

Vilniaus universiteto Teisės fakulteto

Privatinės teisės katedra

Paulos Juchnevič

V kurso, darbo ir socialinės teisės

Studijų šakos studentės

Magistro darbas

BDAR ir darbo teisė

GDPR and Labour Law

Vadovas: Prof. dr. T. Davulis

Recenzentas: Lekt. dr. I. Povilaitienė

Vilnius

2021

ANOTACIJA IR PAGRINDINIAI ŽODŽIAI

Šiame darbe analizuojamas Europos Parlamento ir Tarybos Reglamento (ES) 2016/679 Bendrojo duomenų apsaugos Reglamento ir darbo teisės iššūkiai darbo santykiuose nuo kandidato gyvenimo aprašymo išsiuntimo pradžios iki darbo santykių pabaigos. Kadangi Bendrasis duomenų apsaugos reglamentas taikomas visiems Europos Sąjungos valstybės piliečiams ir įmonėms, įstaigoms, organizacijoms, svarbu išanalizuoti kaip Bendrojo duomenų apsaugos reglamento nuostatos koreliuoja su darbo teise ir darbo sutartimi.

Pagrindiniai žodžiai: duomenų subjektas, duomenų valdytojas, principai, asmens duomenų apsauga, darbo santykiai.

This paper analyzes the challenges of Regulation (EU) 2016/679 of the European Parliament and of the Council General Data Protection Regulation and labor law in the execution employment relationship: from the beginning of sending the candidate's CV till the end of the employment relationship. As the General Data Protection Regulation applies to all citizens and companies, institutions and organizations of the European Union, it is important to analyze how the provisions of the General Data Protection Regulation correlate with stipulations of labor law and the employment contract.

Keywords: data subject, data controller, principles, personal data protection, employment relations.

Turinys

SANTRUMPŲ SĄRAŠAS	4
SĄVOKŲ SĄRAŠAS	5
ĮVADAS	7
1. Ikisutartiniai santykiai ir BDAR.....	9
2. BDAR taikymas įsigaliojus darbo sutarčiai	15
2.1. Darbuotojo duomenų apsauga darbovietėje	16
2.1.1. Darbuotojo specialių kategorijų duomenų tvarkymas	16
2.1.2. Darbuotojų biometrinių duomenų tvarkymas darbo vietoje	18
2.1.3. Kiti darbuotojų tvarkomi duomenys darbo vietoje	21
2.2. Darbuotojo sutikimas dėl atvaizdo išviešinimo	23
2.3. Darbuotojų stebėjimas vaizdo ir garso priemonėmis	26
2.3.1. Darbuotojų stebėjimas vaizdo priemonėmis	27
2.3.2. Darbuotojų stebėjimas garso priemonėmis	30
2.4. Darbuotojų stebėjimas ir sekimas kitomis priemonėmis	33
2.4.1. Darbuotojų automobilio sekimas GPS priemonėmis	33
2.4.2. Darbuotojo elektroninių ryšių stebėjimas	36
3. Duomenų tvarkymas pasibaigus darbo santykiams	39
3.1. Buvusio darbuotojo duomenų saugojimo trukmė	39
3.2. Buvusio darbuotojo teisės BDAR kontekste	42
IŠVADOS	45
ŠALTINIŲ SĄRAŠAS	47
SANTRAUKA	52
SUMMARY	53

SANTRUMPŲ SĄRAŠAS

BDAR – Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas);

Duomenys – Asmens duomenys;

Duomenų apsaugos teisė – Asmens duomenų apsaugos teisė;

Direktyva – Europos Parlamento ir Tarybos direktyva 95/46/EB dėl asmens apsaugos tvarkant asmens duomenis ir dėl tokių duomenų judėjimo;

EBPO - Ekonominio bendradarbiavimo ir plėtros organizacija;

EŽTT – Europos Žmogaus Teisių teismas;

ES – Europos Sąjunga;

ESTT – Europos Sąjungos teisingumo teismas;

EDAV – Europos duomenų apsaugos valdyba;

ES 29 str. darbo grupė – ES Duomenų apsaugos direktyvos 29 straipsniu įsteigta darbo grupė asmenų apsaugai tvarkant asmens duomenis;

GPS - Globali padėties nustatymo sistema;

LAT – Lietuvos Aukščiausiasis teismas;

IP – Interneto protokolas;

VDAI – Valstybinė duomenų apsaugos inspekcija.

SĄVOKŲ SĄRAŠAS

Duomenų subjektas – fizinis asmuo, kurio tapatybę galima nustatyti, yra asmuo, kurio tapatybę tiesiogiai arba netiesiogiai galima nustatyti (Bendrojo duomenų apsaugos reglamento 4 str. 1 d.);

Duomenų tvarkymas – bet kokia automatizuotomis arba neautomatizuotomis priemonėmis su asmens duomenimis ar asmens duomenų rinkiniais atliekama operacija ar operacijų seka, kaip antai rinkimas, įrašymas, rūšiavimas, sisteminimas, saugojimas, adaptavimas ar keitimas, išgava, susipažinimas, naudojimas, atskleidimas persiunčiant, platinant ar kitu būdu sudarant galimybę jais naudotis, taip pat sugretinimas ar sujungimas su kitais duomenimis, apribojimas, ištrynimasis arba sunaikinimas (Bendrojo duomenų apsaugos reglamento 4 str. 2 d.);

