimo trukmę bei informaciją apie asmenį, kuris turi pasirūpinti darbe nesančio darbuotojo užduotimis;

2. darbuotojas gali nukreipti gautus laiškus kitam darbdavio nurodytam asmeniui, kuriam yra pavesta atlikti užduotį;
3. darbuotojas gali duoti sutikimą susitarimui, remiantis kuriuo, darbuotojui nesant darbo vietoje, kitas jo pasirinktas ir darbdavio patvirtintas užduočiai atlikti asmuo gali gauti konkrečiam darbuotojui siunčiamus laiškus siekiant nustatyti, ar darbuotojui buvo išsiųstas pranešimas, kuris aiškiai skirtas darbdaviui darbo valdymo tikslais ir apie kurį darbdaviui būtina turėti informacijos dėl jo veiklos ar tinkamo darbo organizavimo.

Įstatyme yra numatyta, jog darbdavys turi teisę susipažinti su jam skirtais laiškais, kurie buvo siųsti į darbuotojo elektroninį paštą, tačiau šis procesas turi būti atliekamas kartu su asmeniu, turinčiu informacinės sistemos administratoriaus įgaliojimus, turi būti remiamasi informacija apie žinutės siuntėją, gavėją, pavadinimą, kad būtų įsitikinta, jog darbuotojui, jo nebuvimo darbe metu, buvo išsiųstas laiškas, susijęs su darbdavio teisėtais interesais ir prieiga prie jo užtikrins tinkamą tų interesų įgyvendinimą, su tokio proceso atlikimu turi būti supažindintas darbuotojas, o supažindinimo taisyklės apibrėžiamos įstatyme, tai yra, būtina surašyti ataskaitą, kurioje nurodoma koks elektroninis laiškas buvo atidarytas, kokiu tikslu ir kada jis buvo atidarytas, asmenys, kurie dalyvavo laiško atidarymo procese, taip pat kam buvo perduota informacija, sudaranti atitinkamo elektroninio laiško turinį, ataskaitą turi pasirašyti visi procese dalyvaujantys asmenys.

Kitose šio darbo dalyse bus aptariamos technologijos, apimančios ir galimybę rinkti duomenis iš kompiuterio ar mobiliojo įrenginio be vartotojo žinios, taip pat programinė įranga, kuri įrašo kiekvieną kompiuterio ar mobiliojo įrenginio paspaudimą. Tobulinant nuotolinio darbo organizavimo sistemas, tam tikros valstybės priėmė nuostatas, reglamentuojančias darbuotojo stebėjimą, dirbant nuotoliniu būdu ir draudžiančias tokio pobūdžio programinę įrangą. Graikijoje ir Kipre pastaraisiais metais buvo priimtas įstatymas, kuriuo aiškiai uždrausta stebėti darbuotojų veiklą, naudojant internetines kameras, Kipre toks draudimas yra siejamas su tokių prietaisų ar kitų invazinių technologijų metodų panaudojimu darbuotojų veiklos vertinimui. Portugalijoje, yra nustatyta, kad darbdavys privalo informuoti darbuotoją apie prietaisų, programų ir sistemų, skirtų jų veiklai, vykdomai nuotoliniu būdu, stebėti, savybes ir naudojimo būdą (Employee monitoring: A moving target..., 2024). 2024 metais buvo atnaujintas Bulgarijos darbo kodeksas, įtraukiant pakeitimus, susijusius su darbuotojų stebėjimu dirbant nuotoliniu būdu, pakeitimai buvo susiję ir su algoritminiu valdymu, o būtent – buvo apibrėžta, jog nuo šiol darbdaviai privalės tikrinti algoritminius darbo valdymo sprendimus, užtikrindami

žmogiškąją priežiūrą (Bulgaria: Algorithmic management, Restructuring legislation..., 2024).

Detaliai išanalizavus Suomijos Privatumo apsaugos darbo santykiuose įstatymą, taip pat apžvelgus egzistuojančius teisės aktus, susijusius su asmens duomenų apsauga ir privatumo užtikrinimu, išnagrinėjus Prancūzijos nacionalinį reguliavimą, susijusį su darbuotojų teise atsijungti, kuria yra garantuojama darbuotojo teisė į privatumą, galima teigti, jog toks griežtas ir tikslus reguliavimas yra naudingas, nes aiškios ir detalios taisyklės, apibrėžiančios darbo santykių subjektų teises ir pareigas, sumažina pažeidimų riziką, taip pat užkerta kelią skirtingoms interpretacijoms, skatina skaidrumą darbo santykiuose. Šioje dalyje jau buvo paminėtos tokios darbuotojų stebėjimo technologijos, kaip vaizdo ir garso, elektroninio pašto stebėsena, tad toliau yra tikslinga aptarti modernias technologijas, kurios yra aktyviai naudojamos šiuolaikinėje darbo vietoje.

2.4. Darbo santykiuose dažniausiai naudojamų modernių technologijų rūšys

Technologinė pažanga lemia naujų darbo organizavimo būdų atsiradimą, taip pat kelia iššūkių darbuotojų teisėms, ypač teisei į privatumą. Darbdaviai, vykdydami darbuotojų kontrolę vis dažniau naudoja įvairias modernias technologijas – darbuotojų stebėjimo sistemas, dirbtinio intelekto sprendimus, specialių kategorijų asmens duomenų tvarkymą ir kitas inovacijas, kurios daro įtakos darbo santykių pobūdžiui. Šioje dalyje bus aptariamos dažniausiai darbo santykiuose naudojamos šiuolaikinės technologijos ir jų taikymo teisiniai aspektai.

2.4.1. Vaizdo ir garso stebėjimas

Vaizdo stebėjimas yra asmens duomenų tvarkymo būdas, naudojant automatines vaizdo stebėjimo priemones. Kalbant apie tokį duomenų tvarkymo būdą, pažymima, jog nėra svarbu, ar šie duomenys yra išsaugomi laikmenoje, ar ne (Vaizdo stebėjimas pagal bendrąjį duomenų..., 2019). Kaip jau buvo aptarta šiame darbe, atliekant bet kokį su duomenų subjektu susijusį duomenų tvarkymą, reikia nustatyti teisėtą tikslą ir šio tikslo ribas. Civilinio kodekso 2.22 straipsnyje yra pabrėžiama, jog bet koks veiksmas atliekamas su fizinio asmens atvaizdu ar jo dalimi turi būti vykdomas tik jo sutikimu, tokio sutikimo nereikia tik tais atvejais, jei veiksmai yra susiję su visuomenine veikla, asmens tarnybine padėtimi, teisėsaugos institucijų reikalavimu ar fotografuojant viešoje vietoje, tačiau, jei

toks atvaizdo demonstravimas, atgaminimas, perdavimas pažeidžia asmens garbę, orumą, dalykinę reputaciją, atlikti šiuos veiksmus yra draudžiama.

Kalbant apie vaizdo stebėjimą darbo santykių kontekste, reikia laikytis tam tikros tvarkos, o būtent, montuojant vaizdo filmavimo kameras, reikia užtikrinti, kad nebūtų filmuojama konkreti darbo vieta, siekiant kontroliuoti darbuotojus, filmuojama taip pat negali būti poilsio zonose, persirengimo kambariuose ir kitose vietose, kuriose asmuo gali tikėtis absoliutaus privatumo, tad vaizdo kameros turi būti montuojamos tik bendro naudojimo vietose, o asmenys apie vaizdo stebėjimą turi būti informuojami, darbuotojai – pasirašytinai ar kitu jų informavimą įrodančiu būdu, o kiti asmenys – pateikiant informaciją apie vaizdo stebėjimą informacinėse lentelėse (Vaizdo stebėjimas pagal bendrąjį duomenų..., 2019).

Pažymima, kad tais atvejais, kai darbo specifika reikalauja užtikrinti asmenų, turto ar visuomenės saugą, vaizdo stebėjimas darbo vietoje gali būti pradėtas, bet tik tokiu atveju, kai kiti metodai ar priemonės yra nepakankami arba (ir) netinkami šiems tikslams pasiekti (Tamašauskaitė-Janickė, 2016, p. 89). Tačiau atkreiptinas dėmesys, jog vaizdo duomenys turi būti patvirtinti duomenų valdytojo, darbo santykių kontekste – darbdavio rašytiniame dokumente, kuriame turi būti nurodytas vaizdo stebėjimo tikslas, duomenų saugojimo trukmė, prieigos sąlygos, duomenų tvarkymo, jų naikinimo tvarka, bei kiti teisėto duomenų tvarkymo reikalavimai. Su tokiais duomenimis susipažinti gali tik darbdavio įgalioti asmenys, kuriems tokia prieiga būtina jų funkcijoms atlikti ir kurie yra susipažinę su asmens duomenų apsaugos teisiniais reikalavimais ir pasirašytinai įsipareigoję tokių reikalavimų laikytis (Bagdanskis, Sartatavičius, 2012, p. 708). Praktikoje egzistuoja pavyzdžių, kai darbuotojų stebėjimas jų darbo vietoje pripažįstamas teisėtu. Europos Žmogaus Teisių Teismo byloje Lopez Ribalda ir kiti prieš Ispaniją, darbdavys, reaguodamas į prekybos centre vykstančias vagystes, įrengė vaizdo stebėjimo kameras. Kameros, kuriomis buvo siekiama nustatyti galimas klientų vagystes buvo matomos, o kameros, skirtos kasų darbuotojų fiksavimui – paslėptos, prekybos centre buvo pakabinti ženklai, informuojantys apie vaizdo fiksavimą, tačiau darbuotojams tikslingai nebuvo pranešta apie paslėptas kameras, kuriomis galiausiai buvo užfiksuotas darbuotojų vagystės faktas, tad darbuotojai buvo atleisti iš darbo ir kreipėsi į teismą dėl neteisėto atleidimo ir jų privatumo pažeidimo teigdami, kad stebėjimas vyko neteisėtai. Žmogaus teisių teismas šiuo atveju padarė išvadą, kad stebėjimas buvo pagrįstas, būtinas ir proporcingas, nes juo buvo siekiama apsaugoti verslo interesus ir toks stebėjimas gali būti vykdomas be

išankstinio pranešimo asmenims, kurie yra įtariami atliekant neteisėtus veiksmus (López Ribalda and others v. Spain, 2019).

Asmens duomenų teisinės apsaugos įstatymo 5 straipsnio 4 dalyje yra numatyta: Tvarkant vaizdo ir (ar) garso duomenis darbo vietoje ir duomenų valdytojo patalpose ar teritorijose, kuriose dirba jo darbuotojai, tvarkant asmens duomenis, susijusius su darbuotojų elgesio, buvimo vietos ar judėjimo stebėsena, šie darbuotojai apie tokį jų asmens duomenų tvarkymą turi būti informuojami pasirašytinai ar kitu informavimo faktą įrodančiu būdu. Šioje straipsnio dalyje yra išskiriami darbuotojų kontrolės būdai. Vaizdo stebėjimą jau aptarėme, ne ką mažiau yra aptarti ir garso stebėjimo atvejus.

Šiame kontekste atkreiptinas dėmesys į Europos Žmogaus Teisių teismo bylą Halford prieš Jungtinę Karalystę. Pateiktas Teismo sprendimas padeda suprasti kokiais atvejais toks darbuotojų kontrolės būdas gali peržengti proporcingumo ir teisėtumo ribas. Byloje pareiškėja padavė skundą teismui dėl to, kad jai esant darbo vietoje buvo perimti jos pokalbiai telefonu ir tai pažeidė jos teisę į privatų gyvenimą. Žmogaus teisių teismas pripažino, kad buvo pažeistas Žmogaus teisių konvencijos 8 straipsnis, nes pareiškėja pagrįstai tikėjosi privatumo skambinant iš savo kabineto, o skambučiai galėjo būti laikomi privačiais pokalbiais. Tuo tarpu, atsakovas neįrodė, kad pokalbių klausymas buvo būtinas, siekiant užtikrinti Žmogaus teisių konvencijos 8 straipsnio 2 dalyje nurodytų teisėtų tikslų ir toks klausymas neturėjo teisinio pagrindo (Halford v. The United Kingdom, 1997). Tad ši byla yra svarbi tuo, kad joje buvo išaiškinta, jog darbuotojas pagrįstai gali tikėtis privatumo darbo vietoje, o slaptas pokalbių klausymas nėra teisėtas, kai apie tai nėra pranešama darbuotojui ir nėra pagrįsto teisinio pagrindo tokiems veiksmams atlikti.

Verta išanalizuoti ir naujausią Duomenų apsaugos inspekcijos sprendimą, kuriame pateikiamas atvejis, kai garso įrašymo įrangos panaudojimas buvo pripažintas teisėtu ir proporcingu (Valstybinės duomenų apsaugos inspekcijos 2025 m. sausio 10 d. sprendimas). 2023 metais į Duomenų apsaugos inspekciją kreipėsi asmuo, teigdamas, jog jo darbdavys neteisėtai tvarko lokomotyvų įgulų narių garso įrašus, taip pažeisdamas jų teisę į privatumą. Skunde nurodoma, kad pareiškėjo darbo vietoje (traukinio mašinisto kabinoje) yra vykdomas ne tik vaizdo stebėjimas, bet ir nuolatinis garso įrašymas, kuris, jo nuomone, yra perteklinis, nes visi darbdavio įgaliotų asmenų ir pareiškėjo skambučiai darbo klausimais yra vykdomi racijos pagalba ir įrašomi, tad papildomas garso įrašymas mašinisto kabinoje neatitinka Bendrajame duomenų apsaugos reglamente numatyto duomenų kiekio mažinimo principo ir pažeidžia jo teisę į privatumą, nes apima ir asmeninius pokalbius telefonu su kitais asmenimis. Skunde pareiškėjas prašė Duomenų apsaugos inspekcijos įvertinti ar

skundžiamas asmuo teisėtai ir pagrįstai renka garso duomenis mašinisto kabinoje, kai tikslams pasiekti darbdavys gali apsiriboti mažiau pareiškėjo teisę į privatumą ir asmeninio susižinojimo slaptumą varžančiomis priemonėmis ir ar įrašų atskleidimas tretiesiems asmenims darbo pareigų pažeidimo atveju, neturint užfiksuoto darbuotojo sutikimo konkrečiame įraše, yra pagrįstas ir teisėtas. Skundžiamas asmuo Duomenų apsaugos inspekcijai pateikė paaiškinimus, kuriuose numatė, jog vaizdo stebėjimas bei garso įrašymas yra vykdomas siekiant užtikrinti geležinkelių transporto eismo saugą, vykdyti traukinio mašinistų pareigybinių funkcijų priežiūrą, vykdyti prevencinę darbo stebėseną ir užtikrinti sklandžią bei objektyvią darbuotojų praktinių gebėjimų egzamino eigą, pažymėjo, jog garso įrašymas yra būtinas siekiant užtikrinti geležinkelių eismo saugumą vadovaujantis Geležinkelių transporto eismo saugos valdymo sistemų reikalavimų aprašo nuostatomis. Skundžiamasis pažymėjo, jog buvo atliktas teisėtų interesų balanso testas ir poveikio duomenų apsaugai vertinimas, kurie parodė, jog tokių duomenų tvarkymas atitinka ne tik teisėtą interesą, bet ir plačiosios visuomenės interesus, todėl toks teisėtas interesas pripažįstamas svarbesniu nei darbuotojo, kaip duomenų subjekto. Duomenų apsaugos inspekcija, atsižvelgdama į skundžiamo asmens paaiškinimus, taip pat vykdomos veiklos specifiką ir su ja susijusius veiksnius, galimas pasekmes, bei nustatytus elgesio reikalavimus mašinistų darbo vietoje, pripažino, jog garso įrašymas buvo proporcinga ir teisėta priemonė, taip pat buvo nustatyta, kad tiriant pareiškėjo darbo drausmės pažeidimą, darbuotojo duomenys buvo perduoti teisėtai. Duomenų apsaugos inspekcija konstatavo, jog nei garso įrašymas, nei duomenų perdavimas tretiesiems asmenims nepažeidė Bendrojo duomenų apsaugos reglamento ir pareiškėjo teisės į privatumą.

2.4.2. Geolokacinė stebėsena

Šiais laikais plačiai paplito technologijos, suteikiančios darbdaviams galimybę stebėti savo transporto priemones ir konkretų darbuotoją, kuris naudojasi ta transporto priemone. Lietuvos Respublikos elektroninių ryšių įstatymo 3 straipsnio 98 dalyje pateikiama vietos nustatymo duomenų sąvoka: Vietos nustatymo duomenys – elektroninių ryšių tinkluose arba teikiant elektroninių ryšių paslaugas tvarkomi duomenys, įskaitant duomenis, gautus iš elektroninių ryšių tinklo infrastruktūros, taip pat duomenys, gauti iš paslaugų gavėjo galinio įrenginio, nurodantys faktinio viešųjų elektroninių ryšių paslaugų gavėjo mobiliojo ryšio galinio įrenginio geografinę buvimo vietą arba fiksuotojo ryšio tinklo galinio taško fizinio adreso duomenis (Lietuvos Respublikos elektroninių ryšių įstatymas, 2004). Šio

įstatymo 77 straipsnio 1 dalyje yra numatyta, kad viešųjų elektroninių ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjai gali rinkti, saugoti ir tvarkyti tuos abonentų bei registruotų paslaugų gavėjų asmens, srauto ir susijusius duomenis, kurie yra būtini abonentams ir paslaugų gavėjams nustatyti, paslaugoms teikti, apskaitai ir atsiskaitymui. Renkant duomenis apie transporto priemonės buvimo vietą, judėjimo pradžios ir pabaigos laiką, kryptis ir kitus duomenis siekiama užtikrinti darbdavio teisėtą interesą, tačiau net jeigu darbdavys turi teisėtą interesą, iš pradžių reikia įvertinti, ar duomenų tvarkymas darbdavio numatytais tikslais yra reikalingas ir ar jų faktinis įgyvendinimas atitinka proporcingumo ir subsidiarumo principus (29 straipsnio duomenų apsaugos darbo grupė, 2017, p., 22). Asmens buvimo vietos nustatymui yra naudojami palydovai, informacinių ir komunikacinių technologijų priemonės, tokioms sistemoms apibūdinti yra vartojamas terminas "globalaus pozicionavimo sistema", geriau žinoma kaip "GPS", darbdavio interesas žinoti ir kontroliuoti darbuotoją realiuoju laiku, taip pat rinkti informaciją, yra priežastis, dėl kurios yra diegiamos vietos nustatymo sistemos (Tamašauskaitė-Janickė, 2016, p. 97).