Duomenų valdytojas – fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuris vienas ar drauge su kitais nustato duomenų tvarkymo tikslus ir priemones; kai tokio duomenų tvarkymo tikslai ir priemonės nustatyti Sąjungos arba valstybės narės teisės, duomenų valdytojas arba konkretūs jo skyrimo kriterijai gali būti nustatyti Sąjungos arba valstybės narės teise (Bendrojo duomenų apsaugos reglamento 4 str. 7 d.);

Duomenų tvarkytojas – fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuri duomenų valdytojo vardu tvarko asmens duomenis (Bendrojo duomenų apsaugos reglamento 4 str. 8 d.);

Priežiūros institucija – valstybės narės pagal 51 str. įsteigta nepriklausoma valdžios institucija (Bendrojo duomenų apsaugos reglamento 4 str. 21 d.);

Darbuotojas – fizinis asmuo, įsipareigojęs atlygintinai atlikti darbo funkciją pagal darbo sutartį su darbdaviu. Darbuotoju gali būti darbinį teisnumą (galėjimas turėti darbo teises ir pareigas) ir veiksnumą (galėjimas savo veiksmais įgyti darbo teises ir sukurti darbo pareigas) turintis fizinis asmuo. Fizinis asmuo darbinį teisnumą ir veiksnumą įgyja, kai jam sukanka šešiolika metų, išskyrus įstatymų nustatytas išimtis (Lietuvos Respublikos darbo kodekso 21 str. 2 d.);

Darbdavys – asmuo, kurio naudai ir kuriam būdamas pavaldus darbo sutartimi darbo funkciją atlygintinai įsipareigojo atlikti fizinis asmuo. Darbdaviu gali būti Lietuvos Respublikos jurisdikcijai priklausantis juridinis asmuo, turintis darbinį teisnumą ir veiksnumą, taip pat Lietuvos Respublikos teritorijoje įregistruotas užsienio valstybės jurisdikcijai priklausančio juridinio asmens ar kitos organizacijos padalinys (filialas,

atstovybė) ar užsienio valstybės jurisdikcijai priklausantis fizinis ar juridinis asmuo, kita organizacija, juridinio asmens ar kitos organizacijos padalinys (filialas, atstovybė) arba tokių asmenų grupė. Darbdavio – juridinio asmens darbinis teisnumas ir veiksnumas atsiranda nuo jo įsteigimo momento, nebent jo veiklą reglamentuojantys teisės aktai nustato vėlesnį įsisteigimo momentą. Darbdaviu taip pat gali būti fizinis asmuo. Darbdavio – fizinio asmens teisnumą ir veiksnumą reglamentuoja Lietuvos Respublikos civilinis kodeksas (Lietuvos Respublikos darbo kodekso 21 str. 3 d.).

IVADAS

Nuo 2018 m. gegužės 25 d. buvo pradedamas taikyti BDAR, kuris susistemino ir sustiprino asmens duomenų apsaugą, kuri iš esmės duomenų subjektui suteikia teisę pačiam nuspręsti, koku formatu ir būtų duomenų valdytojas gali kontroliuoti, rinkti asmens duomenis. Siekiant išsiaiškinti konkrečius statistinius duomenis Lietuvoje dėl darbuotojų asmens duomenų pažeidimų, autorė kreipėsi į Valstybinę duomenų apsaugos inspekciją, kuri šiuo statistinius duomenis:

1. Per 2020 metus iš viso buvo gauti – 1083 skundai, o iš jų būtent dėl darbuotojų asmens duomenų pažeidimų – 21.

2. Per 2020 metus iš viso buvo išnagrinėti 962 skundai, iš jų pritaikytos sankcijos dėl darbuotojų asmens duomenų – 6.

3. Per 2020 metus iš viso žmonės suteikta konsultacijų – 2210, iš jų dėl darbuotojų asmens duomenų tvarkymo – 108.

4. Per 2020 metus iš viso organizacijoms suteikta konsultacijų – 3284, iš jų dėl darbuotojų asmens duomenų tvarkymo – 278 (informacija gauta el. paštu iš VDAI teisės skyriaus patarėjos, 2021).

Ši statistika parodo, kaip darbuotojas, būdamas silpnesne darbo santykių šalimi, retai kreipiasi į Valstybinę duomenų apsaugos inspekciją dėl asmens duomenų pažeidimo, nes darbdavys nesuteikia pakankamai informacijos, darbuotojas bijo netekti darbo ir pan.

Temos aktualumas. Informacinės technologijos palengvina ne tik kasdieninį gyvenimą, bet ir pasitarnauja profesinėje srityje. Susistemintą informaciją yra lengviau ir pigiau valdyti. Be to, naujos technologijos ne tik sutaupo laiko darbo funkcijoms atlikti, tačiau ir kelia riziką pažeisti darbuotojo teisę į privatumą. Darbdavys, būdamas asmens duomenų valdytoju, dažnai peržengia ribas ir pamirštą esminius ir conceptualius dalykus: tokius kaip kandidato, darbuotojo informavimo apie duomenų tvarkymą, sutikimo gavimą dėl atvaizdo panaudojimo, vaizdo, garso stebėjimo ir pan.