Globalaus pozicionavimo sistemų stebėjimo naudojimas turi būti suderintas su darbuotojo teise į privatumą, o tai reiškia, jog visų pirma, darbuotojas turi būti informuotas apie vykdomą sekimą, o būtent darbdavys suteikia darbuotojui, pavyzdžiui, vairuojančiam atitinkamą transporto priemonę, informaciją apie tai, jog transporte yra sumontuotas sekimo įrenginys ir, kad jų judėjimas įrašinėjamas transporto priemonės naudojimo metu, jeigu atitinkama technologija fiksuoja ir asmens veiksmus, apie tai irgi turi būti suteikta informacija, antra, jeigu darbuotojui yra suteikiama galimybė naudotis transporto priemone ne tik darbo funkcijų atlikimo metu, o ir asmeniniais tikslais, nėra tikėtina, kad darbdavys turės teisinį pagrindą vykdyti buvimo vietos ar judėjimo stebėseną (29 straipsnio duomenų apsaugos darbo grupė, 2017, p., 22), todėl į tokias transporto priemones turėtų būti diegiamos sistemos, leidžiančios išjungti vietos nustatymo funkciją ir apie tai pranešta darbuotojui, tokiu būdu užtikrinant jo teisę į privatumą. Byloje Florindo de Almeida Vasconcelos Gramaxo prieš Portugaliją, pareiškėjas buvo atleistas iš darbo po to, kai darbdavys susipažino su duomenimis, gautais iš globalaus pozicionavimo sistemos, įrengtos jo automobilyje, naudotame darbo tikslais, duomenų valdytojas stebėjo darbuotojo nuvažiuotus atstumus darbo, ir, jei taikytina, privačių kelionių metu, siekdamas kontroliuoti bendrovės išlaidas. Darbuotojas teigė, jog toks stebėjimas pažeidė jo teisę į privataus gyvenimo apsaugą pagal Žmogaus teisių konvencijos 8 straipsnį, tačiau Žmogaus teisių teismas konstatavo, kad šio straipsnio nuostata nebuvo pažeista, o globalaus pozicionavimo

sistemos naudojimas buvo teisėtas, nes darbuotojas žinojo, jog bendrovė jo transporto priemonėje įrengė šią sistemą, taip pat tokiu stebėjimu buvo siekiama teisėto tikslo – bendrovės išlaidų stebėsenos (Florindo de Almeida Vasconcelos Gramaxo v. Portugal, 2022).

Darbo kodekso 31 straipsnio 1 dalyje numatyta, kad darbdavys privalo sudaryti darbuotojui sąlygas darbo funkcijai atlikti, suteikti darbuotojui reikalingas priemones ar turtą. Darbdaviui suteikus darbo priemones darbuotojui, atsiranda galimybė stebėti ir kontroliuoti tokių priemonių naudojimą, norint užtikrinti, kad jos naudojamos tik darbo funkcijų atlikimui, o jeigu darbdavys nedraudžia naudoti tokių priemonių asmeniniais tikslais, tai turi būti iš anksto aptarta su darbuotoju, tačiau leidimas naudoti darbo priemones ir laisvu nuo darbo metu, gali apsunkinti darbdavio vykdomą stebėjimą ir jo teisėtumą, nes vykdant kontrolę ne darbo valandomis, kai darbuotojas gali tikėtis privatumo, gali būti pažeistos darbuotojo, kaip asmens, pagrindinės teisės ir laisvės.

2.4.3. Kitų skaitmeninių technologijų stebėsena

Darbe detaliai buvo apžvelgtas nacionalinis Suomijos reguliavimas, susijęs su darbuotojų privatumo apsaugos užtikrinimu ir darbdavio vykdomo stebėjimo taisyklėmis, įskaitant elektroninio pašto patikrą, tad toliau svarbu yra aptarti Lietuvoje egzistuojančias nuostatas, susijusias su tokio pobūdžio stebėsena, taip pat socialinių tinklų ir susirašinėjimo juose patikros teisinį reguliavimą ir susiformavusią praktiką.

Darbo kodekso 27 straipsnio 2 dalyje nurodyta, jog net jei informacinės ir elektroninių ryšių technologijos nuosavybės ar valdymo teise priklauso darbdaviui, darbuotojų asmeninio susižinojimo slaptumas negali būti pažeidžiamas, tad, pavyzdžiui, jeigu darbuotojas susirašinėja asmeniniais tikslais, darbdavys neturi teisės pažeisti jo slaptumo. Aptariant elektroninių ir informacinių technologijų naudojimo kontrolės klausimą, svarbu aptarti bylą Barbulescu prieš Rumuniją. Pareiškėjas darbdavio prašymu susikūrė paskyrą “Yahoo! Messenger“, kuriame komunikavo su klientais. Vidinėje tvarkoje buvo nurodyta, jog darbuotojai turėtų susilaikyti nuo bet kokios asmeninės veiklos darbo vietoje ir nenaudoti įmonės priemonių asmeniniais tikslais. Darbdavys įvykdė darbuotojo stebėseną ir jos metu buvo nustatyta, kad darbuotojas naudojo šią paskyrą asmeniniais tikslais. Pareiškėjas teigė, jog tokiais veiksmais darbdavys pažeidė jo teisę į privataus gyvenimo gerbimą pagal Žmogaus teisių konvencijos 8 straipsnį. Teismas konstatavo, kad nacionaliniai teismai nenustatė ar darbuotojas buvo įspėtas, kad jo

elektroninis susirašinėjimas gali būti stebimas. Barbulescu nebuvo informuotas dėl stebėjimo pobūdžio ir masto, o būtent apie tai, kad darbdavys galės stebėti jo susirašinėjimo turinį, taip pat teismas pažymėjo, jog toks stebėjimas nebuvo proporcingas ir galima buvo imtis priemonių, mažiau ribojančių darbuotojo teisę į privataus gyvenimo ir susirašinėjimo gerbimą. Tačiau šis sprendimas nereiškia darbdavio teisės stebėti darbuotoją, kai darbuotojas yra įtariamas besinaudojant internetu asmeniniais tikslais, visiško apribojimo. Šio sprendimo 121 punkte nurodyti veiksniai, į kuriuos reikia atsižvelgti, norint įvertinti tokio stebėjimo teisėtumą, o būtent:

1. darbuotojui turi būti pranešta iš anksto apie stebėsenos pobūdį, šiuo atveju, kad darbdavys gali imtis susirašinėjimo kontrolės priemonių ir apie tokių priemonių įgyvendinimą;
2. turi būti vertinamas darbdavio vykdomos stebėsenos mastas ir įsiterpimo į asmens privatų gyvenimą laipsnis;
3. darbdavys turi pateikti teisėtą pagrindą tokiam stebėjimui vykdyti;
4. įvertinti, ar tikslas gali būti pasiektas ne tokiais darbuotoją varžančiais metodais;
5. įvertinti kokias pasekmes stebėsena gali sukelti darbuotojui ir kaip darbdavys panaudoja stebėsenos rezultatus;
6. suteikti darbuotojui tinkamas apsaugos priemones, užtikrinančias darbdavio negalėjimą susipažinti su konkrečiu susirašinėjimo turiniu be išankstinio pranešimo darbuotojui (Bărbulescu v. Romania, 2017).

Socialinių tinklų naudojimas darbo teisiniuose santykiuose, atskleidžia pusiausvyros tarp darbdavio interesų ir darbuotojų teisės į privatumą problematiką. Mokslinėje literatūroje yra pateikiama ne viena socialinių tinklų apibrėžtis, viena iš jų yra tokia, jog tai yra žiniatinklio paslaugos, leidžiančias asmeniui:

1. sukurti viešą arba pusiau viešą profilį ribotoje sistemoje;
2. susidaryti sąrašą kitų naudotojų su kuriais juos sieja bendri ryšiai;
3. peržvelgti ir naršyti po savo ir kitų naudotojų ryšių sąrašą sistemoje.

Priklausomai nuo svetainės tinklų funkcijos ir narystės, pobūdis gali skirtis (Boyd, Ellison, 2007, p. 211). Galima aptikti socialinių tinklų grupavimą į ryšių ir turinio socialinius tinklus (Beye, Jeckmans *et al*., 2010, p. 4-5). Šiame darbe bus aptariami tik socialinių ryšių tinklai, kurie apima tokius visiems gerai žinomus socialinius tinklus kaip „Facebook“, „Instagram“. Pažymėtina, kad galima aptikti šaltinių, kuriuose žmogaus teisės interneto socialiniuose tinkluose yra vadinamos “skaitmeninės teisės”, tačiau iš esmės tai yra tos pačios žmogaus teisės, tik neįprastoje, skaitmeninėje erdvėje, pavyzdžiui, teisė į

privatumą internete ir saviraiškos laisvė, yra Žmogaus teisių deklaracijoje įtvirtintų nuostatų išplėtimas (Hutt, 2015).

Kalbant apie socialinių tinklų tikrinimą, kurį vykdo darbdavys, pažymima, kad asmenų tikrinimas socialiniuose tinkluose yra galimas tik išskirtinais atvejais, tokie patikrinimai yra susiję ne tik su darbo santykių laikotarpiu, tačiau dažnu atveju yra tikrinamos kandidatų socialinės paskyros. Didžiausios žalos kilimas yra siejamas su tuo, kad socialiniuose tinkluose gali būti pateikiama informacija, kuri neskelbiama kandidato teikiamame gyvenimo aprašyme ir nesusijusi su dalykinėmis savybėmis, tai gali apimti Bendrojo duomenų apsaugos reglamento 9 straipsnyje numatytus specialios kategorijos asmens duomenis, pavyzdžiui, informaciją susijusią su lytine orientacija, politiniais įsitikinimais, priklausymu profesinėms sąjungoms. Jeigu tokio pobūdžio duomenų rinkimas nesusijęs su darbo funkcijomis, pažeidžiama kandidato teisė į privatumą ir sukuriamos prielaidos jį diskriminuoti (Grigonienė, 2021), o diskriminacijos draudimas, taip pat kaip ir draudimas pažeisti privatumą yra įtvirtintas Darbo kodekse ir kituose teisės aktuose. Socialiniai tinklai dažniausiai yra naudojami asmeniniais tikslais, todėl darbo kontekste juose esanti informacija negalėtų būti renkama. Tokia taisyklė yra taikoma ir atvejams, kai informacija renkama ir iš kitų viešai prieinamų šaltinių, tačiau, jeigu darbdavys išskirtinais atvejais manytų, kad būtina tikrinti informaciją viešai prieinamuose šaltiniuose, toks asmens duomenų tvarkymas turėtų būti pagrindžiamas, o būtent, turi būti pateikta priežastis, kodėl darbdavio interesas konkrečiu atveju nusveria darbuotojo teisę į privatumą (Gairės smulkiajam ir vidutiniam verslui, 2023, p. 15).

Pagrindinis socialinių tinklų tikslas – dalintis informacija. Asmeninė informacija, kuri įprastai skelbiama socialiniuose tinkluose, apima asmens identifikatorius, kontaktinę informaciją, socialinius ryšius, veiklą internete. Tai kelia riziką privatumo apsaugai, nes tretieji asmenys, panaudoję viešai skelbtinus duomenis, gali įgyvendinti veiksmus, kuriais bus pažeista asmens teisė į privatumą (Chan, Virkki, 2014, p. 41-42). Šiame kontekste paminėtina Žmogaus Teisių Teismo byla Editions Plon prieš Prancūziją. 2004 metų gegužės 18 dieną Teismas konstatavo, kad atvejais, kai asmeninė informacija yra paskelbiama internete, prioritetiniu nebegali būti laikomas poreikis ją apsaugoti, nes praktikoje yra pripažįstama, jog ji tapo paskelbta plačiu mastu ir nuo to laiko nebelaikoma konfidencialia, tačiau 2010 metų gruodžio 16 dienos Žmogaus Teisių Teismo byloje Aleksey Ovchinnikov prieš Rusiją, buvo pažymėta, jog net ir netekus konfidencialumo apsaugos, turi būti garantuojama privataus gyvenimo ir reputacijos apsauga (Civilka, Šlapimaitė, 2015, p. 128, 129). Socialinių tinklų plėtra kelia susirūpinimą dėl būdų, kaip

galima būtų apsaugoti privatumą, asmens duomenis, garbę ir orumą, saviraiškos laisvę. Europos Taryba Rekomendacijose CM/Rec(2012)4 dėl žmogaus teisių apsaugos teikiant socialinių tinklų paslaugas, yra išskyrusi tam tikrus pavojus:

1. teisinių ir procedūrinių apsaugos priemonių, susijusių su procesais, dėl kurių naudotojai gali būti pašalinti, trūkumą;
2. nepakankamą vaikų ir jaunimo apsaugą nuo žalingo turinio ar elgesio;
3. kitų asmenų teisių negerbimą;
4. privatumui palankių nuostatų nebuvimą;
5. skaidrumo apie asmens duomenų rinkimo ir tvarkymo tikslus nebuvimą (Europos duomenų apsaugos teisės vadovas, 2018, p. 376).

Aptariant socialinių tinklų stebėsenos problematiką, svarbu yra atkreipti dėmesį į Konstitucijos 25 straipsnį, kuris numato, jog žmogus turi teisę turėti savo įsitikinimus, juos laisvai reikšti, jam neturi būti kliudoma ieškoti, gauti ir skleisti informaciją bei idėjas. Ši teisė gali būti vadinama saviraiškos, nuomonių reiškimo laisve, ji apima dvi tarpusavyje susijusias asmens teises, o būtent teisę turėti įsitikinimus ir teisę juos laisvai reikšti (Meškauskaitė, 2018, p. 88). Minimame Konstitucijos straipsnyje taip pat numatyta ir galimybė apriboti šią konstitucinę teisę, šio darbo kontekste svarbu yra aptarti teismų praktiką, kurioje yra analizuojami klausimai, susiję su saviraiškos laisvės ir privatumo apribojimo galimybėmis, nes tai yra būdas, kaip darbdavys gali kontroliuoti savo darbuotojus ir kaip darbuotojo piktnaudžiavimas jo turimomis teisėmis gali tapti atleidimo iš darbo priežastimi.

Byloje Preece prieš JD Wetherspoons plc ET/2104806/10 teismas pateisino atleidimą iš darbo, nes užkandinės padavėja parašė neigiamų komentarų „Facebook“ apie klientų šiurkštų elgesį, toks informacijos paviešinimas socialiniame tinkle, pablogino darbdavio reputaciją, taip pat Prancūzijos teismas pripažino, kad darbuotojo vieši, įžeidžiantys komentarai jau minėtame socialiniame tinkle peržengė darbuotojų privatumo ribas, tai pakenkė darbdavio įvaizdžiui ir dalykinei reputacijai, toks elgesys yra vertinamas kaip šiurkštus darbo pareigų pažeidimas. Svarbu paminėti ir Bezansono apeliacinio teismo sprendimą, kuriame pasisakyta, jog darbuotojo įžeidžiančio pobūdžio komentarai socialiniame tinkle laikytini teisėta atleidimo iš darbo priežastimi, lemiamą sprendimą daro tai, ar išsakyti komentarai yra vieši ar privatūs (Tamašauskaitė-Janickė, 2016, p. 172-174).

Socialinių tinklų naudotojai gali keisti savo paskyrų privatumo nustatymus, taip užkertamas kelias asmeninės informacijos atskleidimui tretiesiems asmenims. Pavyzdžiui, „Instagram“ suteikia galimybę padaryti uždarą vartotojo profilį, toks profilio kūrimas

neleidžia asmenims, kurie nėra priimti į draugų sąrašą, peržiūrėti įkeliamą informaciją (nuotraukas, vaizdo įrašus, diskusijas ir panašiai).

Tad darbuotojų stebėsena gali apimti ir jų naudojimąsi socialiniais tinklais, vidinės darbo vietos tvarkos gali riboti naudojimąsi tokio pobūdžio technologijomis, kaip buvo numatyta byloje Barbulescu prieš Rumuniją, kai kurie darbdaviai turi norą tikrinti ir traukti informaciją iš darbuotojų socialinių tinklų paskyrų, darydami prielaidą, jog jie taip gali elgtis, nes informacija yra skelbiama viešai. Tokia informacija yra naudojama ir žmogiškųjų išteklių valdymo subjektų, kurie naudojasi dirbtinio intelekto algoritmais, pateikiančiais įžvalgas dėl darbuotojų, taip pat siekiant užtikrinti, kad viešas darbuotojų elgesys socialinėje erdvėje nedarytų neigiamo poveikio įmonės reputacijai (Murugesan, *et al*, 2023, p. 3).

Tokio pobūdžio stebėsena turi būti vertinama remiantis Bendrajame duomenų apsaugos reglamente numatytu proporcingumo principu, siekiant nustatyti stebėsenos pagrįstumą ir tinkamumą, taip pat būtinumą, tačiau kaip ir daugelis kitų technologijų stebėsenos būdu, taip ir šis kelia klausimų, susijusių su galimu privatumo teisių pažeidimu, ypač atsižvelgiant į tai, kad daugumoje valstybių nėra konkretaus socialinių tinklų naudojimo darbo santykių kontekste, reglamentavimo. Dėl asmens duomenų viešo prieinamumo, Bendrojo duomenų apsaugos reglamento reikalavimai netampa mažiau taikytini, taip pat nesumažėja ir duomenų subjektui suteikiama teisinė apsauga (Employee monitoring: A moving target, 2024). Tad duomenų paviešinimas nesuteikia teisės naudoti juos ne tais tikslais, dėl kurių jie buvo paviešinti internete (Civilka, Šlapimaitė, 2015, p. 129).

Apibendrinant galima teigti, kad bet kokia darbuotojų skaitmeninių technologijų stebėsena, turi būti atliekama tik turint teisinį pagrindą, numatytą įstatyme, tai apima ir įdarbinimo procesą. Svarbu, kad asmuo, naudojantis socialiniais tinklais, aktyviai taikytų privatumo apsaugos priemones, siekdamas riboti savo asmeninės informacijos, skelbiamos internete, prieinamumą tretiesiems asmenims. Tai yra vienas iš efektyviausių būdų užkirsti kelią tokio pobūdžio stebėsenai, nes neatlikus šių veiksmų yra sukuriama terpė darbdaviui, neinformavus darbuotojo, peržiūrėti viešai prieinamus profilius be asmens žinios. Vis dėlto, darbdaviai gali vykdyti socialinių tinklų stebėseną esant teisiniam pagrindui, tai yra ypač naudinga siekiant apsaugoti konfidencialią informaciją ir (ar) įmonės reputaciją, tokių pačių tikslų yra siekiama ir vykdant darbuotojų susirašinėjimo kontrolę, o tam, kad būtų išvengta konfliktų, tiek darbdavys turi atsakingai vykdyti šią veiklą, tiek ir darbuotojas turi nepiktnaudžiauti jo turimomis teisėmis ir tinkamai atlikti darbo funkcijas.

2.4.4. Debesų kompiuterija

Debesų kompiuterija – informacinių ir ryšių technologijų paslaugų teikiamų per tinklą, pavyzdžiui, internetą, modelis. Ši technologija leidžia naudotis ištekliais, nepriširšant prie konkretaus fizinio įrenginio (Davies, 2016, p. 1). Yra išskiriami tam tikri debesų kompiuterijos modeliai, o būtent:

1. debesies infrastruktūra kaip paslauga (angl. *Infrastructure as a Service*), šio modelio pavyzdžiai yra virtualūs serveriai, saugyklos (Aravamudhan, 2021);
2. debesies platforma kaip paslauga (angl. *Platform as a Service*), tai tokios platformos kaip, pavyzdžiui, „Google App Engine“, skirtos interneto programoms kurti ir talpinti dideliu mastu (IBM, 2021);
3. debesies programinė įranga kaip paslauga (angl. *Software as a Service*), pavyzdžiui, „Outlook“, „Hotmail“, „Teams“.

Šiuolaikiniuose darbo santykiuose yra aktyviai naudojami visi šie metodai, tačiau daugiau dėmesio šiame darbe bus skiriama aptariant būtent debesies platformą kaip paslaugą, nes tai yra pirminis ir populiariausias debesų kompiuterijos paslaugų modelis. Tai programinės įrangos licencijavimo modelis, kai programinė įranga suteikiama prenumeratos pagrindu ir yra centralizuotai talpinama (Bania, Geradin, 2023, p. 102). Debesies programinės įrangos kaip paslaugos naudojimas išsaugo įmonės išteklius, nes suteikiama prieiga prie pažangių programų, taip pat apmokamas tik faktinis naudojimas, yra lengvai mobilizuojama darbo jėga ir galima prieiga iš bet kurios vietos, tačiau debesų kompiuterijos modelių naudojimas darbo santykiuose kelia ir tam tikrų iššūkių užtikrinant šios technologijos naudotojų, šio darbo kontekste – darbuotojų teisę į privatumą ir duomenų apsaugą bei kelia tam tikras rizikas darbdaviui, todėl svarbu aptarti teisinius iššūkius debesies platformos kaip paslaugos srityje.

Debesų kompiuterijos naudojimas darbo santykiuose suteikia galimybę darbuotojui pasiekti programas, duomenis iš bet kurio interneto ryšį turinčio įrenginio, tai reiškia, jog darbuotojas darbui gali panaudoti ne darbdavio suteiktą priemonę, o ir asmeninius prietaisus, kurie gali sukelti tam tikrą grėsmę informacijos saugumui, tokios grėsmės atsiradimas yra siejamas su darbdavio rizika pažeisti konfidencialumo įsipareigojimus duotus savo klientams. Darbuotojas, naudodamas savo asmeninius įrenginius ir dalijimosi per debesų kompiuteriją paslaugą, gali nepastebėti, jog darbinė informacija, kuri yra pasiekiama asmeniniame įrenginyje, gali būti persiunčiama į asmeninę debesies talpyklą,

dėl to, kad dalis įrenginių ir naudojamų programėlių automatiškai bendrina informaciją, dėl įrenginyje numatytų nustatymų, taip pat asmeninių prietaisų naudojimas darbo funkcijų atlikimui gali sukelti riziką būtent darbuotojų privatumui, kai darbdavys siekia kontroliuoti darbuotojo veiklą (Vasiliauskienė, 2024). Kai darbuotojui yra suteikiama galimybė naudotis savo priemonėmis, pavyzdžiui, į asmeninį telefoną įdiegti laiškų tikrinimo programą, naudojama darbe, tokiu atveju turinys tampa privačia informacija, kurios darbdavys negali tikrinti, nebent iš anksto darbo santykių šalys susitaria kitaip (Darbuotojų teisė į privatumą: ribos…, 2016). Tai reiškia, jog naudojant asmeninius prietaisus darbo funkcijoms atlikti išsitrina riba tarp privataus gyvenimo ir darbo, o nuo to nukenčia darbdavys, nes atvejais, kai yra įtariama, jog darbuotojas pažeidė įmonės vidines tvarkas ir norima įvykdyti vidinį tyrimą, darbdavį riboja tai, jog įrenginyje yra tiek asmeninio pobūdžio, tiek ir darbo pobūdžio informacija, nes, pavyzdžiui, patikrinus subendrintas asmeninio ir darbo elektroninio pašto žinutes atsiranda didelė rizika pažeisti asmens teisę į privatų gyvenimą (Vasiliauskienė, 2022, p. 49).

Debesų kompiuterijos įrankiai suteikia darbdaviams prieigą prie didelio kiekio darbuotojų duomenų, kurie gali būti naudingi siekiant suprasti ir įvertinti produktyvumą, tokie kontrolės būdai gali apimti:

1. darbuotojo darbalaukio stebėjimą realiuoju laiku;
2. periodinį ekrano nuotraukų darymą;
3. darbo laiko sekimą;
4. pelės paspaudimų kiekio matavimą;
5. įvedamo teksto kiekio ir turinio kontrolę (Navigating employee data privacy in..., 2024).

Vis dėl to mažai tikėtina, kad darbdavys turės tinkamą teisinį pagrindą tokiam darbuotojų stebėjimui, nes tokiomis technologijomis vykdomas duomenų tvarkymas yra neproporcingas (29 straipsnio duomenų apsaugos darbo..., 2017, p. 18). Taip pat rizika gali būti siejama su šio darbo pirmoje dalyje aptartu atveju, kai darbuotojui darbo funkcijas atliekant nuotoliniu būdu vyksta duomenų teikimas į trečiąsias šalis, kuriose negalioja Bendrasis duomenų apsaugos reglamentas (Vasiliauskienė, 2022, p. 49).

Apibendrinant pažymėtina, kad debesų kompiuterija suteikia patogumą ir lankstumą darbo vietoje, tačiau ji kelia ir nemažai teisinių iššūkių, didžiausia problema iškyla tais atvejais, kai darbuotojai naudojasi asmeniniais įrenginiais kartu su šia technologija, nes kyla pavojus, jog informacija susijusi su profesine veikla bus perkelta į asmeninę saugyklą, tokiu atveju darbdavys, rizikuodamas pažeisti darbuotojų teisę į privatumą, nevykdys

asmeninio įrenginio stebėsenos ir praras konfidencialios informacijos kontrolę, negalėdamas garantuoti, kad darbuotojas atsakingai naudojasi debesų kompiuterijos paslaugomis arba, kad taiko tinkamas saugumo priemones.

2.4.5. Biometrinės technologijos

Bendojo duomenų apsaugos reglamento 9 straipsnyje yra numatytas draudimas tvarkyti specialių kategorijų duomenis, tokie duomenys apima informaciją atskleidžiančią rasinę ar etninę kilmę, politines pažiūras, religinius ar filosofinius įsitikinimus ar narystę profesinėse sąjungose, taip pat draudžiama tvarkyti genetinius duomenis, biometrinius duomenis, siekiant konkrečiai nustatyti fizinio asmens tapatybę, sveikatos duomenis arba duomenis apie fizinio asmens lytinį gyvenimą ir lytinę orientaciją. Kiekvienas neteisėtas tokių duomenų atskleidimas gali pažeisti asmenų teisę į privatumą, tačiau šioje dalyje plačiau bus aptariamos biometrinės technologijos, kurių naudojimas darbo santykiuose yra pakankamai dažnas pastarųjų metų reiškinys.

Biometriniai duomenys – po specialaus techninio apdorojimo gauti asmens duomenys, susiję su fizinio asmens fizinėmis, fiziologinėmis arba elgesio savybėmis, pagal kurias galima konkrečiai nustatyti arba patvirtinti to fizinio asmens tapatybę, kaip antai veido atvaizdai arba daktiloskopiniai duomenys (Bendrasis duomenų apsaugos reglamentas 4 straipsnio 14 punktas).

Iš biometrinių duomenų apibrėžties yra matoma, kad šie duomenys yra priskiriami specialiosios kategorijos duomenų grupei tik tada, kai jie yra techniškai apdorojami, o tai reiškia, jog, pavyzdžiui, tvarkant vaizdinę medžiagą, kurioje yra aiškiai matomas asmuo, toks tvarkymas nebus laikomas specialiosios kategorijos duomenų tvarkymu iki tol, kol ji nebus techniškai apdorota, siekiant nustatyti asmens tapatybę, tokiai analizei yra pritariama ir Bendrojo duomenų apsaugos reglamento 51 konstatuojamojoje dalyje (Gairės 05/2020 dėl sutikimo pagal..., 2020, p. 18).

Lietuvos teismų praktikoje yra pavyzdžių, susijusių su biometrinių duomenų, kaip specialios kategorijos duomenų, tvarkymu. Lietuvos Vyriausiasis Administracinis Teismas išnagrinėjo bylą dėl darbuotojų biometrinių duomenų tvarkymo vidaus administravimo tikslu sutikimo pagrindu. Duomenų apsaugos inspekcija atliko tyrimą savo iniciatyva dėl biometrinių asmens duomenų (pirštų antspaudų) tvarkymo teisėtumo patikrinimą Sanatorijoje ir padarė išvadą, jog trys įmonės tvarkė Sanatorijos darbuotojų biometrinius duomenis neturėdamos teisinio pagrindo, numatyto tuo metu galiojusio Asmens duomenų

teisinės apsaugos įstatymo 5 straipsnio 1 dalies 1 punkte, taip pat šio straipsnio 2 – 6 punktuose, taip tvarkydami asmens duomenis neteisėtai, pažeisdamos Asmens duomenų teisinės apsaugos įstatymo 3 straipsnio 1 dalies 2 punktą, tad Duomenų apsaugos inspekcija davė nurodymą nutraukti Sanatorijos darbuotojų biometrinių duomenų tvarkymą ir sunaikinti esančius darbdavio žinioje darbuotojų pirštų antspaudų modelius. Bendrovė apskundė šį nurodymą teismui. Pirmos instancijos teismas panaikino Duomenų apsaugos inspekcijos nurodymą, argumentuodami tuo, kad darbuotojai buvo informuoti apie planuojamą asmens duomenų rinkimą ir tvarkymą, taip pat buvo išaiškinti duomenų rinkimo tikslai, su kuriais darbuotojai sutiko žodžiu bei veiksmais. Duomenų apsaugos inspekcija apskundė šį sprendimą. Teisėjų kolegija nesutiko su pirmosios instancijos teismo išvada, jie teigė, kad darbuotojams nebuvo pateikta informacija apie jų biometrinių duomenų tvarkymą, jų sutikimai nebuvo gauti, nes tyrimo metu Sanatorija neturėjo jokio dokumento, kuriame būtų reglamentuojamas asmens duomenų tvarkymas ir dokumento, patvirtinančio darbuotojų žodinį sutikimą. Taip pat teisėjų kolegija pažymėjo, kad vėlesnis darbuotojų sutikimu pateikimas nekeičia fakto, jog tyrimo metu Sanatorija neturėjo tokio sutikimo, Bendrovė taip pat neįrodė, kad nagrinėjamu atveju laikėsi teisės į privatų gyvenimą ir asmens duomenų apsaugos standartų. Tad buvo padaryta išvada, jog darbdaviai biometrinių duomenų tvarkymo priemones galėtų taikyti siekdami tikslų tik tam tik išskirtinėmis aplinkybėmis, kurios nagrinėjamu atveju nustatytos nebuvo (Lietuvos Vyriausiojo Administracinio Teismo 2020 m. balandžio 2 d sprendimas administracinėje byloje).

Biometrinių duomenų tvarkymas siekiant nustatyti tapatumą, turi būti vykdomas atsakingai, duomenų valdytojas privalo suteikti alternatyvią galimybę, kuri nereikalautų specialios kategorijos duomenų naudojimo ir nesukeltų papildomų apribojimų, išlaidų duomenų subjektui (Gairės 05/2020 dėl sutikimo pagal..., 2020, p. 21). Bendrojo duomenų apsaugos reglamento 9 straipsnio 2 dalis numato teisinius pagrindus, kai tokius duomenis tvarkyti galima, tačiau net ir egzistuojant asmens sutikimui, biometrinių duomenų tvarkymas gali būti nepateisinamas, jei jis neproporcingai riboja asmens teisę į privatumą.

Siekiant užtikrinti fizinio asmens teisę į privatumą ir duomenų apsaugą, reikėtų vengti naudoti biometrinius duomenis. Teisėtvarkoje turi būti aiškiai ir tiksliai reglamentuotas biometrinių duomenų naudojimas ir kaupimas duomenų bazėse, nes saugant biometrinę informaciją skirtingose duomenų bazėse, kyla nekontroliuojamo duomenų panaudojimo rizika dėl duomenų bazių galimo sujungimo ir tai gali sukurti terpę

trečiosioms šalims neteisėtai pasinaudoti tokiais duomenimis, taip pažeidžiant asmenų teisę į privatumą (Poškaitienė, 2022, p. 94).

2.4.6. Dirbtinis intelektas

Šiais laikais egzistuoja technologijos, sudarančios sąlygas globalizuotai saugoti, tvarkyti asmens duomenis ir suteikti plačią prieigą prie duomenų. Tai gali pakenkti teisės į privatumą esmei, todėl jau 2015 metais buvo įsteigta Etikos patariamoji grupė, kurios tikslas – skatinti atvirą informuotų asmenų diskusiją apie skaitmeninę etiką, leisiančią Europos Sąjungai geriau suvokti technologijų naudą visuomenei ir ekonomikai kartu sustiprinant asmenų teises ir laisves, ypač asmenų teises į privatumą ir duomenų apsaugą (Europos Vadovų Taryba, Europos Sąjungos pagrindinių..., 2021, p. 360). Egzistuoja daug inovacijų, tokių kaip daiktų internetas, blokų grandinės ir kitos, tačiau šiame darbe plačiau bus aptariamas dirbtinio intelekto panaudojimas darbo teisiniuose santykiuose ir jo teisinis reguliavimas, taip pat problemos, su kuriomis yra susiduriama panaudojant šią, jau visiems gerai žinomą, technologiją.

Dirbtinis intelektas yra technologijų sritis, apimanti kompiuterinius algoritmus, gebančius skirtingai įgyvendinti užduotis, kurios įprastai reikalauja žmogaus intelekto. Egzistuoja tolesnis dirbtinio intelekto išplėtimas, kuris apima sistemas ir algoritmus, savarankiškai generuojančius turinį, tokiu būdu skatinant veiklos efektyvumą – generatyvus dirbtinis intelektas. Galima išskirti pagrindines generatyvinio dirbtinio intelekto technologijas ir platformas:

1. tekstus generuojantys modeliai;
2. vaizdus generuojantys modeliai;
3. vaizdo įrašus generuojantys modeliai;
4. tekstą analizuojantys modeliai (Generatyvinio dirbtinio intelekto saugaus naudojimo…,2024, p. 2).

Skaitmeninės technologijos gali generuoti daug duomenų susijusių su darbuotojais, kuriuos darbdavys naudotų skirtingiems darbo procesams, pavyzdžiui, įdarbinimui, užduočių paskirstymui, darbo stebėsenai, atliekant tokius veiksmus turi būti užtikrinamas skaidrumas (The digital age: Implications of…, 2021, p. 23). Dėl dirbtinio intelekto galimybės tvarkyti didelį kiekį duomenų ir generuoti duomenis apie konkretų asmenį iškyla tam tikros rizikos.

Dirbtinis intelektas, kaip technologija, yra paremta dideliu kiekiu duomenų naudojimu algoritmų apmokymui, tad kuo daugiau medžiagos jam bus pateikta, tuo tikslesnius ir nešališkesnius atsakymus jis pateiks, tačiau atvejais, kai yra naudojami realūs asmens duomenys, apmokymui reikia turėti teisinį pagrindą, kai dirbtinio intelekto algoritmo apmokymui naudojami jautrūs duomenys, tokie kaip informacija apie asmens sveikatą, lytinę orientaciją, biometriniai duomenys, bus reikalingas asmenų sutikimas. Teisinio pagrindo problemos galima išvengti naudojant nuasmenintus duomenis arba naudojant valstybės turimus išteklius: Registrų centro, meteorologinė ar kita informacija iš valstybės ir savivaldybių resursų (Vasiliauskienė, 2024).

Svarbu yra tai, kad 2024 metais įsigaliojo Europos Parlamento ir Tarybos reglamentas (ES) 2024/1689 kuriuo nustatomos suderintos dirbtinio intelekto taisyklės ir iš dalies keičiami reglamentai (EB) Nr. 300/2008, (ES) Nr. 167/2013, (ES) Nr. 168/2013, (ES) 2018/858, (ES) 2018/1139 ir (ES) 2019/2144 ir direktyvos 2014/90/ES, (ES) 2016/797 ir (ES) 2020/1828 (toliau – Dirbtinio intelekto aktas), kuris visapusiškai bus pradėtas taikyti po dviejų metų, o būtent 2026 metų rugpjūčio 2 dieną. Bendrajame duomenų apsaugos reglamente numatyti teisiniai reikalavimai užkerta kelią pažeidimams, susijusiems su asmens duomenų tvarkymu, tačiau vien tik šio teisės akto egzistavimo nepakanka tam, kad būtų išspręstos problemos, kylančios dėl dirbtinio intelekto sistemų naudojimo. Svarbu, pažymėti, kad Dirbtinio intelekto akte yra numatomi dirbtinio intelekto sistemų rizikos lygiai:

1. nepriimtina rizika (Dirbtinio intelekto aktu yra draudžiamos aštuonios praktikos rūšys, kurių panaudojimas gali kelti grėsmę žmonių saugumui, pragyvenimui ir teisėms);
2. didelė rizika (Dirbtinio intelekto naudojimo atvejai, kurie gali kelti didelę riziką sveikatai, saugai, pagrindinėms teisėms, turi atitikti griežtus reikalavimus ir apimti griežtas pareigas, o tai reiškia, jog tokios sistemos turi būti testuojamos ir naudojamos tik esant žmogaus vykdomai priežiūrai;
3. nedidelė rizika (reikalaujama skaidrumo principo užtikrinimo, kad naudotojas žinotų, jog sistemų turinys sugeneruotas dirbtinio intelekto).