Darbo originalumas. Šios temos originalumas pasižymi tuo, kad tarp begalės straipsnių, rekomendacijų, gairių ir kitų dokumentų, nerasime vientisos analizės asmens duomenų darbo teisės kontekste, kurioje būtų išanalizuotos egzistuojančios problemos darbo santykiuose nuo gyvenimo aprašymo išsiuntimo iki darbo santykių pabaigos. Šiame darbe ne tik atskleidžiami probleminiai aspektai, tačiau taip pat lygiagrečiai pateikiami pasiūlymai ir sprendimo būdai, kurie padės darbdaviui apsaugoti duomenų subjekto duomenis, siekiant išvengti pažeidimo ir galimybės juos atskleisti trečiosioms šalims.

Tyrimo objektas. Šio darbo objektas yra BDAR reguliavimo įtaka darbo santykių, kartu siekiant išanalizuoti esminius ir svarbiausius BDAR taikymo probleminius aspektus darbo vietoje ir už jos ribų.

Darbo tikslas. Šio darbo tikslas yra įvertinti BDAR reguliavimo problematiką darbo sutarties sudarymo ir vykdymo kontekste, kartu pateikiant pasiūlymus, kurie padėtų mažinti duomenų pažeidimų atvejus Lietuvos darbo teisėje.

Uždaviniai:

1) išnagrinėti ikisutartiniuose santykiuose esantį BDAR nuostatų tarpusavio ryšį su darbo teise;

2) pateikti racionalius pasiūlymus darbdaviui, siekiant efektyviau spręsti asmens duomenų srityje kylančias problemas darbo santykių vykdymo procese;

3) išnagrinėti BDAR suderinamumą su konkrečiais Lietuvos teisės aktais darbo santykiams pasibaigus;

Tyrimo metodai:

1) **loginis** – šiuo metodu darbo autorė siekė teikti pasiūlymus bei racionalius sprendimo būdus, kurie padėtų darbdaviams išvengti pažeidimų asmens duomenų apsaugos darbo teisės srityje;

2) **lingvistinis** – šio metodo pagalba buvo lingvistiškai aiškinamos BDAR nuostatos bei jų sąsaja su darbo teise nuostatomis;

3) **lyginamasis** – šio metodo pagalba buvo analizuojamas BDAR suderinamumas su Lietuvos Respublikos darbo kodeksu, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu, taip pat lyginami Europos Sąjungos Teisingumo teismo, Europos Žmogaus teisių teismų formuojama praktika su Lietuvos Aukščiausio teismo, Lietuvos vyriausiojo administracinio teismo ir žemesnių instancijų teismų išaiškinimais;

4) **sisteminis** – šio metodo pagalba buvo siekiama išanalizuoti BDAR nuostatas, koreliuojančias su konkrečiais Lietuvos teisės aktais darbo santykių kontekste.

Svarbiausi šaltiniai. Daugiausiai dėmesio šiame rašto darbe buvo skiriama BDAR nuostatomis, Lietuvos Respublikos darbo kodeksui, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymui. Darbe analizuojamos Europos Žmogaus teisių teismo, Europos sąjungos teisingumo teismo, Lietuvos Aukščiausio teismo, Lietuvos vyriausiojo administracinio teismo ir kita Lietuvos teismų formuojama praktika. Šiame darbe remiamasi ir J. Zaleskio, I. Petrylaitės, G. Tamašauskaitės-Jancikės, C. Ogriseg, M.C. Eklund straipsniais, Europos Komisijos sudarytais *soft law* šaltiniais ir darbais.

1. Ikisutartiniai santykiai ir BDAR

Įdarbinimo procesas yra procesas, skirtas nustatyti laisvą darbo vietą, išanalizuoti darbo reikalavimus, peržiūrėti paraiškas, atrinkti ir pasirinkti tinkamą kandidatą. Šiandieninėje visuomenėje darbo rinkos pasiūla ir paklausa dažnai vykdoma per socialines medijas (pvz., „LinkedIn“), darbo skelbimo portalus (pvz., „CV-online“, „CV bankas“, „CV market“ ir pan.), viešuosius renginius (pvz., Vilniaus universiteto karjeros dienos), skelbimus (laikraščiai, stendai ir pan.) ir kt. Platus pasirinkimo spektras atveria ne tik naujas galimybes, bet ir sukelia pavojus asmens duomenų srityje. Kadangi BDAR taikoma fiziniams asmenims, tai reiškia, kad ikisutartinių santykių procese asmens duomenų teisės sritis reguliuoja ne bet kokių duomenų, o būtent fizinio asmens duomenų tvarkymą.

Paprastai, žmogiškųjų išteklių specialistas, gavęs gyvenimo aprašymą iš kandidato, pradeda pirminę analizę, kurios metu nagrinėjami kandidato pateikti bendro pobūdžio duomenys (darbo patirtis, išsilavinimas ir pan.). Praėjęs pirminę atranką, kandidatas paprastai kviečiamas į darbo pokalbį, kurio metu vertinama, ar jis tinkamas laisvai darbo pozicijai. Keliami klausimai atskleidžia kandidato gyvenimo būdą bei darbinę patirtį. Gali būti atvejų, kai kandidatui duodamos užduotys, testai. Šis formatas naudojamas siekiant plačiau atskleisti žinias ir kompetenciją darbo srityje. Natūralu, kad skirtingos įmonės, įstaigos ar organizacijos turi skirtingus vidinius atrankos procesus, tačiau tai neginčija fakto, kad informacija apie kandidatą tampa žinoma ne tik žmogiškųjų išteklių specialistui, bet ir platesniam asmenų ratui. Ikisutartiniai santykiai, kaip ir darbo santykiai, kuriuos siekiama sukurti, gyvenime reikšmingai skiriasi, todėl negalima teigti esant vienodam šalių elgesio standartai visiems ikisutartiniams santykiams. Pavyzdžiui, pokalbio dėl darbo metu suteikiamos informacijos kiekis ir turinys kiekvienu atveju, atsižvelgiant į darbuotojo profesiją ar darbdavio ekonominės veiklos rūšį bei įprastą darbo rinkoje praktiką, gali būti labai skirtingi (Davulis, 2018, p. 166).

Atrankos procedūra yra būtina įdarbinimo proceso dalis, norint atrinkti darbuotojus į konkrečias darbo vietas pagal konkrečius kriterijus. Ikisutartinių santykių procese žmogiškųjų išteklių specialistas gavęs gyvenimo aprašymą, motyvacinį laišką ar kitą su kandidatu susijusią informaciją sužino tokius duomenis kaip vardas, pavardė, informaciją apie išsilavinimą, darbo patirtį, užsienio kalbų lygį ir pan.

Pasauliui tampant vis labiau inovatyviam, informacinės technologijos sukuria papildomą naudą individams ne tik jų privačiame, bet ir profesiniame gyvenime. Vis dėlto, daugelis veiklų, kurios susijusios su darbo santykiais, persikelia į skaitmeninę erdvę.

Pabrėžtina, kad dar prieš pradedant užmezgant kontaktą su potencialiu darbuotoju reikia identifikuoti, ar tikrai kandidato siunčiamas gyvenimo aprašymas patenka į BDAR taikymo sritį. Vadinasi reikia išsiaiškinti, kas gi slypi po asmens duomenų apibrėžimu.

BDAR 4 str. 1 p., pateiktas apibrėžimas asmens duomenys – tai yra bet kokia informacija apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti (duomenų subjektas); fizinis asmuo, kurio tapatybę galima nustatyti, yra asmuo, kurio tapatybę tiesiogiai arba netiesiogiai galima nustatyti pagal identifikatorių, kaip antai vardą ir pavardę, asmens identifikavimo numerį, buvimo vietos duomenis ir interneto identifikatorių arba pagal vieną ar kelis to fizinio asmens fizinės, fiziologinės, genetinės, psichinės, ekonominės, kultūrinės ar socialinės tapatybės požymius. Taip pat galima pažvelgti, kaip ši sąvoka apibrėžiama Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo 1 str. 1 d. Nurodoma, kad įstatymo paskirtis – saugoti žmogaus pagrindines teises ir laisves, visų pirma, žmogaus teisę į asmens duomenų apsaugą ir užtikrinti aukštą asmens duomenų apsaugos lygį (Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas, 1996).

Žvelgiant į ESTT aiškinimus, vienoje iš bylų teismas nurodė, kad „asmens duomenys“ reiškia bet kurią informaciją, susijusią su asmeniu (duomenų subjektu), kurio tapatybė yra nustatyta arba gali būti nustatyta; asmuo, kurio tapatybė gali būti nustatyta, yra tas asmuo, kurio tapatybė gali būti nustatyta tiesiogiai ar netiesiogiai, ypač pasinaudojus nurodytu asmens identifikavimo kodu arba vienu ar keliais to asmens fizinei, fiziologinei, protinei, ekonominei, kultūrinei ar socialinei tapatybei būdingais veiksniais. Informacija laikoma taip, kad duomenų subjektų tapatybes būtų galima nustatyti ne ilgiau, nei tai yra reikalinga tais tikslais, dėl kurių duomenys buvo surinkti arba po to tvarkomi (Europos Sąjungos Teisingumo Teismo byla *College van burgemeester en wethouders van Rotterdam v. M. E. E. Rijkeboer*, 2008, Nr. I-3889, punktas 8). Vadinasi, kad būtų galima suvokti, kas slypi po asmens duomenų apibrėžtimi, būtina išskirti keturis pagrindinius aspektus, kurie detalizuoja, kokie konkrečiai duomenys yra laikomi asmens duomenimis. Toliau šie aspektai aptariami plačiau.

Pirmiausia aptariama vartojama frazė „bet kokia informacija“. Kalbant apie informacijos turinį, asmens duomenų sąvoka apima duomenis, kuriais pateikiama visa galima informacija. Sąvoka „asmens duomenys“ apima informaciją, susijusią su asmens asmeniniu ir šeimos gyvenimu *stricto sensu*, taip pat informaciją apie visas asmens vykdomas veiklos rūšis, pavyzdžiui, asmens darbo santykius arba ekonominę ar socialinę elgesį. Taigi apima ir informaciją apie asmenis neatsižvelgiant į jų padėtį ar pareigas (ES 29 str. duomenų apsaugos..., 2007, p. 6). Vadinasi, tai yra visa įmanoma informacija apie

asmenį: vardas ir pavardė, asmens kodas, adresas, informacija apie asmeninį ir šeimos gyvenimą, darbo santykius, sveikatą, pomėgius, batų dydį, plaukų spalvą, genetinius ir biometrinius duomenis ir t. t. Paminėtina, kad ši informacija gali būti tiek objektyvi, tiek subjektyvi ir yra visiškai nesvarbu tos informacijos teisingumas.