Dirbtinio intelekto akte nėra nustatytos taisyklės dėl dirbtinio intelekto, keliančio minimalią riziką ar išvis jos nekeliančios, tai apima dirbtiniu intelektu grindžiamus žaidimus, brukalo filtrus (Regulatory Framework for AI, 2024).

Šiuo aktu yra nustatomos taisyklės dirbtinio intelekto technologijų tiekėjams ir diegėjams. Daugiau dėmesio reikėtų skirti būtent šių technologijų tiekėjams, kurie kuria

dirbtinio intelekto sistemą arba bendrosios paskirties dirbtinio intelekto modelį arba nurodo kurti sistemą arba bendrosios paskirties modelį ir pateikia juos rinkai, nes asmenys, kuriantys tokias sistemas turi pakankamai kompetencijos suvokti ir įvertinti keliamas rizikas, tuo tarpu ne visi diegėjai naudojantys dirbtinio intelekto sistemą gali tinkamai įvertinti rizikas ir suprasti netinkamo šios technologijos panaudojimo padarinius, o tokių technologijų neteisėtas panaudojimas gali sukelti žalą ir atsakomybę ją netinkamai naudojusiems asmenims.

2025 metų vasario 2 dieną buvo pradėtas taikyti Dirbtinio intelekto aktas. Sistemų tiekėjams ir naudotojams, pagal šio akto 4 dalį, atsirado pareiga imtis priemonių užtikrinti pakankamą dirbtinio intelekto raštingumo lygį tarp darbuotojų ir kitų asmenų, naudojančių šią technologiją, tai reiškia, jog įmonėms atsiranda įpareigojimas įdiegti mokymus, skirtus supažindinti darbuotojus su dirbtinio intelekto veikimu, pavojais, reguliaciniais reikalavimais (Šapkauskaitė, 2025). Lietuvoje verslo įmonės yra parengusios Generatyvinio dirbtinio intelekto saugaus naudojimo organizacijoje gaires, kurių tikslas yra rekomendacijų dėl šių technologijų naudojimo, akcentuojant informacijos saugumą verslo sričiai pateikimas ir struktūros, kuri padėtų efektyviai ir saugiai integruoti šias technologijas į įmonės veiklą, stiprinant jos konkurencingumą ir inovacijų potencialą. Gairėse yra išskiriami tam tikri saugumo aspektai. Jų teigimu saugumas organizacijoje priklauso nuo aiškiai paskirstytos atsakomybės ir vadovų supratimo apie galimas rizikas ir naudą. Svarbu aptikti įgūdžių spragas ir įtraukti specialistus į sprendimų priėmimą, organizacija iš anksto turėtų įvertinti galimus incidentus, turėti aiškų reagavimo planą, užtikrinantį efektyvų saugumo pažeidimų planą, taip pat kiekvienu atveju, kai norima tvarkyti duomenis apie asmenis dirbtinio intelekto sistemų pagalba, būtina atlikti poveikių duomenų apsaugai vertinimą (Generatyvinio dirbtinio intelekto saugaus naudojimo…,2024, p. 1). Europos Sąjungos lygmeniu yra įsteigti keli valdymo organai, kurie turėtų užtikrinti tinkamą Dirbtinio intelekto akto vykdymą: Dirbtinio intelekto tarnyba Europos Komisijoje, nepriklausomų ekspertų mokslinė komisija, Dirbtinio intelekto valdyba, suinteresuotų subjektų patariamasis forumas (Regulatory Framework for AI, 2024), tačiau šio darbo nagrinėjimo metu dar nėra pateikta gerosios praktikos, praktinių pavyzdžių susijusių su šio teisės akto taikymu.

Europos Parlamentas yra pabrėžęs, kad naujų technologinių galimybių, pavyzdžiui, dirbtinio intelekto, pažanga atlieka lemiamą vaidmenį formuojant ateities darbo vietą ir vertinant darbo našumą, tokios technologijos neturėtų lemti dehumanizuoto skaitmeninių priemonių naudojimo ar kelti susirūpinimą dėl privatumo ir neproporcingo bei neteisėto

asmens duomenų rinkimo, darbuotojų stebėjimo ir stebėsenos (Data subjects, digital surveillance, AI…, 2020, p. 96). Dirbtinio intelekto naudojimas vykdant darbuotojų stebėjimą atveria naujų galimybių darbdaviams kontroliuoti darbuotojus ir jų darbo aplinką intensyviau nei kada nors iki šiol (Mole, 2022 cituota Breskienė, 2024, p. 109-110).

Dirbtinio intelekto sistemų panaudojimo pavyzdys yra algoritminis valdymas – įvairios technologinės priemonės ir metodai, kuriais struktūrizuojamos darbo sąlygos ir nuotoliniu būdu valdoma darbo jėga. Algoritminio valdymo sistemų atsiradimas darbo vietoje pasižymi nukrypimu nuo ankstesnių valdymo struktūrų, kuriose vadovavimas darbuotojams labiau priklausė nuo žmonių vadovų. Algoritminis valdymas leidžia didinti veiklos mastą, pavyzdžiui, koordinuojant didelių, išskaidytų darbuotojų grupių veiklą arba naudojant duomenis, kad būtų galima optimizuoti pageidaujamus rezultatus, pavyzdžiui, mažesnes darbo sąnaudas. (Mateescu, Nguyen, 2019, p. 3). I. Breskienės teigimu, toks darbuotojų stebėsenos būdas yra priskiriamas didelės rizikos lygiui, todėl darbdaviui, naudojančiam šią sistemą yra numatomi griežti reikalavimai, jos įgyvendinimas gali vykti tik tuo atveju, jei yra paskirtas kvalifikuotas asmuo, kurio žinių pakaktų užtikrinti tinkamą šios sistemos naudojimą, gebantis interpretuoti generuojamus išvedinius, atitinkamai elgtis su gautais rezultatais, taip pat suvokiantis atvejus, kai algoritminio valdymo, ar jo metu sukurto rezultato naudoti nereikia. Darbdavys turėtų pateikti informaciją darbuotojui apie vykdomą stebėjimą, įtvirtinti ir detalizuoti darbovietės vidaus teisės aktuose darbuotojo stebėjimo mastą, teisėtas stebėjimo priežastis, pagrįsti algoritminio valdymo, veikiančio dirbtinio intelekto sistemų pagrindu, naudojimą darbuotojams stebėti kaip vienintelės tam atvejui tinkamos priemonės, detalizuoti stebėjimo padarinius, įvardyti kam bus naudojami stebėjimo rezultatai, taip pat įvardinti ir apsaugos priemones taikomas darbuotojams dėl atliekamo jų stebėjimo (Breskienė, 2024, p. 113-114).

Teisė į privatumą yra esminė vertybė, kurią būtina apsaugoti vis aktyviau taikant inovatyvias technologijas darbo teisiniuose santykiuose. Dirbtinio intelekto aktas nustato sistemų naudojimo reikalavimus ir taisykles, tačiau, reikia laiko, kad būtų išgrynintas praktinis šio reglamento taikymas, o būtent dėl nepakankamai suformuotos praktikos šioje srityje ir galimo skirtingo taisyklių interpretavimo šiuo metu sunku užtikrinti veiksmingą dirbtinio intelekto technologijų panaudojimo kontrolę ir prevenciją nuo galimo piktnaudžiavimo. Modernių technologijų, įskaitant dirbtinio intelekto naudojimas darbo santykiuose, suteikia galimybę darbdaviams naujais būdais kontroliuoti darbuotojus, tačiau tokių priemonių gausa taip pat sukuria daug erdvės pažeisti darbuotojų teises, todėl kitoje

dalyje bus aptariami iššūkiai su kuriais susiduria darbo santykių subjektai, realizuodami savo teises ir siekdami numatytų tikslų.

3. IŠŠŪKIAI DARBUOTOJŲ PRIVATUMO APSAUGOS SRITYJE

Teisę į privatumą galima suprasti plačiai ir kiekvienu atveju reikia įvertinti visas aplinkybes tam, kad tinkamai pritaikytume šį institutą. Modernių technologijų naudojimas darbo vietoje užtikrina sklandesnį darbo funkcijų atlikimą ir suteikia daugiau galimybių tiek darbuotojui, atliekant jam pavestas užduotis, tiek ir darbdaviui kontroliuojant jų darbo efektyvumą, tačiau reikia suvokti, kokios yra tokio pobūdžio kontrolės ribos ir ar yra atvejų, kai darbuotojo teisė į privatumą gali būti apribojama.

3.1. Darbuotojo teisė į privatumą ir darbdavio teisėti interesai

Kiekvienas asmuo turi teisę į privatumą, ši teisė yra užtikrinama tarptautiniais ir nacionaliniais teisės aktais, taip pat pagrindiniu įstatymu – Lietuvos Respublikos Konstitucija. Lietuvos Respublikos Konstitucinis Teismas yra nustatęs sąlygas, kurioms egzistuojant galima apriboti konstitucines teises ir laisves, o būtent atvejais, kai:

1. tai daroma įstatymu;
2. ribojimai yra būtini demokratinėje visuomenėje siekiant apsaugoti teises ir laisves bei Konstitucijoje įtvirtintas vertybes;
3. siekiant konstituciškai svarbių tikslų;
4. apribojimais nepaneigiama teisių ir laisvių prigimtis ir esmė;
5. nepažeidžiamas konstitucinis proporcingumo principas (Lietuvos Respublikos Konstitucinio Teismo 2002 m. spalio 23 d. nutarimas).

Taip pat Žmogaus teisių konvencijos 8 straipsnio 2 dalyje yra numatytos situacijos, kai gali būti apribojama teisė į privataus ir šeimos gyvenimo gerbimą: kai tai būtina demokratinėje visuomenėje valstybės saugumo, visuomenės saugos ar šalies ekonominės gerovės interesams, siekiant užkirsti kelią viešos tvarkos pažeidimams ar nusikaltimams, taip pat žmonių sveikatai ar moralei arba kitų asmenų teisėms ir laisvėms apsaugoti.

Tad yra suprantama, jog teisė į privatumą gali būti ribojama tada, kai ji yra nesuderinama su kitomis teisėmis ir teisėtais interesais. Lietuvos Respublikos įstatymuose yra numatyti atskiri atvejai, kai teisė į privatumą gali būti ribojama, pavyzdžiui, Lietuvos Respublikos kriminalinės žvalgybos įstatyme numatytos kriminalinės žvalgybos subjektų teisės, tarp kurių yra teisė specialia tvarka panaudoti technines priemones, atlikti slaptą siuntų, dokumentų apžiūrą, kontrolę, paėmimą, taip pat vykdyti susirašinėjimo ir kitokio susižinojimo slaptą kontrolę, įstatymų nustatyta tvarka apribojant žmogaus teisę į privataus

gyvenimo neliečiamumą (Lietuvos Respublikos kriminalinės žvalgybos įstatymas, 2012), taip pat Lietuvos Respublikos baudžiamojo proceso kodekse numatoma, jog kiekvienas asmuo turi teisę, kad būtų gerbiamas jo ir jo šeimos privatus gyvenimas, taip pat teisę į būsto neliečiamybę, susirašinėjimo, telefoninių pokalbių, telegrafo pranešimų ir kitokio susižinojimo slaptumą, tačiau šios asmens teisės baudžiamojo proceso metu gali būti apribotos baudžiamojo proceso kodekso numatytais atvejais ir tvarka (Lietuvos Respublikos baudžiamojo proceso kodeksas, 2002).

Darbo santykių kontekste svarbu pažymėti tai, jog darbdavys turi teisėtą interesą veikti efektyviai. Taip pat jis siekia išvengti žalos, atsakomybės, kuri gali atsirasti darbuotojui netinkamai atliekant savo darbo funkcijas ar kitus veiksmus, todėl darbdavys imasi priemonių, norėdamas kontroliuoti darbuotoją. Svarbu aptarti kokius interesus bando apsaugoti darbdavys, vykdydamas tokio pobūdžio kontrolę. Išskiriamos šios priežastys:

1. darbo drausmės užtikrinimas;
2. dalykinės reputacijos apsauga;
3. darbuotojų efektyvumo ir produktyvumo didinimas;
4. finansinių išteklių taupymas;
5. kompiuterių sistemos saugumo ir našumo poreikių tenkinimas (Bagdanskis, Sartatavičius, 2012, p. 199).

Anksčiau šiame darbe buvo aptarta nuotolinio darbo organizavimo forma, kuri sukelia tam tikrų sunkumų darbdavio teisėtų interesų ir kontrolės užtikrinimo srityje, tad svarbu pažymėti, jog Duomenų apsaugos inspekcija yra pateikusi rekomendacijas, kuriose numatoma kaip reikėtų užtikrinti tinkamą darbuotojų duomenų tvarkymą asmeniui dirbant neįprastoje darbo vietoje. Darbdavys turėtų įvertinti darbuotojo stebėsenos proporcingumą siekiamiems tikslams, atlikti poveikio duomenų apsaugai vertinimą, parengti stebėsenos taisykles ir supažindinti su jomis darbuotojus, svarbu, kad darbdavys turi turėti įrodantį faktą, jog darbuotojai tikrai buvo supažindinti su pateiktomis taisyklėmis, kitokiu atveju, atsiradus ginčui dėl duomenų tvarkymo, darbdaviui bus sunku įrodyti tai, jog darbuotojas tikrai davė sutikimą vykdyti tokio pobūdžio kontrolę. Atsiradus bet kokiam duomenų tvarkymo veiklos papildymui darbdavys privalo parengti privatumo pranešimą arba atnaujinti jau turimą privatumo pranešimą ir aiškiai identifikuoti kas yra keičiama (Darbuotojų asmens duomenų tvarkymas, organizuojant…, 2020, p. 2-3).

Darbdavys turėtų apsvarstyti prevencinių priemonių taikymą, pavyzdžiui, asmens duomenų, susijusių su darbuotojo lankomais interneto ar intraneto puslapiais, filtrus, prieš pradedant taikyti labiau teisę į privatumą galinčias apriboti priemones arba įrengti

prietaisus, tačiau gali būti atvejų, kai įgyvendinti prevencines priemones nėra įmanoma, svarbu, kad bet kuriuo atveju darbdavys užtikrintų, kad jų vykdomos stebėsenos politika būtų aiški ir skaidri, atitiktų nacionalinę teisę, taip pat privalumas būtų, jei taisyklės būtų rengiamos vykdant konsultaciją su socialiniais partneriais, darbuotojais (Komanovics, 2023, p. 466).

Tad tam, kad būtų užtikrintas balansas tarp darbdavio interesų ir darbuotojų teisių, įskaitant teisę į privatumą, darbdavys turi apibrėžti aiškias taisykles, susijusias su suteiktų priemonių ir įrankių panaudojimu tik darbo tikslais, tokios taisyklės gali būti įtvirtintos darbo tvarką reglamentuojančiuose vidiniuose įmonės aktuose. Būtina nustatyti aiškias vykdomos kontrolės taisykles – darbuotojui suteikti informaciją apie vykdomą tikrinimą, jo apimtį, tikslus, papildomai numatant tikrinamos informacijos saugojimo tvarką. Darbuotojai privalo suvokti, kokiais būdais darbdavys vykdo darbuotojų kontrolę, todėl geriausia yra tokią informaciją suteikti pasirašytinai, kad kilus ginčui, darbdavys turėtų įrodymą, jog jis teisėtai siekė savo interesų (Prof. dr. Mindaugas Kiškis. Ką…, 2016).

Atsižvelgiant į apibrėžtus teisėtus interesus, kuriuos bando apsaugoti darbdavys vykdydamas darbuotojo kontrolę, atrodo, kad darbdaviui yra pakankamai lengva apriboti darbuotojo teisę į privatumą, tačiau veiksmų, kuriuos turi atlikti darbdavys, norėdamas vykdyti teisėtą darbuotojų kontrolę, gausa, įrodo, jog šis procesas yra sudėtingas, reikalaujantis teisės aktuose įtvirtintų nuostatų tinkamo suvokimo.

3.2. Darbdavio interesų ir darbuotojų teisės į privatumą derinimas

Pagrindiniai duomenų tvarkymo principai

Kiekvienu darbo santykių etapu yra tvarkomi asmenų duomenys, tai gali apimti tokius veiksmus kaip darbuotojų asmens bylų tvarkymas, dokumentų archyvavimas, atostogų, laisvadienių, komandiruočių organizavimas, mokymai ir kvalifikacijos kėlimas, skundų nagrinėjimas, veiklos vertinimas, užduočių vykdymas, susirašinėjimas, darbuotojų veikla, naudojantis darbdavio įrenginiais ir kitais elektroniniais resursais ir panašiai (Gairės smulkiajam ir vidutiniam verslui, 2023, p. 6). Darbdavys, bandantis užtikrinti savo interesus, imasi veiksmų, kurie padeda kontroliuoti darbuotojus.

Tam, kad pasitelkiant tokią kontrolę nebūtų pažeidžiamos darbuotojo teisės, įskaitant ir teisę į privatumą, Bendrajame duomenų apsaugos reglamente yra numatyti tam tikri principai, apsaugantys asmenis nuo tokio pobūdžio pažeidimų. Bendrojo duomenų

apsaugos reglamento 5 straipsnio 1 dalies a punkte numatyta, kad asmens duomenys turi būti tvarkomi teisėtu, sąžiningu ir skaidriu būdu, tai reiškia, jog bet koks duomenų tvarkymas turi būti vykdomas tik tada, kai juo siekiama teisėto tikslo ir darbuotojas, kurio duomenys yra tvarkomi, turi būti detaliai informuotas apie tai, kokiais atvejais bus renkami jo duomenys, renkamų duomenų apimtis ir tikslai. Tad antrasis principas, numatytas minėtame straipsnyje – tikslo apribojimo principas, kuris reiškia, jog duomenys renkami teisėtais ir aiškiai apibrėžtais tikslais ir toliau netvarkomi su tais tikslais nesuderinamu būdu, norint naudoti duomenis apie darbuotoją keliais skirtingais tikslais, tai turi būti iškarto apibrėžta. Kitas principas – duomenų kiekio mažinimo, reiškiantis tai, kad duomenys turi būti adekvatūs, tinkami ir tik tokie, kurių reikia siekiant tikslų, dėl kurių jie yra tvarkomi. Straipsnyje minimas ir saugojimo trukmės apribojimo principas, kuriuo užtikrinama, kad duomenų subjektų tapatybę būtų galima nustatyti ne ilgiau, nei tai yra būtina tais tikslais, kuriais asmens duomenys yra tvarkomi. Vientisumo ir konfidencialumo principas reiškia tai, kad duomenys turi būti tvarkomi tokiu būdu, kad taikant atitinkamas technines, organizacines priemones būtų užtikrintas tinkamas duomenų saugumas, tai apima apsaugą nuo duomenų tvarkymo be leidimo, neteisėto tvarkymo, jų praradimo, sunaikinimo ar sugadinimo.

Bendrasis duomenų apsaugos reglamentas numato bendruosius principus, tokius kaip atskaitomybės, skaidrumo, sąžiningumo, teisėtumo principai, jie užtikrina tinkamą asmens duomenų apsaugą ir naujausių technologijų kontekste (Philippe Renaudiere: BDAR kurtas praeities…, 2018). Paminėtina naujausia byla, kurioje yra atskleidžiama Bendrajame duomenų apsaugos reglamente pateiktų principų reikšmė ir jų nesilaikymo pasekmės. 2025 metų kovo 26 dieną Lietuvos Vyriausiasis administracinis teismas išnagrinėjo ginčą dėl Valstybinės duomenų apsaugos inspekcijos skirtos baudos Viešojo valdymo agentūrai (toliau – pareiškėjas, Agentūra) už Bendrojo duomenų apsaugos reglamento 5 straipsnio 1 dalies a ir f punktų pažeidimą. J. R. (toliau – duomenų subjektas) pateikė skundą Valstybinei duomenų apsaugos inspekcijai, kuriame nurodė, jog Agentūros Specialistė be teisinio pagrindo, ne darbo metu, 7 kartus peržiūrėjo jos asmens duomenis VATARAS sistemoje ir galimai šie duomenys buvo nutekinti. Pareiškėjas, tuo tarpu, buvo parengęs tarnybinio tyrimo išvadą, kurioje nurodyta**,** jog jų darbuotoja neturėjo nei teisinio, nei faktinio pagrindo tvarkyti duomenų subjekto asmens duomenis VATARAS, todėl Specialistei buvo paskirta tarnybinė nuobauda – papeikimas. Taip pat buvo nurodyta, jog 4 darbuotojai turėjo teisę peržiūrėti duomenų subjekto asmens duomenis, nes tai buvo susiję su jų vykdomomis funkcijomis, kiti norėjo sužinoti jos gimimo datą, o duomenys nebuvo

perduoti tretiesiems asmenims. Ginčo nagrinėjimo metu buvo išsiaiškinta, jog duomenų subjekto duomenų peržiūra vyko 244 kartus. Šiuo atveju buvo pažeistas duomenų subjekto asmens duomenų saugumas, pažeidimas atitiko Bendrojo duomenų apsaugos reglamento 4 straipsnyje numatytą asmens duomenų saugumo pažeidimo apibrėžimą. Darbuotojai, peržiūrėję duomenų subjekto asmens duomenis, susipažino su labai dideliu informacijos kiekiu apie jos privatų gyvenimą. Beveik 2 metus Agentūra duomenų subjekto asmens duomenis VATARAS tvarkė, pažeisdama teisę į duomenų apsaugą. Sistemingas asmens duomenų tvarkymo pažeidimas užkirto kelią duomenų subjektui kontroliuoti savo asmens duomenis, paneigė jo teisę į Lietuvos Respublikos Konstitucijoje įtvirtiną privatų gyvenimą, o Agentūros atliktas vidaus tyrimas tik patvirtino, jog buvo pažeistos duomenų subjekto teisės ir teisėti lūkesčiai į tinkamą ir teisėtą jo asmens duomenų tvarkymą (Lietuvos Vyriausiojo Administracinio Teismo 2025 m. kovo 26 d. nutartis administracinėje byloje).

Svarbu tai, jog toks didelis kiekis tvarkomų duomenų lemia būtinumą nustatyti darbuotojams, kaip duomenų subjektams, teises, kurios taip pat yra apibrėžtos skirtingose Bendrojo duomenų apsaugos reglamento straipsniuose. Šios teisės yra:

1. teisė būti informuotam, kuri reiškia, jog kiekvienu atveju, kai duomenų valdytojas gauna duomenis tiek iš duomenų subjekto, tiek ir ne iš jo, duomenų subjektui turi būti pateikta tam tikra teisės akte numatyta informacija;
2. teisė susipažinti su savo asmens duomenimis, kuri garantuoja duomenų subjektui galimybę gauti patvirtinimą iš duomenų valdytojo, ar su juo susiję duomenys yra tvarkomi ir jeigu yra, susipažinti su duomenimis ir kita informacija;
3. teisė reikalauti ištaisyti netikslius su juo susijusius duomenis arba reikalauti papildyti neišsamius duomenis;
4. teisė reikalauti ištrinti duomenis;
5. teisė apriboti duomenų tvarkymą;
6. teisė gauti informaciją apie duomenų gavėjus;
7. teisė į duomenų perkeliamumą;
8. teisė nesutikti, kad su juo susiję asmens duomenys būtų tvarkomi, kai toks duomenų tvarkymas vykdomas pagal 6 straipsnio 1 dalies e arba f punktus, įskaitant profiliavimą remiantis tomis nuostatomis;
9. teisė reikalauti, kad duomenų subjektui nebūtų taikomas tik automatizuotu duomenų tvarkymu, įskaitant profiliavimą, grindžiamas sprendimas (Bendrasis duomenų apsaugos reglamentas 13 – 22 straipsniai).

Galima teigti, jog apribojant informacijos, kurią gali rinkti darbdavys, kiekį ir nustatant taisykles, kaip ir kokia informacija gali būti renkama, o taip pat suteikiant duomenų subjektui teisę kontroliuoti su jo asmeniu susijusių duomenų tvarkymą yra skatinamas atsakingas duomenų valdymas, mažinama pažeidimų, įskaitant ir darbuotojų teisės į privatumą, rizika ir kuriama saugi darbo aplinka.

Poveikio duomenų apsaugai vertinimas ir teisėtų interesų pusiausvyros testas

Darbdavys privalo atsakingai vertinti duomenų tvarkymo veiklos poveikį, siekdamas užtikrinti darbuotojų pagrindines teises ir laisves, įskaitant teisę į privatumą. Šiam tikslui pasiekti reikia teisės aktuose numatytas taisykles pritaikyti praktikoje, todėl yra pasitelkiami specialūs vertinimo mechanizmai padedantys rasti pusiausvyrą tarp darbdavio interesų ir darbuotojų teisių apsaugos.

Kai dėl duomenų tvarkymo gali kilti didelis pavojus asmenų teisėms ir laisvėms yra atliekamas atitikties užtikrinimo ir įrodymo procesas, kuris vadinamas poveikio duomenų apsaugai vertinimu (Kada reikia atlikti poveikio duomenų…). Ši procedūra ir mechanizmas yra įtvirtinti Bendrojo duomenų apsaugos reglamento 35 straipsnyje. Šio Reglamento konstatuojamosiose dalyse yra nurodoma, jog toks vertinimas turi būti atliekamas visų pirma tada, kai atliekamos didelio masto duomenų tvarkymo operacijos, kuriomis siekiama regioniniu, nacionaliniu, viršnacionaliniu lygmeniu tvarkyti didelį kiekį asmens duomenų, kurie galėtų daryti poveikį daugeliui duomenų subjektų ir kelti pavojų dėl savo turinio. Pažymima, kad toks vertinimas turi būti atliekamas, kai asmens duomenys yra tvarkomi priimant sprendimus dėl konkrečių fizinių asmenų, atlikus plataus masto asmeninių aspektų vertinimą, remiantis duomenų profiliavimu, atlikus specialių kategorijų, biometrinių duomenų ar duomenų apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas ar susijusias saugumo priemones tvarkymą, taip pat poveikio duomenų apsaugai vertinimas atliekamas sistemingai stebint viešąsias erdves dideliu mastu. 35 straipsnio 7 dalyje yra pateikiamas minimalus sąrašas to, ką turi pateikti duomenų valdytojas įvertinime, o būtent:

1. pateikiamas sistemingas numatytų duomenų tvarkymo operacijų aprašymas ir duomenų tvarkymo tikslai, įskaitant, kai taikoma, teisėtus interesus, kurių siekia duomenų valdytojas;
2. duomenų tvarkymo operacijų reikalingumo ir proporcingumo, palyginti su tikslais, vertinimas;
3. duomenų subjektų teisėms ir laisvėms kylančių pavojų vertinimas;

4. priemonės, numatytos pavojams šalinti, įskaitant apsaugos, saugumo priemones ir mechanizmus, kuriais yra užtikrinama asmens duomenų apsauga ir įrodoma, kad yra laikomasi Bendrojo duomenų apsaugos reglamento, atsižvelgiant į duomenų subjektų ir kitų susijusių asmenų teises ir laisves.

Svarbu atkreipti dėmesį, kad Poveikio duomenų apsaugai vertinimo operacijos neturėtų būti nurodomos formaliai, operacijas reikia išskirti, jas paaiškinti. Taip pat vykdant šį vertinimą turi būti pateikta duomenų apsaugos eksperto, dar vadinamo duomenų apsaugos pareigūnų, nuomonė, kuri taip pat turi būti pagrįsta, nurodant tikslius argumentus dėl operacijos reikalavimų atitikimo ar neatitikimo (Poveikio duomenų apsaugai vertinimas. 10…, p. 14).

Teisėtų interesų pusiausvyros testas, kitaip dar vadinamas balanso testu, yra atliekamas siekiant įvertinti, ar duomenų valdytojo interesas yra viršesnis už duomenų subjekto pagrindines teises ar laisves. Tad šis testas yra atliekamas siekiant įsitikinti, jog duomenų tvarkymas atitinka Bendrojo duomenų apsaugos reglamento 6 straipsnio 1 dalies f punkte nustatytą teisinį pagrindą (duomenų tvarkymas yra būtinas siekiant teisėto intereso). Prieš pradedant tvarkyti asmens duomenis duomenų valdytojai turėtų kiekvienu konkrečiu atveju įvertinti, ar numatomas tvarkymas atitinka tris sąlygas:

1. duomenų tvarkymo tikslą;
2. būtinumą;
3. teisėto intereso viršenybę prieš duomenų subjektų apsaugą (Teisėto intereso taikymo ir balanso…, 2023).

Taip pat turi būti įvertinta ar siekiamo tikslo negalima užtikrinti kitomis priemonėmis, mažiau ribojančiomis duomenų subjektų pagrindines laisves ir teises, visų pirma teisę į privataus gyvenimo gerbimą ir teisę į asmens duomenų apsaugą. Be to, siekiant įsitikinti, kad teisėtų interesų pusiausvyros testas įvykdytas tinkamai, duomenų valdytojams gali tekti įgyvendinti tinkamas apsaugos priemones, pavyzdžiui, naudoti privatumą didinančias technologijas (EDAV duomenų apsaugos vadovas smulkiajam…, 2024, p. 32).

Apibendrinant galima teigti, jog darbuotojo teisė į privatumą nugali darbdavio interesą siekti efektyvumo, o darbdavio vykdomą kontrolę apsunkina tai, jog vis dar trūksta išsamaus privatumo teisinio reguliavimo, ypač inovatyvių technologijų panaudojimo kontekste. Tokie vertinimo mechanizmai, kaip poveikio duomenų apsaugai vertinimas ir teisėtų interesų pusiausvyros testas, padeda sumažinti darbdavio pažeidimų riziką, tačiau jie visiškai nepašalina egzistuojančios rizikos, tad akivaizdu, jog šioje srityje vis dar reikia tobulinti teisinį reglamentavimą.

4. ATSAKOMYBĖ UŽ PAŽEIDIMUS

Pavojus privatumui yra susijęs su dideliais renkamų duomenų apie darbuotojus kiekiais ir algoritminiu atskaitingumu darbo pasaulyje (International Labour Organization, 2022). Netinkamas modernių technologijų naudojimas darbo vietoje gali sukelti rimtas pasekmes, tai apima atsakomybę už darbo drausmės pažeidimus, darbo sutarčių nutraukimą, konfidencialios ir komercinės paslapties sudarančios informacijos, dalykinės reputacijos praradimą, papildomas išlaidas dėl teisinių ginčų, kylančių dėl asmens privatumo pažeidimų ir kita. Technologijų naudojimas, kuriuo yra pažeidžiama teisės aktuose nustatyta arba darbo santykių subjektų sulygta naudojimosi tvarka lemia teisinės atsakomybės taikymą, ne tik pagal darbo teisę, bet ir pagal kitose teisės šakose numatytas teisinės atsakomybės rūšis (Weatherbee, 2010, p. 35-36).

Darbo kodekso 24 straipsnyje įtvirtinti sąžiningumo ir bendradarbiavimo principai. Pabrėžiama, jog darbo teisių įgyvendinimas ir pareigų vykdymas neturi pažeisti kitų asmenų teisių ir teisėtų interesų, darbo priemonės turi būti naudojamos pagal paskirtį, turi būti vengiama interesų konflikto ir siekiama darbo santykių darnaus vystymosi. Pažeidus šias pareigas, kita šalis turi teisę į žalos atlyginimą ar kitokią pažeistų teisių gynybą. 151 straipsnyje yra numatyta, kad kiekviena darbo sutarties šalis privalo atlyginti kitai sutarties šaliai padarytą turtinę ir neturtinę žalą, kai žala padaryta savo darbo pareigų pažeidimu dėl jos kaltės. Darbo kodekso 153 straipsnyje yra numatomos darbuotojo atlygintinos žalos ribos, o 154 straipsnyje įvardijami atvejai, kai turi būti atlygintina visa žala, tokie atvejai apima:

1. žalą padarytą tyčia;
2. žalą padarytą veikla, turinčia nusikaltimo požymių;
3. žalą padarytą neblaivaus ar apsvaigusio nuo narkotinių, toksinių ar psichotropinių medžiagų darbuotojo;
4. žalą padarytą pažeidus pareigą saugoti konfidencialią informaciją, susitarimą dėl nekonkuravimo;
5. darbdaviui padarytą neturtinę žalą;
6. kai visiškas žalos atlyginimas yra numatytas kolektyvinėje sutartyje.

Svarbus yra ir minėto kodekso 20 straipsnis, kuriame numatoma, jog atsakomybė už šiame kodekse nustatytų pareigų nevykdymą ar netinkamą vykdymą gali nustatyti ne tik Darbo kodeksas, bet ir kiti įstatymai, teisės normos, darbo santykių dalyvių sutartys ir susitarimai. Tad atsakomybė už asmens privataus gyvenimo neliečiamumo pažeidimus yra

numatyta ir Lietuvos Respublikos baudžiamajame kodekse, kuriame reglamentuojama, jog už neteisėtą susirašinėjimo, kitokių pranešimų, siuntų ar pokalbių telefonu slaptumo pažeidimus, neteisėtą informacijos apie privatų asmens gyvenimą rinkimą, neteisėtos informacijos apie asmens privatų gyvenimą atskleidimą ar panaudojimą yra baudžiami tiek fiziniai, tiek ir juridiniai asmenys.

Pažymėtina, kad mokslininkai siūlo taikyti *respondeat superior* doktriną, kuri nustato, kad darbdaviai yra atsakingi už savo darbuotojų veiksmus, net ir tuo atveju, kai darbdavys nepatvirtino atliekamų veiksmų ir net jei vykdė tinkama darbuotojų priežiūrą ir kontrolę. Pagal šią doktriną, jei darbuotojas darbe padaro neteisėtą veiką ir ji buvo padaryta vykdant darbo funkcijas, darbdavys yra atsakingas nukentėjusiajam už darbuotojo veiksmus (Understanding the theory of respondeat...2021).

Asmens duomenų tvarkymo kontekste svarbu paminėti, kad nacionalinėje teisėje nėra teisės normų atskirai reguliuojančių būtent darbuotojų duomenų tvarkymą, tad atkreiptinas dėmesys į Administracinių nusižengimų kodeksą, o būtent 83 straipsnį, kuriame numatyta, jog už duomenų tvarkymo ir privatumo pažeidimus, numatytus Lietuvos Respublikos elektroninių ryšių įstatyme yra skiriama bauda. Asmens duomenų teisinės apsaugos įstatyme yra apibrėžta, kad už pažeidimus tvarkant asmens duomenis *mutatis mutandis* taikomos Bendrojo duomenų apsaugos reglamento 58 straipsnio 2 dalyje nurodytos priemonės, įskaitant administracinės baudos skyrimą, o reglamento 129 konstatuojamojoje dalyje numatyta, jog siekdamos užtikrinti vienodą Bendrojo duomenų apsaugos reglamento taikymo stebėseną ir vykdymą visoje Europos Sąjungoje, priežiūros institucijos kiekvienoje valstybės narėje turi vienodus įgaliojimus, jos gali nustatyti duomenų tvarkymo apribojimus, kreiptis į teismą dėl reglamento pažeidimų, taip pat tokie veiksmai turi atitikti nacionalinės teisės reikalavimus, užtikrinti veiksmingą teisinę gynybą.

Tad jau išnagrinėta tai, jog už turtinės ir neturtinės žalos sukėlimą atsakomybė yra numatyta Darbo kodekse, atsakomybė susijusi su netinkamu duomenų tvarkymu yra reguliuojama administracinės teisės, tuo tarpu atvejais, kai privatumo pažeidimas turi nusikalstamos veikos požymių – atsakomybė kyla ir pagal baudžiamosios teisės nuostatas, tačiau pažymėtina, jog baudžiamajame įstatyme nėra detalizuojama privataus gyvenimo sąvoka, taigi kaip jau išsiaiškinome šiame darbe, minėta sąvoka suprantama plačiai, todėl kiekvienu konkrečiu atveju teismas, įvertinęs bylos aplinkybes turi spręsti ar neteisėtas darbuotojo asmens duomenis sudarančios informacijos tvarkymas bus laikomas tik asmens duomenų apsaugos kategorija, atitinkamai taikant administracinę teisinę atsakomybę, ar

bus pripažįstamas neteisėtu informacijos apie darbuotoją tvarkymu, kai pažeistos teisės ginamos Baudžiamojo kodekso nuostatomis (Tamašauskaitė-Janickė, 2016, p. 122).