Taip pat duomenys yra informacija, kuri yra tiesiogiai „susijusi“ su fiziniu asmeniu. Informacija gali būti tiesiogiai susijusi per konkretų subjektą. Verta pabrėžti, kad asmens tapatybės nustatymas galimas ne tik tiesiogiai, bet ir netiesiogiai. Pavyzdžiui, netiesioginės informacijos samprata suvokiama per asmens kodą, telefono numerį, gyvenamąjį adresą, IP adresą ir pan. Tai reiškia, kad už šio duomens slepiasi konkretus šių duomenų savininkas, kuris yra pripažįstamas vartotoju.

Netiesioginės informacijos sampratą pateikė ir Lietuvos vyriausiasis administracinis teismas byloje, kurioje nurodyta, kad kai kuriais atvejais iš duomenų gaunama informacija pirmiausia yra susijusi su objektais, o ne su asmenimis. Tie objektai paprastai kam nors priklauso, jiems asmenys gali daryti tam tikrą poveikį arba jie gali daryti tam tikrą poveikį asmenims. Be to, objektai gali būti fizine ar geografinė prasme artimi asmenims arba kitiems objektams. Tokiais atvejais galima teigti, kad informacija su tais asmenimis arba objektais susijusi netiesiogiai (Lietuvos vyriausiasis administracinis teismas 2012 m. liepos 26 d. sprendimas administracinėje byloje Nr. A⁸⁵⁸-2133/2012). Kitoje byloje teisėjų kolegija nustatė, kad net fizinio asmens telefono ryšio numeris priskirtinas asmens duomenų kategorijai (Lietuvos vyriausiasis administracinis teismas 2020 m. liepos 1 d. nutartis administracinėje byloje Nr.eA-2601-629/2020).

Kitas aspektas, kuris yra susijęs su asmens duomenimis laikoma informacija, yra „su fiziniu asmeniu“. BDAR preambulės 14 punkte apibrėžiama, kad šiuo reglamentu užtikrinama apsauga turėtų būti taikoma fiziniams asmenims tvarkant jų asmens duomenis, neatsižvelgiant į jų pilietybę ar gyvenamąją vietą.

Paminėtina, kad direktyvos nuostatomis nustatyta apsauga taikoma fiziniams asmenims, t. y. žmonėms. Teisė į asmens duomenų apsaugą šia prasme yra visuotinė, neapribota konkrečios šalies piliečiams ar gyventojams.

Paskutinis išskiriamas aspektas būtų toks, kad duomenys yra informacija apie fizinį asmenį, kurio „tapatybė nustatyta arba gali būti nustatyta“. Vertinant informacijos sąsajas su asmeniu, pati informacija nebūtinai turi būti apie asmenį ir atskleisti konkrečius duomenis apie jį. Pakanka, kad ji yra ar gali būti susijusi su asmeniu tam tikrais ryšiais, sąveika ar santykiais (pavyzdžiui, adresas, automobilio valstybinis numeris, telefono numeris, sutuoktinio vardas ir kt.) (Civilka, Šlapimaitė, 2015, p. 134). Vadinasi, tam tikri asmens duomenys gali būti nuoroda į asmens tapatybę.

Paminėtina, kad duomenų apsaugos teisės norminis reguliavimas apima plačią taikymo sritį. Teisės normoms būdingas abstraktumas, bendrumas, technologinis neutralumas ir specifinė terminija. Šie reguliavimo ypatumai kelia grėsmę jo apibrėžtumui, dinamiškumui ir efektyvumui, taip pat sukelia praktinių problemų, tobulinant duomenų apsaugą. Minėtuosius duomenų apsaugos teisės iššūkius padeda išspręsti *soft law* (liet. švelnioji teisė) šaltiniai. Teisės doktrina *soft law* šaltiniais laiko elgesį reguliuojančias taisykles įtvirtintas dokumentuose, kurie neturi teisiškai privalomosios galios, tačiau vis tiek turi tam tikrų (netiesioginių) teisnių padarinių ir kuriais siekiama sukelti praktinių padarinių. Tai – kompetentingų institucijų ir ekspertų priimtos, formaliai neprivalomos, tačiau autoritetingos nuomonės, rekomendacijos, gairės. Jos padeda atskleisti ir tinkamai pritaikyti duomenų apsaugos teisės normų turinį (Zaleckis, 2019, p. 62–63). Kadangi teismai nesuformavo BDAR aiškinimo ir taikymo praktikos, pagrindinis tyrimo šaltinis yra ES 29 str. darbo grupės ir ją su BDAR pakeitusios Europos duomenų apsaugos valdybos nuomonės ir rekomendacijos – formaliai neprivaloma, tačiau autoritetinga medžiaga, kuria formuodami praktiką remiasi teismai (Zaleckis, 2019, p. 24).

Išanalizavus asmens duomenų sąvokos apibrėžimą galima teigti, kad kandidato siunčiamame gyvenimo aprašyme pateikta informacija: vardas, pavardė, gimimo data, telefono numeris, elektroninis paštas, informacija apie kandidato patirtį (darbovietė, pareigos, darbo laikotarpis, atsakomybės ir pasiekimai), informacija apie kandidato išsilavinimą (mokymosi įstaiga, laikotarpis, išsilavinimas, kvalifikacija), informacija apie kvalifikacijos kėlimą (sertifikatai, mokymai), informacija apie užsienio kalbų mokėjimą, informacija apie vairavimo kategorija ir stažą, bei kita aktuali informacija gyvenimo aprašyme patenka po BDAR reguliavimu. Nepriklausomai nuo informacijos pobūdžio ir tikrumo, to pakanka, kad būtų galima tiek tiesiogiai, tiek netiesiogiai identifikuoti duomenų subjektą.

Pagal BDAR 12 str. darbdavys yra įpareigojamas imtis priemonių, kad duomenų subjektui būtų pateikta visa BDAR nurodyta informacija apie duomenų tvarkymą. Taigi, darbdaviui leidžiama rinkti ir tvarkyti asmens duomenis, bet kandidatai turi būti teisingai informuoti (Ogriseg, 2017, p. 14).

Atkreipiamas dėmesys, kad kiekvienas darbdavys pagal BDAR 88 str. vidiniuose dokumentuose gali apsirašyti pranešimo turinį, formą, kuri bus pateikta kandidatui prieš išsiunčiant, o darbdaviui prieš gaunant gyvenimo aprašymą ar kitus susijusius dokumentus. Aiškiai suformuotos nuostatos gali atspindėti darbdavio vidiniuose dokumentuose, pavyzdžiui, įsakyme dėl kandidato asmens duomenų tvarkymo ir pan. Toliau aptariami pranešimo turinio esminiai elementai.

Visų pirma, darbdavys elektroniniu laišku, elektronine forma ar kitomis kandidatui prieinamomis priemonėmis pateikia informacinį pranešimą, koku pagrindu ir tikslu bus naudojami gauti kandidato duomenys. Darbdavys turėtų pabrėžti, kad pateikiami duomenys bus laikomi konfidencialiais, taip pat informuoti, ar kandidato įsidarbinimo anketoje ar pridedamuosiuose dokumentuose (gyvenimo aprašyme, motyvaciniame laiške ir kt.) pateikti duomenys bus įrašyti į kandidatų duomenų bazę. Pavyzdžiui, kandidato duomenų tvarkymas ar rinkimas gali būti reikalingas įvertinant kandidato kandidatūrą, pateikti pasiūlymą į laisvas darbo pozicijas ateityje, įvertinti kandidato kompetenciją, žinių bagažą, nustatyti užsienio kalbos lygį ir kt. Paminėtina, kad pranešimo turinyje kandidatui turi būti aišku ir suprantama, kam reikalingas toks duomenų tvarkymas. Greta to nurodyti, ar kiti įmonės, įstaigos ar organizacijos darbuotojai galės peržiūrėti ir naudoti kandidato pateiktus duomenis. Šiame kontekste kandidatas, būdamas savo duomenų šeimininku, privalo žinoti, kas konkrečiai kaups ir rinks duomenis apie jį.

Visgi, kandidatas turi teisę ir nesutikti su asmens duomenų tvarkymu pagal BDAR 21 str. 1 d. Paminėtina, kad kandidatas neprivalo nurodyti priežasčių dėl tokio savanoriško apsisprendimo. Pavyzdžiui, darbdavys šiuo atveju negavęs sutikimo dėl duomenų tvarkymo, neturi teisės tokiam kandidatui nesuteikti galimybės dalyvauti atrankos etape, jeigu jis atitinka visus darbo skelbime nurodytus kriterijus.

Kandidatui pranešime turėtų būti pateikta informacija, kas gali peržiūrėti gautus duomenis. Pavyzdžiui, duomenis gali peržiūrėti duomenų valdytojo darbuotojai, kurie atsakingi už personalo atranką ir įdarbinimą, padalinių vadovai, kurių skyriuje ar departamente vykdoma atranka, asmens duomenų apsaugos pareigūnas ir kt.

Kita vertus, kai duomenų valdytojas turi teisėtą interesą įtraukti kandidato duomenis į duomenų bazes, yra reikalingos ir specialios informacinės sistemos. Pavyzdžiui, siekiant efektyviau ir saugiau tvarkyti kandidato asmens duomenis, sistemų veikimą prižiūri informacinių technologijų specialistai bei profesionalios paslaugas teikiantys tiekėjai. Vis dėlto, tai darbdavio darbuotojai ar asmenys, kurie gali turėti prieigą prie kandidato duomenų, kiek tai reikalinga programinės įrangos tinkamam veikimui užtikrinti. Primintina, kad pranešime darbdavys privalo patikinti kandidatą, kad jo duomenys nebus naudojami jokiais kitomis aplinkybėmis ar teikiami tretiesiems asmenims.

Be kita ko, pranešime kandidatui turi būti pateikiama informacija, kiek laiko bus saugoma informacija apie jį. Atkreipiamas dėmesys, kad pranešime dėl kandidato asmens duomenų tvarkymo darbdavys turėtų nurodyti, kad tuo atveju, jeigu darbo pasiūlymas nepateikiamas, asmens duomenys bus saugomi ir tvarkomi kandidatų duomenų bazėse būsimums atrankos. Paminėtina, kad tokia informacija gali būti pateikiama matomoje

vietoje tiek internetinėje erdvėje, tiek darbo skelbime, tiek tiesiogiai darbdavio puslapyje. Tai reiškia, kad turi būti nurodytas konkretus terminas nuo duomenų įvedimo datos. Terminas turėtų būti proporcingas numatytiems teisėtiems interesams pasiekti. Pavyzdžiui, iki kol bus vykdoma atranka, bet ne ilgiau kaip 1 mėnesį pasibaigus atrankos procesui, ne ilgiau kaip 30 kalendorinių dienų ir pan. Ilgesnis laikotarpis gali būti privalomas ir pagal privalomus teisės aktus ar teisminių ginčų atvejus. Atkreipiamas dėmesys, kad pagal BDAR 5 str. 1 d. e p. terminas negali būti neribotas.