Anksčiau galiojusioje Darbo kodekso redakcijoje (redakcija nuo 2003 metų iki 2016 metų), o būtent 17 skyriuje, buvo nustatytas materialinės atsakomybės teisinis reguliavimas ir atvejai, kai yra taikoma civilinės teisės normos. (Tamašauskaitė-Janickė, 2016, p. 200). 246 straipsnyje buvo numatytos tokios sąlygos:

1. padaroma žala;
2. žala padaroma neteisėta veika;
3. yra priežastinis ryšys tarp neteisėtos veikos ir žalos atsiradimo;
4. yra pažeidėjo kaltė;
5. pažeidėją ir nukentėjusiąją šalis teisės pažeidimo metu siejo darbo santykiai;
6. žalos atsiradimas yra susijęs su darbo veikla.

Naujajame darbo kodekse nebeliko materialinės atsakomybės, tačiau šiuo metu galiojančio Darbo kodekso 151 straipsnis numato turtinės ir neturtinės žalos, kai žala padaryta darbo pareigų pažeidimu dėl kaltės, atlyginimo sąlygas. Darbo kodekso 153 straipsnio 1 dalyje numatoma, jog tokios žalos atlyginimas turi būti ne daugiau kaip darbuotojo trijų vidutinių darbo užmokesčio dydžio, o jeigu turtinė žala padaryta dėl didelio neatsargumo – ne daugiau kaip šešių jo vidutinių darbo užmokesčio dydžio, išskyrus kodekse ir kituose įstatymuose numatytus atvejus. Darbo kodekso nuostatos taip pat numato galimybę nutraukti darbo sutartį su darbuotoju, kai yra padaromas darbo pareigų pažeidimas, nustatytas darbo teisės normomis arba darbo sutartimi. Šio kodekso 58 straipsnyje yra numatytas nebaigtinis sąrašas pagrindų, dėl kurių gali būti nutraukta darbo sutartis darbdavio iniciatyva dėl darbuotojo kaltės, viena iš priežasčių yra šiurkštus darbuotojo darbo pareigų pažeidimas. Lietuvos Respublikos Aukščiausiasis Teismas yra konstatavęs, jog sprendžiant ar pažeidimas priskirtinas prie šiurkščių būtina analizuoti darbuotojo neteisėto elgesio pobūdį, dėl šio pažeidimo atsiradusius nuostolius bei kitokius neigiamus padarinius, darbuotojo kaltę ir jos formas, kitų asmenų veiksmų įtaką šiam pažeidimui bei kitas svarbias aplinkybes. Tam, kad būtų konstatuotas šiurkštus darbo pareigų pažeidimas, ne visais atvejais būtina, kad darbdavys dėl darbuotojo neteisėtų veiksmų patirtų realius nuostolius (Lietuvos Respublikos Aukščiausiojo teismo 2022 m. birželio 23 d. nutartis civilinėje byloje).

Taip pat šiame darbe buvo analizuojama teismų praktika susijusi su saviraiškos laisve ir teise į privatumą, kuri leidžia teigti, jog šios teisės darbo vietoje nėra besąlyginės. Atsakomybės už darbo pareigų pažeidimą taikymas, kuris yra susijęs su technologijų

panaudojimu darbo vietoje, neriboja kitos teisinės atsakomybės rūšies taikymo. Nagrinėjant ginčus dėl šiurkštaus darbo pareigų pažeidimo, siejamo su darbuotojo teisės į privatų gyvenimą turiniu, kiekvienu atveju reikia vertinti darbuotojo funkcijas, darbo vietos ir laiko aplinkybes, darbdavio suteiktų priemonių naudojimo apribojimus, profesinį ir privatų veiksmų pobūdį (Tamašauskaitė-Janickė, 2016, p. 171).

Tais atvejais, kai žala yra padaroma darbo sutarties šalims ar tretiesiems asmenims veiksmais, kurie nėra susiję su darbo funkcijų vykdymu, nors asmuo tai padaro darbo vietoje ir darbo metu, turtinė atsakomybė atsiranda ne pagal darbo, o pagal civilinės teisės normas, nes egzistuoja keturios sąlygos civilinei atsakomybei kilti:

1. žala;
2. žala padaroma neteisėtais veiksmais;
3. kaltė;
4. priežastinis ryšys tarp neteisėtų veiksmų ir žalos atsiradimo (Teismų praktikos dėl sutartinės civilinės…, 2018, p. 1).

Būtent dviejų sąlygų nebuvimas, kurios buvo įvardijamos nurodant Darbo kodekso senos redakcijos normą, kurioje kalbama apie materialinėss atsakomybės kilimo sąlygas, lemia atsakomybės pagal civilinę ir darbo teisę atskyrimą.

Aktualu yra aptarti ir Civilinio kodekso nuostatas, susijusias su atsakomybe už pažeidimus. Darbuotojui gali kilti materialinė atsakomybė dėl darbo pareigų pažeidimo, jei šiuo pažeidimu yra pažeidžiamas asmens privatumas. Civilinio kodekso 6.263 straipsyje yra numatyta pareiga kiekvienam asmeniui laikytis tokio elgesio taisyklių, kad savo veiksmais kitam asmeniui nebūtų padaryta žala, atsakingas asmuo privalo atlyginti visą turtinę, numatytais atvejais ir neturtinę žalą. Šio kodekso 6.264 straipsnyje yra apibrėžiama samdančio darbuotojus asmens atsakomybė už žalą, atsiradusią dėl jo darbuotojo kaltės, o būtent tai, jog samdantis darbuotojus asmuo privalo atlyginti žalą, kuri kilo dėl jo darbuotojų, einančių savo darbines pareigas, kaltės, o jeigu įstatymų numatytais atvejais samdantis darbuotojus asmuo ir darbuotojas už žalą atsako kartu, tai darbuotojas atsako jį nusamdžiusiam asmeniui tik tuo atveju, kai yra darbuotojo tyčia ar neatsargumas. Darbo kodekse numatyta, kad darbdavys, patyręs žalos dėl darbuotojo kaltės, gali išskaityti pinigines sumas iš darbuotojo darbo užmokesčio (Darbo kodekso 150 straipsnis), ši teisė yra kildinama iš Civiliniame kodekse numatytos regreso teisės į žalos padariusį asmenį (Civilinio kodekso 6.280 straipsnis).

Norminiai teisės aktai nepateikia aiškaus atsakymo žalos atlyginimo atvejais, kai:

1. darbuotojas dirba su darbdavio žinia, bet ne darbdavio interesais;

2. darbuotojas dirba darbdavio interesais, bet be darbdavio žinios.

Kai darbdaviui yra žinoma, kad darbuotojas atliks veiklą, nesusijusią su darbo funkcijomis, žalos atsiradimas yra laikytinas susijusiu su darbo veikla, nes darbdavys sprendžia ar leisti savo darbuotojui atlikti veiksmus. Antruoju atveju, jeigu veikla yra atliekama darbdavio interesais, bet be darbdavio žinios, o tokia veikla atliekama asmeniui esant darbovietėje, laikoma, kad ji yra susijusi su darbo veikla. Žalos atlyginimą galima užginčyti tada, kai darbuotojas dirba darbo sutartyje nesulygtą darbą darbdavio interesais ir naudai. Tais atvejais, kai darbuotojas dirba ne įmonės suteiktoje darbo vietoje, tada taikoma prezumpcija, jog žalos atsiradimas nelaikytinas susijęs su darbu (Bagdanskis, 2008, p. 87).

Atsakomybės kontekste pažymėtina 3– ioje šio darbo dalyje jau minėta naujausia Lietuvos vyriausio administracinio teismo 2025 metų kovo 26 dienos nutartis. Šiame ginče Agentūra siekė įrodyti, jog atsakomybė turėtų būti taikoma tik jos darbuotojams, nes ji yra VATARIS naudotoja, o šios sistemos tvarkytojas – Informatikos ir ryšių departamentas. Lietuvos vyriausiasis administracinis teismas šiuos argumentus atmetė, nustatydamas, kad Agentūra taip pat laikytina VATARAS duomenų ir asmens duomenų tvarkytoja. Teismas pabrėžė, kad pagal Bendrąjį duomenų apsaugos reglamentą būtent Agentūra, kaip darbdavys, kuris nustato duomenų tvarkymo tikslus ir priemones, yra atsakinga už Bendrojo duomenų apsaugos reglamento reikalavimų laikymąsi. Agentūra buvo atsakinga už tai, kad darbuotojai nesinaudotų asmens duomenimis be teisinio pagrindo, todėl Duomenų apsaugos inspekcijos sprendimą Lietuvos vyriausias administracinis teismas paliko galioti (LVAT:Viešojo valdymo agentūroje asmens…, 2025). Tad šioje byloje buvo išaiškinta, jog Agentūra, visų pirma, elgėsi nesąžiningai, kaltindama vieną darbuotoją, nors su informacija susipažino keli darbuotojai, antra, nebuvo įgyvendintos tinkamos prevencinės organizacinės ir techninės priemonės, todėl galima teigti, kad pradinis saugumas buvo netinkamas. Pažymėtina, jog teisinės baudos paskirtis yra atgrasyti ir užtikrinti Bendrojo duomenų apsaugos reglamento nuosatatų laikymąsi. Teisingumo Teismas 2023 metų gruodžio 5 dienos sprendime C-807/21, konstatavo, kad sankcijų sistema, leidžianti skirti administracinę baudą pagal Bendrojo duomenų apsaugos reglamento 83 straipsnį, skatina duomenų valdytojus, duomenų tvarkytojus laikytis šio reglamento, o baudos prisideda prie fizinių asmenų apsaugos tvarkant asmens duomenis stiprinimo (Lietuvos Vyriausiojo Administracinio Teismo 2025 m. kovo 26 d. nutartis).

Dirbtinio intelekto panaudojimas taip pat kelia tam tikrus iššūkius atsakomybės klausimu. Europos Komisija yra numačiusi, jog būtina nustatyti mechanizmus, kuriais būtų užtikrinta atsakomybė už dirbtinio intelekto sistemas ir jų rezultatus, taip pat būtina

nustatyti mechanizmus, kuriais būtų užtikrintos tinkamos galimybės, kai padaromas neteisingas ir (ar) neigiamas poveikis (Communication from the Comission to..., 2019). Atsakomybės už dirbtinio intelekto sukeltą žalą klausimai patekdavo į 1985 metų Tarybos direktyvos 85/374/EEB ir ją įgyvendinančių Civilinio kodekso 6.292-6.300 straipsnių taikymo sritį (Ar dirbtinio intelekto sistemų kūrėjai…, 2024). 2024 metų spalio 23 dieną įsigaliojo nauja Europos parlamento ir Tarybos direktyva (ES) Nr. 2024/2853 dėl atsakomybės už gaminius su trūkumais, kuria panaikinama Tarybos direktyva 85/374/EEB, tačiau ji dar nėra implementuota į nacionalinės teisės nuostatas. Tad privataus gyvenimo kontekste, svarbu tai, jog naudojant dirbtinį intelektą gali būti pažeidžiama asmenų teisė į duomenų apsaugą ir privatumą, o atsakomybei už duomenų apsaugos teisės pažeidimus yra taikomos Bendrojo duomenų apsaugos reglamento nuostatos (Montagnani, Cavallo, 2021, p. 213).

Pritartina G. Tamašauskaitės-Janickės nuomonei, jog darbuotojo veiksmų ir darbinės veiklos sąsajos padeda nustatyti, kuri iš teisinės atsakomybės rūšių padarytai žalai atlyginti turi būti taikoma konkrečiu atveju. Tam tikrais atvejais žala gali būti susijusi ne su tradicinių darbo sutarties šalių pareigų nevykdymų ar netinkamu vykdymu, bet siejama su asmeninių teisių įgyvendinimu darbo vietoje, toks papildomas statusas yra apibrėžiamas ne darbo teisės, bet asmens duomenų teisinės apsaugos ar kitų teisės normų (Tamašauskaitė-Janickė, 2016, p. 214). Taip pat manoma, kad kalbant apie atsakomybę, kylančią dėl neteisėto duomenų tvarkymo, reikėtų neatmesti darbuotojui galinčios kilti individualios atsakomybės už pažeidimą, tuo atveju, jei darbdavys įgyvendina visas būtinas prevencines priemones, kad būtų užkirstas kelias tokiems pažeidimams. Tačiau tais atvejais, kai darbdavys, nors ir turėdamas pareigą nustatyti konkretų kontrolės mechanizmą ir taisykles, užtikrinančias tinkamą duomenų tvarkymą ir privatumo apsaugą, šių pareigų neįvykdo, sutinkama su Lietuvos bei tarptautinių teismų formuojama praktika, kad darbdavys turi prisiimti atsakomybę už tokio pobūdžio pažeidimus.

IŠVADOS

1. Teisė į privatumą yra viena iš pagrindinių demokratinės visuomenės vertybių, tačiau iki šiol nėra suformuoto visiems priimtino apibrėžimo, apibūdinančio privatumą, nes ši sąvoka yra subjektyvi ir priklausomai nuo aplinkybių, ji gali būti skirtingai interpretuojama. Svarbu tai, kad asmens privatumas yra ginamas teisės normomis. Ryšys tarp teisės į privatumą ir teisės į asmens duomenų apsaugą yra reikšmingas. Šios teisės yra atskiros, tačiau glaudžiai susijusios tarpusavyje, toks ryšys yra grindžiamas tuo, kad Bendrasis duomenų apsaugos reglamentas ne tik nustato fizinių asmenų apsaugą tvarkant jų duomenis, bet ir padeda suderinti fizinių asmenų pagrindinių teisių ir laisvių apsaugą vykdant duomenų tvarkymo veiklą, taip sukuriant subalansuotą teisinį mechanizmą teisės į privatumą ir teisės į asmens duomenų apsaugą įgyvendinimo kontekste.

2. Darbo vieta yra suvokiama kaip faktinė vieta, kurioje darbuotojas vykdo savo darbo funkcijas. Šiuolaikinės darbo organizavimo formos suteikia lankstumo bei kitų privalumų darbo santykių subjektams, tačiau jos taip pat kelia teisinių iššūkių, ypač susijusių su darbuotojų teisės į privatumą užtikrinimu. Technologinė evoliucija lėmė darbo santykių pokytį, kuriame įsitvirtino nuolatinio darbuotojų pasiekiamumo kultūra, taip pat darbdavio vykdoma stebėsena, pasitelkiant modernias technologijas. Siekiant užtikrinti darbuotojų privatumo apsaugą, pradėti formuoti teisiniai apsaugos mechanizmai, tokie kaip darbuotojo teisė atsijungti, taip pat taisyklės, reglamentuojančios darbuotojų stebėseną, kurios formuojamos tiek teisės aktuose, tiek ir teismų praktikoje, pabrėžiant, jog darbdaviui vykdant darbuotojų stebėseną pažangiausiomis technologijomis, būtina laikytis teisinių pagrindų ir principų, užtikrinančių tokios stebėsenos teisėtumą.

3. Teisė į privatumą išimtinais atvejais gali būti ribojama, tačiau darbdavys, vykdydamas darbuotojų stebėjimą ir taip siekdamas ginti savo teisėtus interesus, turi užtikrinti, kad jo veiksmai nepažeistų šios vienos iš pagrindinių žmogaus teisių. Darbdavys, vykdydamas stebėseną, pasitelkiant modernias technologijas, turi aiškiai apibrėžti tokios kontrolės taisykles, pasirinkti proporcingas, mažiausiai teisę į privatumą galinčias apriboti priemones, įsitikinti, kad pasirinktas tinkamas teisinis pagrindas ir yra laikomasi duomenų tvarkymo principų, vykdyti poveikio duomenų apsaugai vertinimą ir teisėtų interesų pusiausvyros testą, kurie gali sumažinti pažeidimų riziką. Veiksmų, kuriuos turi

atlikti darbdavys prieš stebėjimo vykdymą, gausa, įrodo, jog darbuotojų teisė į privatumą nusveria darbdavio interesą užtikrinti darbo efektyvumą. Darbuotojai taip pat turi prisiimti atsakomybę už savo asmeninės informacijos apsaugą, jie turi imtis prevencinių priemonių ir elgtis atsakingai darbo vietoje, kad galimybė pažeisti jų teisę į privatumą būtų minimizuota.

4. Modernių technologijų naudojimas, pažeidžiantis teisės aktuose nustatytą arba darbo santykių šalių sulygtą tvarką, gali lemti atsakomybės atsiradimą ne tik pagal darbo teisę, bet ir pagal kitas teisės šakas. Darbdavys turi užtikrinti būtinas prevencines priemones, kad būtų išvengta atsakomybės, už pažeidimus, sietinus su duomenų apsaugos ir privatumo taisyklių nesilaikymu. Priešingu atveju būtent darbdavys bus atsakingas už teisės aktų pažeidimais sukeltą žalą asmenims.

5. Sparčiai besivystanti technologinė pažanga kelia vis daugiau iššūkių darbuotojų privatumo apsaugai. Bendrasis duomenų apsaugos reglamentas nustato bendrąsias taisykles, susijusias su teisėtu duomenų tvarkymu, tačiau matoma, jog teisinė sistema nespėja vytis modernių technologijų plėtros. Siekiant efektyvios darbuotojų privatumo apsaugos, būtina modernizuoti nacionalinius teisės aktus, taip pat Europos Sąjungos lygmeniu numatyti detalias, aiškias taisykles, reguliuojančias modernių technologijų panaudojimą darbo santykiuose ir darbuotojų privatumo apsaugos užtikrinimą.