Atitinkamai, jeigu kandidatas atrankos metu jaučiasi diskriminuojamas, provokuojamas, užduodami klausimai nėra susiję su būsimomis darbo funkcijoms, kandidatas gali kreiptis į Darbo ginčų komisiją dėl diskriminacijos arba skųstis VDAI dėl duomenų pažeidimo. Pavyzdžiui, vienoje iš bylų teismas pripažino tiesioginės diskriminacijos faktą dėl etninės priklausomybės įsidarbinimo procese (Lietuvos apygardos teismas 2008 m. gruodžio 10 d. sprendimas civilinėje byloje Nr. 2A-1020- 464/2008).

Taip pat, kandidatas turi žinoti, kaip galima bus ateityje susipažinti su savo duomenimis, kurie bus saugomi darbdavio vidinėse duomenų bazėse. Darbdavys į pranešimo turinį turėtų įtraukti paaiškinimą kandidatui dėl teisės susipažinti su duomenimis bei galimybę juos taisyti, ištrinti, pildyti, atnaujinti. Pavyzdžiui, kandidatas atnaujina užsienio kalbų lygius, nes pabaigia akademinius kursus. Tokiu atveju, pranešime turėtų būti nurodytas elektroninis paštas, kuriuo kandidatas galėtų susisiekti dėl duomenų atnaujinimo.

Analogiškai, pranešime turėtų būti nuoroda, kur kreiptis kandidatui dėl teisių pažeidimo. Pavyzdžiui, jeigu kandidatas mano, kad jo teisės į privatumą buvo pažeistos pateikiama nuoroda, kad jis gali pateikti skundą VDAI.

Apibendrinant galima teigti, kad darbdavys privalo pateikti kandidatams privatumo pranešimą, kuriame, be kita ko, nurodomas jų duomenų tvarkymo tikslas ir teisinis pagrindas bei jų teisė nesutikti su duomenų tvarkymu. Visgi, siekiant išvengti teisminių ginčų dėl duomenų kaupimo ir rinkimo, darbdaviui rekomenduojama pateikti informatyvias, aiškias taisykles ir nuorodas, kurios aiškiai, suprantamai išdėstytų kandidatui darbdavio poziciją dėl duomenų rinkimo.

2. BDAR taikymas įsigaliojus darbo sutarčiai

Pagal Lietuvos Respublikos darbo kodekso 41 str. darbo sutartis laikoma sudaryta, kai šalys susitaria dėl būtinųjų darbo sutarties sąlygų (Lietuvos Respublikos darbo kodeksas, 2016). Būtiniosios sutarties sąlygos yra darbo funkcijos, darbo apmokėjimo ir darbovietės (Lietuvos Respublikos darbo kodeksas, 2016). Reiškia tam, kad tinkamai būtų sudaryta darbo sutartis, darbuotojas turi pateikti informaciją apie save: vardą, pavardę, gimimo datą, asmens kodą, kontaktinius duomenis, pavyzdžiui, namų adresą, telefono numerį, elektroninio pašto adresą, banko rekvizitus ir kt. Paprastai šie duomenys iš darbuotojo gaunami prieš pasirašant darbo sutartį, kadangi darbdavys turi paruošti individualiai konkrečiam asmeniui skirtą darbo sutartį.

Visgi skirtingos Europos Sąjungos valstybės eina skirtingu keliu ir darbo teisės kontekste priima nevienodus sprendimus. BDAR 88 str. 1 d. teigiama, kad valstybės narės gali teisėje ar kolektyvinėse sutartyse numatyti konkretesnes taisykles, kuriomis siekiama užtikrinti teisių ir laisvių apsaugą, tvarkant darbuotojų asmens duomenis su darbo santykiais susijusiame kontekste. Visų pirma, taisyklės numatomos juos įdarbinant, vykdant darbo sutartį, įskaitant teisės aktais arba kolektyvinėmis sutartimis nustatytą prievolių vykdymą, užtikrinant darbo administravimą, planavimą ir organizavimą, lygybę ir įvairovę darbo vietoje, darbuotojų saugą ir sveikatą, darbdavio ar kliento turto apsaugą, taip pat siekiant pasinaudoti su darbo santykiais susijusiomis individualiomis ir kolektyvinėmis teisėmis ir išmokomis ar siekiant nutraukti darbo santykius. Tai reiškia, kad norint išsiaiškinti kiekvienos valstybės lygį, priemonės darbo teisės kontekste turime žiūrėti kiekvienos valstybės nacionalinės teisės nuostatas.

Būtent Lietuvos atveju nacionalinės teisės nuostatos pateikiamos Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo 5 str. Taip pat nacionalinėje teisėje turime ir Lietuvos Respublikos darbo kodekso 27 str., kuris užsimena apie tai, kad darbdavys turi užtikrinti teisę į privatumą darbo vietoje. Visgi šios normos yra bendro pobūdžio ir konkrečiai dėl atitinkamų situacijų darbo santykiu atveju nepasisakoma. Pavyzdžiui, kiek ir kaip plačiai darbdavys gali stebėti darbuotoją, darbuotojų duomenų tvarkymo tikslai, kada pažeidžiama darbuotojo teisė į privatumą, koks yra sutikimo turinys dėl duomenų tvarkymo ir kt. Toliau darbo autorė pateiks darbo santykių vykdymo procese esančias konkrečias problemas ir sprendimo būdus dėl atvaizdo viešinimo, vaizdo, garso, automobilių GPS įrangos ir susirašinėjimo stebėjimo priemonių.