ŠALTINIŲ SĄRAŠAS

Teisės norminiai aktai:

1. Lietuvos Respublikos Konstitucija (1992) *Lietuvos Aidas*, Nr. 220 (1992-11-10); *Valstybės Žinios*, Nr. 33-1014 (1992-11-30).
2. Visuotinė žmogaus teisių deklaracija (1948) *Valstybės žinios*, Nr. 048T001DEKLRG480005.
3. Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija (1995) *Valstybės žinios*, Nr. 40-987.
4. Europos Parlamento ir Tarybos Direktyva 95/46/EB (1995) dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo.
5. Tarptautinis pilietinių ir politinių teisių paktas (2002) *Valstybės žinios*, Nr. 77-3288
6. Europos Parlamento ir Tarybos Direktyva 2002/58/EB (2002) dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių).
7. Europos Parlamento ir Tarybos Direktyva 2003/88/EB (2002) dėl tam tikrų darbo laiko organizavimo aspektų.
8. Europos Sąjungos pagrindinių teisių Chartija (2016/C 202). C 202/389.
9. Europos Parlamento ir Tarybos Reglamentas (ES) 2016/679 (2016) dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas).
10. Europos Parlamento ir Tarybos Reglamentas (ES) 2024/1689 (2024) kuriuo nustatomos suderintos dirbtinio intelekto taisyklės ir iš dalies keičiami reglamentai (EB) Nr. 300/2008, (ES) Nr. 167/2013, (ES) Nr. 168/2013, (ES) 2018/858, (ES) 2018/1139 ir (ES) 2019/2144 ir direktyvos 2014/90/ES, (ES) 2016/797 ir (ES) 2020/1828 (Dirbtinio intelekto aktas).
11. Lietuvos Respublikos civilinio kodekso patvirtinimo, įsigaliojimo ir įgyvendinimo įstatymas. Civilinis kodeksas (2000) *Valstybės žinios*, Nr. 74-2262.
12. Lietuvos Respublikos baudžiamojo kodekso patvirtinimo ir įsigaliojimo įstatymas. Baudžiamasis kodeksas (2000) *Valstybės žinios*, Nr. 89-2741.
13. Lietuvos Respublikos darbo kodekso patvirtinimo, įsigaliojimo ir įgyvendinimo įstatymas. Lietuvos Respublikos darbo kodeksas (2002) *Valstybės žinios*, Nr. 64-2569.

14. Lietuvos Respublikos baudžiamojo proceso kodekso patvirtinimo, įsigaliojimo ir įgyvendinimo įstatymas. Baudžiamojo proceso kodeksas (2002) *Valstybės žinios*, Nr. 37-1341.
15. Lietuvos Respublikos administracinių nusižengimų kodekso patvirtinimo, įsigaliojimo ir įgyvendinimo tvarkos įstatymas. Lietuvos Respublikos administracinių nusižengimų kodeksas (2015) *TAR*, Nr. 11216.
16. Lietuvos Respublikos darbo kodekso patvirtinimo, įsigaliojimo ir įgyvendinimo įstatymas. Darbo kodeksas (2016). *TAR*, Nr. 23709.
17. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas (1996) *Valstybės žinios*, Nr. 63-1479.
18. Lietuvos Respublikos saugos ir sveikatos įstatymas (2003) *Valstybės žinios*, Nr. 70-3170.
19. Lietuvos Respublikos elektroninių ryšių įstatymas (2004) *Valstybės žinios*, Nr. 69-2382.
20. Lietuvos Respublikos kriminalinės žvalgybos įstatymas (2012), *Valstybės žinios*, Nr. 122-6093.

Teismų praktika:

21. Lietuvos Respublikos Konstitucinio Teismo 2000 metų gegužės 8 dienos nutarimas. *Valstybės žinios*, 39-1105.
22. Lietuvos Respublikos Konstitucinio Teismo 2002 m. spalio 23 d. nutarimas. *Valstybės žinios,* 36/2000.
23. Lietuvos Respublikos Konstitucinio Teismo 2004 metų gruodžio 29 dienos nutarimas. *Valstybės žinios*, 85-3094.
24. *Niemetz v. Germany* [ECHR], Nr. 13710/88, [1992-12-16]. ECLI:CE:ECHR:1992:1216JUD001371088
25. *Halford v. the United Kingdom* [ECHR], Nr. 20605/92, [1997-06-25] ECLI:CE:ECHR:1997:0625JUD002060592
26. Opinion of Advocate General Sharpston delivered on 17 June 2010. Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v Land Hessen. Opinion of Advocate General Sharpston delivered on 17 June 2010. [2010-06-17]. ECLI:EU:C:2010:353.

27. *Bărbulescu v. Romania* [ECHR], Nr. 61496/08, [2017-09-05]. ECLI:CE:ECHR:2017:0905JUD006149608
28. *Ville de Nivelles v. Rudy Matzak* [CJEU], Nr. C-518/15, [2018-02-21]. ECLI:EU:C:2018:82.
29. *López Ribalda and others v. Spain* [ECHR], Nr. 1874/13 ir 8567/13, [2019-10-17]. ECLI:CE:ECHR:2019:1017JUD000187413
30. *Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems* [CJEU], Nr. C-311/18 [2020-07-16]. ECLI:EU:C:2020:559
31. *Florindo de Almeida Vasconcelos Gramaxo v. Portugal* [ECHR], Nr. 26968/16, [2022-12-13]. ECLI:CE:E CHR:2022:1213JUD002696816
32. Lietuvos Aukščiausiojo Teismo 2021 m. birželio 16 d. nutartis civilnėje byloje Nr. e3K-3-150-313/2021.
33. Lietuvos Aukščiausiojo Teismo 2022 m. birželio 23 d. nutartis civilinėje bylose Nr. e3K-3-187-421/2022.
34. Lietuvos Aukščiausiojo Teismo 2023 m. gruodžio 20 d. nutartis civilinėje byloje Nr. e3K-3-328-684/2023.
35. Lietuvos Aukščiausiojo Teismo 2024 m. spalio 8 d. nutartis civilnėje byloje Nr. e3K-3-176-684/2024.
36. Lietuvos Vyriausiojo Administracinio Teismo 2020 m. balandžio 2 d. sprendimas administracinėje byloje Nr. A-3345-822/2020.
37. Lietuvos Vyriausiojo Administracinio Teismo 2025 m. kovo 26 d. nutartis administracinėje byloje Nr. eA-483-821/2025
38. Valstybinės duomenų apsaugos inspekcijos 2025 m. sausio 10 d. sprendimas Nr. 3R-19 (2.13-1.E).

Specialioji literatūra:

39. Aldhafferi, N., Watson, C. ir Sajeev, A.S.M. (2013). Personal Information Privacy Settings of Online Social Networks and their Suitability for Mobile Internet Devices. *International Journal of Security, Privacy and Trust Management (IJSPTM)*, 2, 2, https://doi.org/10.5121/ijsptm.2013.2201
40. Andriulis, V. (sud.) (2005). *Petras Leonas. Teisės filosofijos istorija. Raštai I tomas.* Vilnius: Teisinės informacijos centras.
41. Bagdanskis, T. (2008). *Materialinė atsakomybė darbo teisėje*. Vilnius: Registrų centras.

42. Bagdanskis, T., Sartatavičius, P. (2012). Workplace Privacy: Different Views and Arising Issues. *Jurisprudencija*, 19 (2), 697-713.
43. Bania, K. and Géradin, D. (2023). The regulation of cloud computing: why the European Union failed to get it right. *Information and Communications Technology Law*, 33(1), 99-113. https://doi.org/10.1080/13600834.2023.2260687.
44. Bell, M., Lasek-Markey, M., Eustace, A. ir Pahlen, T. (2021). A right to Disconnect: Irish and European Legal Perspectives, *A Public Policy Report of the COVID-19 Law and Human Rights Observatory, School of Law, Trinity College Dublin* [interaktyvus]. Prieiga per internetą: https://www.tcd.ie/law/2020.21/Final%20RTD%20report.pdf [žiūrėta 2025 m. vasario 28 d.].
45. Beye, M. ir kt. (2010). Literature Overview - Privacy in Online Social Networks. CTIT Technical Report Series, TR-CTIT-10-36, *Centre for Telematics and Information Technology (CTIT), Enschede* [interaktyvus]. Prieiga per internetą: https://ris.utwente.nl/ws/portalfiles/portal/5577719/Beye12privacy.pdf [žiūrėta 2024 m. gruodžio 27 d.].
46. Boyd, D.M., Ellison, N.B. (2007). Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication*, 13, 1, 210-230. https://doi.org/10.1111/j.1083-6101.2007.00393.x.
47. Breskienė, I. (2025). Darbuotojų stebėjimas panaudojant algoritminį valdymą, grįstą dirbtinio intelekto sistemomis. *Teisė*, 133, 103-117. https://doi.org/10.15388/Teise.2024.133.7
48. Chan, C.K., Virkki, J. (2014). Perspectives for Sharing Personal Information on Online Social Networks. *Social Networking, 3, 1, 2014.* [interaktyvus] DOI: 10.4236/sn.2014.31005
49. Civilka, M. (2002). Europos Sąjungos asmens duomenų apsaugos teisinis reguliavimas interneto kontekste. Iš: Vadapalas. V. (2002*). Europos Sąjungos teisė ir Lietuva*, Vilnius: Justitia, 226-260.
50. Civilka, M., Šlapimaitė, L. (2015). Asmens duomenų samprata elektroninėje erdvėje. *Teisė,* 96, 126-148. https://doi.org/10.15388/Teise.2015.96.8761
51. Davulis, T. (2018). *Lietuvos Respublikos darbo kodekso komentaras.* Vilnius: Registrų centras.
52. Davulis, T. (2019). p. 217. Iš: Žalimienė, S. et al. (2019) *Europos Sąjungos pagrindinių teisių chartijos, kaip individualių teisių gynybos standarto, taikymas*

supra- ir nacionaliniu lygmenimis : kolektyvinė monografija Vilnius: Vilniaus universiteto leidykla.

53. European Parliament, Directorate-General for Parliamentary Research Services, Davies, R. (2016). *Cloud computing : an overview of economic and policy issues : in-depth analysis*. https://data.europa.eu/doi/10.2861/705354
54. Hannelais, J., Machrhoul Lhotellier, S., (2021*) Protection of privacy at work in France* [interaktyvus]. Prieiga per internetą: https://va-fr.com/wp-content/uploads/2021/04/VA-Protection-of-privacy-at-work-in-France-16042021.pdf [žiūrėta 2025 m. kovo 1 d.].
55. Jočienė, D., Čilinskas, K. (2004). *Žmogaus teisių apsaugos problemos tarptautinėje ir Lietuvos Respublikos teisėje.* Vilnius : Petro ofsetas.
56. Komanovics, A. (2023). Workplace privacy in the EU. The impact of emerging technologies on employee's fundamental rights. *EU and Comparative Law Issues and Challenges Series (ECLIC).* 7, 443–474. https://doi.org/10.25234/eclic/27458.
57. Lerouge, L. (2022). Contribution to the study on the 'right to disconnect' from work. Are France and Spain examples for other countries and EU law? *European Labour Law Journal*, 13, 3, 450-465. https://doi.org/10.1177/20319525221105102
58. Markevičius, E. (2019). *E. Privatumo direktyvos įgyvendinimo problemos ir jų sprendimai e. Privatumo reglamento projekte*. Teisė, 113, 139-154. https://doi.org/10.15388/Teise.2019.113.8
59. Mateescu, A., Nguyen, A. (2019). Explainer: Algorithmic Management in the Workplace. *Data and Society research Institute* [interaktyvus]. Prieiga per internetą: https://datasociety.net/wp-content/uploads/2019/02/DS_Algorithmic_Management_Explainer.pdf [žiūrėta 2025 m. vasario 4 d.]
60. Meškauskaitė, L. (2004). *Žiniasklaidos teisė : visuomenės informavimo teisė : teoriniai ir praktiniai aspektai*. Lietuvos teisės universitetas. Vilnius: Teisinės informacijos centras.
61. Meškauskaitė, L., Lankauskas, M. (2016) Baudžiamoji atsakomybė už asmens privataus gyvenimo neliečiamumo pažeidimus Europos žmogaus teisių teismo bet Lietuvos teismų praktikos kontekste. *Teisės problemos.* 1 (91), 52-80. Prieiga per internetą: https://teise.org/wp-content/uploads/2023/01/Meskauskaite-Lankauskas-2016_1.pdf [žiūrėta 2024 m. gruodžio 27 d.].
62. Mikelėnas, V. (2001). *Tarptautinės privatinės teisės įvadas*. Vilnius: Justitia.

63. Montagnani, M.L., Cavallo, M. (2021). Liability and Emerging Digital Technologies: An EU Perspective. *Notre Dame Journal of International & Comparative Law*, 11, 2, 4 [interaktyvus]. Prieiga per internetą: https://scholarship.law.nd.edu/ndjicl/vol11/iss2/4 [žiūrėta 2025 m. vasario 10 d.].
64. Murugesan, U., et al (2023) A study of Artificial Intelligence impacts on Human Resource Digitalization in Industry 4.0. *Elsevier, Decision Analytics Journal.* https://doi.org/10.1016/j.dajour.2023.100249
65. Mykolo Romerio universiteto Teisės mokyklos Privatinės teisės institutas, Grigonienė, R. (2020). *Darbuotojų asmens duomenų apsaugos užtikrinimo teisinio reguliavimo ypatumai.* Vilnius: Jurisprudencija, 27(2), 346–369. https://doi.org/10.13165/JUR-20-27-2-06
66. Petraitytė, I. (2011). *Asmens duomenų apsaugos teisinis reguliavimas Lietuvos teisės sistemoje.* Teisė, 79, 2011, 125–38. https://doi.org/10.15388/Teise.2011.0.175.
67. Petraitytė, I. (2013). *The personal data protection principles.* Summary of Doctoral Dissertation, Social Sciences, Law (01 S), Vilniaus universitetas. Vilnius: Vilniaus universiteto leidykla.
68. Tamašauskaitė-Janickė, G. et al. (2016) *Informacinių ir komunikacinių technologijų panaudojimas darbo vietoje darbo teisės požiūriu.* Daktaro disertacija, Socialiniai mokslai, teisė (01 S), Vilniaus universitetas. Vilnius: Vilniaus universiteto leidykla.
69. Vartiainen, M. et al. (2007). *Distributed and Mobile Work - Places, people and technology*. Otatieto, Helsinki [interaktyvus]. Prieiga per internete: https://www.researchgate.net/publication/239731062_Distributed_and_Mobile_Work_-Places_People_and_Technology [žiūrėta 2025 m. sausio 5 d.].
70. Wachter, S., Mittelstadt, B. (2018). A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI. *Columbia Business Law Review, 2019(2)* [interaktyvus]. Prieiga per internetą: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248829.
71. Weatherbee, T.G. (2010). Counterproductive use of technology at work: Information & communications technologies and cyberdeviancy. *Human Resource Management Review*, 20(1). https://doi.org/10.1016/j.hrmr.2009.03.012.
72. Zaleskis, J. (2019). *Europos Sąjungos Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė : monografija.* Vilniaus universiteto Teisės fakultetas. Vilnius: Registrų centras.
73. Žiobienė, E. (2002). Legal Doctrine of Privacy in USA. 32 (24), *Jurisprudencija*.

Kiti šaltiniai:

74. 29 straipsnio duomenų apsaugos darbo grupė. Nuomonė 2/2017 dėl duomenų tvarkymo darbe. (2017). Prieiga per internetą: https://vdai.lrv.lt/uploads/vdai/documents/files/Nuomonedelduomenutvarkymodrabe20170608wp249lt(2).pdf [žiūrėta 2024 m. spalio 17 d.].
75. Act on the Protection of Privacy in Working Life (759/2004), (2004). Neoficialus teisės akto vertimas. Prieiga per internetą: https://www.finlex.fi/api/media/statute-foreign-language-translation/150778/mainPdf/main.pdf?timestamp=2004-08-13T00%3A00%3A00.000Z [žiūrėta 2025 m. kovo 1 d.].
76. Aravamudhan, A. *SaaS vs PaaS vs SaaS: Key Differences Explain*ed. [interaktyvus] (modifikuota 2024-08-27). Prieiga per internetą: https://www.eginnovations.com/blog/saas-vs-paas-vs-iaas-examples-differences-how-to-choose/ [žiūrėta 2025 m. vasario 20 d.].
77. Berthereau, J. *Droit à la déconnexion : la Cour de cassation rappelle la loi.* [interaktyvus] (modifikuota 2024-12-16) Prieiga per internetą: https://www.experts-et-decideurs.fr/vie-entreprise/droit-a-la-deconnexion-la-cour-de-cassation-rappelle-la-loi/ [žiūrėta 2025 m. kovo 1 d.].
78. Data Protection Comission. (2019). Guidance note: Legal Bases for Processing Personal Data. Prieiga per internetą: https://www.dataprotection.ie/en/dpc-guidance/guidance-legal-bases-processing-personal-data [žiūrėta: 2024 spalio 17 d.].
79. Data protection laws of the world: Finland (2023). Prieiga per internetą: https://www.dlapiperdataprotection.com/?t=law&c=FI [žiūrėta 2025 sausio 8 d.].
80. Ekalba.lt. (n.d.) *Lietuvių kalbos išteklių informacinė sistema E. KALBA*. Prieiga per internetą: https://ekalba.lt/dabartines-lietuviu-kalbos-zodynas/privatus [žiūrėta 2025 sausio 8 d.].
81. *Ekspozicija darbo vietoje. Terminija.* (2024). Prieiga per internetą: https://lsmu.lt/cris/entities/standard/401b7552-a151-476d-a9ff-ab69dfcd6e71 [žiūrėta 2025 sausio 25 d.].
82. Eurofound (2021). The digital age: Implications of automation, digitisation and platforms for work and employment, Challenges and prospects in the EU series, Publications Office of the European Union, Luxembourg. https://doi:10.2806/288

83. Eurofound (2022), The rise in telework: Impact on working conditions and regulations, Publications Office of the European Union, Luxembourg.
84. Eurofound (2023), Hybrid work in Europe: Concept and practice, Publications Office of the European Union, Luxembourg. https://doi:10.2806/069206
85. Eurofound (2023), Right to disconnect: Implementation and impact at company level, Publications Office of the European Union, Luxembourg. https://doi:10.2806/430915
86. Eurofound (2024), Bulgaria: Algorithmic management, Restructuring legislation database, Dublin. Prieiga per internetą: https://apps.eurofound.europa.eu/legislationdb/algorithmic-management/bulgaria [žiūrėta 2025 m. vasario 15 d.].
87. European Agency for Safety and Health at Work, Roquelaure, Y. (2023). Hybrid work: New opportunities and challenges for occupational safety and health. Prieiga per internetą: https://osha.europa.eu/en/publications/hybrid-work-new-opportunities-and-challenges-occupational-safety-and-health [žiūrėta 2025 m.sausio 30 d.].
88. European Comission (2019). Communication from the Comission to the European Parliament, the Council, the European Economic and Social Comitee and the Committee of thre Regions. Building trust in Human-Centric Artificial Intelligence. Brussels. Prieiga per internetą: https://digital-strategy.ec.europa.eu/library/communication-building-trust-human-centric-artificial-intelligence [žiūrėta 2025 m. vasario 12 d.].
89. European Data Protection Board. (2024). EU-U.S. Data privacy framework. F.A.Q. for European businesses [interaktyvus]. Prieiga per internetą: https://www.edpb.europa.eu/system/files/2024-07/edpb_dpf_faq-for-businesses_en.pdf (žiūrėta 2025 m. kovo 28 d.).
90. European Parliament (2020) Data subjects, digital surveillance, AI and the future of work. doi: 10.2861/879078
91. Europos duomenų apsaugos valdyba (2020). Gairės 05/2020 dėl sutikimo pagal Reglamentą 2016/679 1.1 versija. Prieiga per internetą: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_lt_0.pdf [žiūrėta 2024 m. gruodžio 29 d.]
92. Europos duomenų apsaugos valdyba. (2024). EDAV duomenų apsaugos vadovas smulkiajam verslui [interaktyvus]. Prieiga per internetą:

https://www.edpb.europa.eu/sme-data-protection-guide/home_lt [žiūrėta 2025 m. sausio 10 d.].

93. Europos Komisija (2023). *Regulatory Framework for AI*. Prieiga per internetą: https://digital-strategy.ec.europa.eu/lt/policies/regulatory-framework-ai [žiūrėta 2025 m.vasario 10 d.].
94. Europos Komisija. (2023). Kada Reikia Atlikti Poveikio Duomenų Apsaugai Vertinimą (PDAV)? Prieiga per internetą: commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/when-data-protection-impact-assessment-dpia-required_lt. [žiūrėta 2024 m. spalio 17 d.].
95. Europos Komisija. (n.d.) Kas yra duomenų valdytojas ir duomenų tvarkytojas? [interaktyvus]. Prieiga per internetą: https://commission.europa.eu/law/law-topic/data-protection/rules-business-and-organisations/obligations/controllerprocessor/what-data-controller-or-data-processor_lt [žiūrėta 2025 m. sausio 10 d.].
96. Europos Parlamentas (2021). 2021 m. sausio 21 d. Europos Parlamento rezoliucija su rekomendacijomis Komisijai dėl teisės atsijungti (2019/2181(INL)). Prieiga per internetą: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0021_LT.html [žiūrėta 2025 m. vasario 15 d.].
97. Europos Sąjungos leidinių biuras (2020). Duomenų apsauga elektroninių ryšių sektoriuje|EUR-Lex. Prieiga per internetą: https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=LEGISSUM:l24120 [žiūrėta 2025 m. vasario 25 d.].
98. Europos Sąjungos pagrindinių teisių agentūra. (2018). Europos duomenų apsaugos teisės vadovas. Liuksemburgas: Europos Sąjungos leidinių biuras (2021) https://doi:10.2811/022710.
99. Europos Vadovų Taryba. Europos Sąjungos Taryba. (n.d.). Dirbtinio intelekto aktas. Prieiga per internetą: https://www.consilium.europa.eu/lt/policies/artificial-intelligence/ [žiūrėta 2025 m. vasario 5 d.]
100. Fomm, K. [interaktyvus] (modifikuota 2024-05-14). Navigating employee data privacy in the SaaS-powered workplace. Prieiga per internetą: https://www.didomi.io/blog/saas-employee-data-privacy-nikolai-fomm
101. Generatyvinio dirbtinio intelekto (GenDI) saugaus naudojimo organizacijoje gairės. (2024). Prieiga per internetą: https://www.nksc.lt/naujienos/parengtos_generatyvinio_dirbtinio_intelekto_gendi_.html [žiūrėta 2024 m. spalio 17 d.].

102. Hietanen, J., (2001). *Act on protection of Privacy in working life adopted, Finland*. Prieiga per internetą: https://www.eurofound.europa.eu/en/resources/article/2001/act-protection-privacy-working-life-adopted [žiūrėta 2025 m. kovo 1 d.].
103. Hutt, R. [interaktyvus] (modifikuota 2015-11-13).*What are your digital rights?* Prieiga per internetą: https://www.weforum.org/stories/2015/11/what-are-your-digital-rights-explainer/ [žiūrėta 2025 m. kovo 1 d.].
104. IBM. [interaktyvus] (modifikuota 2021-10-20).*What are Iaas, Paas and Saas?* Prieiga per internetą: https://www.ibm.com/think/topics/iaas-paas-saas [žiūrėta 2025 m. kovo 1 d.].
105. International Labour Organization. (2022). Protection of worker's personal data: General principles. Prieiga per internetą: https://webapps.ilo.org/static/english/intserv/working-papers/wp062/index.html [žiūrėta 2025 m. vasario 25 d.].
106. International Trade Administration. (n.d.). Data Privacy Framework Program Participation Requirements Data Privacy Framework (DPF) Principles. Prieiga per internetą: https://www.dataprivacyframework.gov/program-articles/Participation-Requirements-Data-Privacy-Framework-(DPF)-Principles (žiūrėta 2025 m. kovo 28 d.).
107. Juozapaitienė, R. (2023). Teisėto intereso taikymo ir balanso nustatymo/balanso testo atlikimo praktika. Prieiga per internetą: https://vdai.lrv.lt/media/viesa/saugykla/2023/11/VGvbyEToXG0.pdf [žiūrėta 2024 m. spalio 17 d.].
108. *Kas yra debesies sauga? | „Microsoft" sauga*. (2025). Prieiga per internetą: https://www.microsoft.com/lt-lt/security/business/security-101/what-is-cloud-security [žiūrėta 2025 m. kovo 1 d.].
109. Lietuvos Aukščiausiojo Teismo Teisės tyrimų ir apibendrinimo departamentas. (2018). Teismų praktikos dėl sutartinės civilinės atsakomybės taikymo apžvalga. Prieiga per internetą: https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.lat.lt/data/public/uploads/2018/11/2018_sutartines_atsakomybes_taikymo_apzvalga.docx&ved=2ahUKEwju88GKyK-MAxXMQ_EDHVBDDuAQFnoECBUQAQ&usg=AOvVaw0r0PNnjMEC6wbkNGuaeb7i [žiūrėta 2025 m. kovo 23 d.].

110. Lietuvos Respublikos Seimas (2022). Darbo kodekso 52 straipsnio pakeitimo įstatymo projektas. Prieiga per internetą: https://e seimas.lrs.lt/portal/legalAct/lt/TAP/2211b7e022cd11edb36fa1cf41a91fd9?jfwid=ywjmsi0f4 [žiūrėta 2025 m. vasario 15 d.].
111. Lietuvos Respublikos socialinės apsaugos ir darbo ministerija (2024). *Teisė atsijungti: Lietuvos darbuotojai turi šią galimybę.* Prieiga per internetą: https://socmin.lrv.lt/lt/naujienos/teise-atsijungti-lietuvos-darbuotojai-turi-sia-galimybe/ [žiūrėta 2025 m. vasario 15 d.].
112. Mykolo Romerio universitetas [interaktyvus] (modifikuota 2016-04-04). Prof. dr. Mindaugas Kiškis. Ką reikia žinoti darbdaviams apie socialinių tinklų ir interneto naudojimą darbo vietoje. Prieiga per internetą: https://www.mruni.eu/news/prof-dr-mindaugas-kiskis-ka-reikia-zinoti-darbdaviams-apie-socialiniu-tinklu-ir-interneto-naudojima-darbo-vietoje-2/
113. Naujienos.vu.lt. [interaktyvus] (modifikuota 2016-02-03). *Darbuotojų teisė į privatumą ribos ir paribiai*. Prieiga per internetą: https://naujienos.vu.lt/darbuotoju-teise-i-privatuma-ribos-ir-paribiai/
114. Nelson, N. [interaktyvus] (modifikuota 2021-04-12).Understanding the theory of respondeat superior liability. Prieiga per internetą: https://www.wolterskluwer.com/en/expert-insights/understanding-the-theory-of-respondeat-superior-liability [žiūrėta 2025 m. kovo 10 d.].
115. Online etymology dictionary. (n.d.). *Privacy (n).* Prieiga per internetą: https://www.etymonline.com/word/privacy [žiūrėta 2024 m. spalio 17 d.].
116. Poškaitienė, V. (2022) p. 94. Iš: Lietuvos duomenų apsaugos pareigūnų asociacija (2022). Asmens duomenys besikeičiančiame pasaulyje: praktinis straipsnių rinkinys. Prieiga per internetą: https://ldapa.lt/wp-content/uploads/2023/04/Asmens-duomenys-besikeiciame-pasaulyje_praktinis-straipsniu-rinkinys.pdf. [2025 m. vasario 25 d.].
117. Raupelienė, A. (2024). Aiškinamasis žmogiškųjų išteklių valdymo terminų žodynas. Kaunas: Vytauto Didžiojo universitetas. https://doi.org/10.7220/9786094676116.
118. Riso S., Litardi C. (2024). Employee monitoring: A moving target for regulation | European Foundation for the Improvement of Living and Working Conditions. Prieiga per internetą:

https://www.eurofound.europa.eu/en/resources/article/2024/employee-monitoring-moving-target-regulation [žiūrėta 2025 m. sausio 10 d.].

119. Šapkauskaitė, G. [interaktyvus] (modifikuota 2025-02-06).*ES dirbtinio intelekto aktas: pirmosios nuostatos jau taikomos.* Prieiga per internetą: https://www.teise.pro/index.php/2025/02/06/es-dirbtinio-intelekto-aktas-pirmosios-nuostatos-jau-taikomos/ [žiūrėta 2025 m. kovo 1 d.].
120. Shaping Europe's digital future. (2017). Proposal for an ePrivacy regulation. Prieiga per internetą: https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation [žiūrėta 2025 m. vasario 27 d.].
121. Speičys O., Pavlovič, M. [interaktyvus] (modifikuota 2024-11-26) *Ar dirbtinio intelekto sistemų kūrėjai atsako už šių sistemų sukeltą žalą?* Prieiga per internetą: https://www.infolex.lt/portal/start.asp?act=news&Tema=54&Str=138856
122. Teisė.pro. *LVAT: Viešojo valdymo agentūroje asmens duomenys buvo tvarkomi pažeidžiant BDAR reikalavimus* [interaktyvus] (modifikuota 2025-03-31). Prieiga per internetą: https://www.teise.pro/index.php/2025/03/31/lvat-viesojo-valdymo-agenturoje-asmens-duomenys-buvo-tvarkomi-pazeidziant-bdar-reikalavimus/ [žiūrėta 2025 m. kovo 31 d.].
123. Teisė.Pro. *Phillipe Renaudiere: BDAR kurtas praeities, o ne ateities problemoms spręsti* [interaktyvus] (modifikuota 2018-11-08). Prieiga per internetą: https://www.teise.pro/index.php/2018/11/08/philippe-renaudiere-bdar-kurtas-praeities-o-ne-ateities-problemoms-spresti/ [žiūrėta 2025 m. kovo 5 d.].
124. Teisės departamentas (2022). XIVP-191(2) Teisės Departamento išvada dėl Darbo kodekso 52 straipsnio pakeitimo įstatymo projekto. Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAK/aefdaf90247811edb36fa1cf41a91fd9?jfwid=ywjmsi0f4 [žiūrėta 2025 m. vasario 15 d.].
125. Valstybinė duomenų apsaugos inspekcija (2020). Darbuotojų asmens duomenų tvarkymas, organizuojant darbą nuotoliniu būdu. Prieiga per internetą: https://vdai.lrv.lt/uploads/vdai/documents/files/Rekomedacija%20del%20darbuotoju%20duomenu%20tvarkymo%20nuotolinio%20darbo%20metu%202020-04-09.pdf [žiūrėta 2024 m. spalio 17 d.].
126. Valstybinė duomenų apsaugos inspekcija, Mykolo Romerio universitetas. Gairės verslui apie asmens duomenų apsaugą darbo santykių kontekste. (2023). Prieiga per internetą: https://vdai.lrv.lt/uploads/vdai/documents/files/el_ASMENS%20DUOMENŲ%20

APSAUGA%20DARBO%20SANTYKIŲ%20KONTEKSTE%20Gairės%20smulkiajam%20ir%20vidutiniam%20verslui.pdf [žiūrėta 2024 m. spalio 17 d.].

127. Valstybinė duomenų apsaugos inspekcija, Mykolo Romerio universitetas. Gairės viešajam sektoriui apie asmens duomenų apsaugą darbo santykių kontekste. (2023). Prieiga per internetą: https://vdai.lrv.lt/uploads/vdai/documents/files/el_ASMENS%20DUOMENŲ%20APSAUGA%20DARBO%20SANTYKIŲ%20KONTEKSTE%20Gairės%20smulkiajam%20ir%20vidutiniam%20verslui.pdf [žiūrėta 2024 m. spalio 17 d.].
128. Valstybinė duomenų apsaugos inspekcija, Mykolo Romerio universitetas (2019). Vaizdo stebėjimas pagal bendrąjį duomenų apsaugos reglamentą. Prieiga per internetą: https://vdai.lrv.lt/uploads/vdai/documents/files/02_%20Lankstinukas%20Vaizdo%20stebejimas%202020-02-20.pdf [žiūrėta 2025 m. vasario 10 d.].
129. Valstybinė duomenų apsaugos inspekcija. Poveikio duomenų apsaugai vertinimas. 10 dažniausių klaidų. Prieiga per internetą: https://vdai.lrv.lt/uploads/vdai/documents/files/05_%20PDAV.pdf [žiūrėta 2024 m. spalio 17 d.].
130. Vasiliauskienė, R. [interaktyvus] (modifikuota 2024-06-14). *Dirbtinio intelekto reglamentas ir BDAR: įgimta trintis?|COBALT.* Prieiga per internetą: https://www.cobalt.legal/lt/news-cases/dirbtinio-intelekto-reglamentas-ir-bdar-igimta-trintis/ [žiūrėta 2025 m. vasario 15 d.].
131. Vasiliauskienė, R., (2022), p. 49. Iš: Lietuvos duomenų apsaugos pareigūnų asociacija (2022). Asmens duomenys besikeičiančiame pasaulyje: praktinis straipsnių rinkinys. Prieiga per internetą: https://ldapa.lt/wp-content/uploads/2023/04/Asmens-duomenys-besikeiciame-pasaulyje_praktinis-straipsniu-rinkinys.pdf. [2025 m. vasario 25 d.].

SANTRAUKA

Modernios technologijos ir darbuotojų privatumo apsauga

Emilija Rimanaitė

Magistro darbe analizuojama modernių technologijų įtaka darbuotojų privatumo apsaugai, nagrinėjant ne tik nacionalinius teisės aktus, bet ir teisės aktus, taikomus visoje Europos Sąjungoje, taip pat mokslininkų išvadas, teismų praktikoje pateiktus išaiškinimus.

Siekiant išvengti privatumo pažeidimų darbo santykiuose, svarbu pripažinti, jog privatumo apibrėžimas gali būti suprantamas skirtingai. Lietuvoje nėra konkrečių teisės aktų, išsamiai reglamentuojančių darbuotojų privatumo apsaugą šiuolaikinių technologijų kontekste, tad svarbu remtis asmens duomenų apsaugą reguliuojančiais teisės aktais, nustatančiais teisinius duomenų tvarkymo pagrindus. Tinkamo teisinio pagrindo parinkimas leidžia išvengti darbuotojų teisės į privatumą pažeidimų ir užtikrina etišką darbuotojų kontrolę.

Modernių technologijų gausa suteikia darbuotojams galimybę atlikti darbo funkcijas praktiškai iš bet kurios vietos, tačiau tokios galimybės kelia iššūkius darbuotojų privatumui, nes nyksta riba tarp privataus ir profesinio gyvenimo. Darbdaviai, siekdami kontroliuoti kaip silpnesnioji darbo santykių šalis vykdo savo įsipareigojimus, pasitelkia stebėsenos būdus, kurie gali neatitikti proporcingumo principo, todėl siekiant teisės į privatumą pažeidimo prevencijos, svarbu įtvirtinti tikslų ir detalų reguliavimą, kad šios problemos būtų sprendžiamos veiksmingiau.

Užtikrinant pusiausvyrą tarp darbo santykių šalių teisių ir teisėtų interesų, darbdavys, kaip kontrolę vykdanti šalis, turėtų atsakingai žvelgti į vykdomą stebėseną, kiekvienu atveju vertinti jos būtinumą, laikytis teisėtų duomenų tvarkymo principų, pagrindų ir apie tai pranešti darbuotojams. Darbuotojai taip pat turi atsakingai žvelgti į savo pareigas, nepiktnaudžiauti turimomis teisėmis ir moderniomis technologijomis naudotis tiek, kiek tai yra būtina darbo funkcijoms atlikti, kad būtų išvengta ginčų, susijusių su darbo pareigų ir teisės į privatumą pažeidimais.

SUMMARY

Modern Technologies and Protection of Employee Privacy

Emilija Rimanaitė

The master’s thesis analyses the impact of modern technologies on the protection of employees' privacy, looking not only at national legislation, but also at legislation applicable throughout the European Union, as well as at scholarly findings and interpretations in case law.

To avoid privacy breaches in employment relationships, it is important to recognize that the definition of privacy may be interpreted differently. In Lithuania, there is no specific legislation that regulates, in detail, the protection of employees' privacy in the context of modern technologies, so it is important to refer to the legislation regulating the protection of personal data, which establishes the legal basis for processing data. Choosing the right legal basis avoids infringements of employees' right to privacy and ensures ethical monitoring of employees.

The abundance of modern technology enables employees to carry out their job functions from virtually anywhere, but such opportunities pose challenges to employees' privacy as the boundaries between private and professional life are blurred. Employers use monitoring techniques to monitor the fulfilment of their obligations by the weaker party in the employment relationship, which may not be proportionate, and it is therefore important to establish precise and detailed regulation to prevent breaches of the right to privacy in order to address these issues more effectively.

In order to ensure a balance between the rights and legitimate interests of the parties to the employment relationship, the employer, as the party carrying out the monitoring, should take a responsible approach to the monitoring carried out, assess the necessity of the monitoring in each case, comply with the principles of lawful data processing, the grounds for the processing, and notify the employees. Employees must also take a responsible approach to their duties, not abuse their rights and use modern technologies to the extent necessary for the performance of their job functions, in order to avoid disputes related to breaches of their employment duties and the right to privacy.