2.1. Darbuotojo duomenų apsauga darbovietėje

Kiekviena įmonė, įstaiga ar organizacija turi skyrius ar departamentus, kurie tvarko ar koordinuoja darbuotojų duomenis darbo santykių vykdymo procese. Tai reiškia, kad darbuotojas perduoda savo duomenis darbdaviui ir duomenų šeimininku (angl. *data owner*) tampa bendrovės padalinio vadovas (departamentas, departamento skyrius ar panašus organizacinis darinys Bendrovės viduje), kurio veiklos, funkcijų tikslams yra reikalingas duomenų tvarkymas.

Paminėtina, kad įmonėje, įstaigoje ar organizacijoje duomenų šeimininkas gali būti ir vienas padalinys ar net keli padaliniai, jeigu jų vykdoma duomenų tvarkymo veikla vienija bendri duomenų tvarkymo tikslai ir priemonės.

Įmonės darbuotojai ar kiti atsakingi asmenys, kuriems suteikta teisė tvarkyti darbuotojų duomenis, turi laikytis konfidencialumo principo ir laikyti paslapyje bet kokią su asmens duomenimis susijusią informaciją, su kuria jie susipažino eidami savo pareigas, nebent tokia informacija būtų vieša pagal galiojančių teisės aktų nuostatas. Pareiga saugoti asmens duomenų paslaptį taip pat galioja įmonės darbuotoją paskyrus į kitas pareigas bei pasibaigus darbo santykiams.

Vadinasi, atitinkamas padalinys nustato duomenų tvarkymo tikslus, tvarkomų duomenų apimtį, duomenų tvarkymo priemones jų veiklos, funkcijų srityje. Dažniausiai tai yra įmonėje esantys personalo, finansų skyriai ar departamentai, kurie konkrečiai apimtimi atsako už darbuotojų duomenų tvarkymo įgyvendinimą duomenų srityje.

2.1.1. Darbuotojo specialiųjų kategorijų duomenų tvarkymas

Žmogiškųjų išteklių specialistui yra pateikiami ir darbuotojų specialiųjų kategorijų duomenys. Pagal BDAR 9 str. 1 d. specialiųjų kategorijų asmens duomenys, tai duomenys, atskleidžiantys rasinę ar etninę kilmę, politines pažiūras, religinius ar filosofinius įsitikimus ar narysę profesinėse sąjungose, taip pat genetiniai duomenys, biometriniai duomenys, siekiant konkrečiai nustatyti fizinio asmens tapatybę, sveikatos duomenis (tokie duomenys susiję su fizine ar psichine fizinio asmens sveikata, įskaitant duomenis apie sveikatos priežiūros paslaugų teikimą, atskleidžiantys informaciją apie to fizinio asmens sveikatos būklę) arba duomenis apie fizinio asmens lytinį gyvenimą ir lytinę orientaciją. Pavyzdžiui, darbuotojas prieš pradėdamas vykdyti darbo funkcijas, darbdaviui privalo pateikti privalomojo sveikatos patikrinimo medicininę pažymą, kurioje pateikiami itin jautrūs asmens duomenys, susiję su sveikatos būkle.

Pagal BDAR 9 str. 2 d. darbdavys specialiųjų kategorijų asmens duomenis gali tvarkyti esant bent vienam teisėtam pagrindui. Toliau bus aptariami keli atvejai.

Pirma tai atvejai, kai tvarkyti duomenis būtina, kad darbdavys arba darbuotojas galėtų įvykdyti prievoles ir naudotis specialiomis teisėmis darbo ar socialinės apsaugos teisės srityje, kiek tai leidžiama Europos sąjungos ar valstybės narės teisėje arba pagal valstybės narės sudaryta kolektyvine sutartimi, kuriuose nustatytas tinkamos darbuotojų pagrindinių teisių ir interesų apsaugos priemonės. Pavyzdžiui, pagal Lietuvos Respublikos darbo kodekso 132 str. 1 d. darbuotojai suteikiamos nėštumo ir gimdymo atostogos. Tai reiškia, kad darbuotoja informuoja tiesioginį vadovą, bei personalo skyriui ar departamentui pateikia sveikatos priežiūros įstaigos medicininę pažymą su informacija apie nėštumą.

Antra, tvarkyti duomenis būtina profilaktinės arba darbo medicinos tikslais, siekiant įvertinti darbuotojų darbingumą. Pavyzdžiui, pagal Lietuvos Respublikos darbuotojų saugos ir sveikatos įstatymo 21 str. 1 d. darbdavys tvirtina darbuotojų, kuriems privaloma pasitikrinti sveikatą, sąrašą ir darbuotojų sveikatos patikrinimo grafiką, su juo pasirašytinai supažindina darbuotojus ir kontroliuoja, kaip laikomasi šio grafiko (Lietuvos Respublikos darbuotojų saugos ir sveikatos įstatymas, 2003). Tai reiškia, kad darbdavys pagal teisės aktus turi kontroliuoti darbuotojų sveikatos patikrinimo procesą. Tai yra, darbuotojas turi pristatyti darbdaviui pažymą, kurioje nurodoma darbuotojo sveikatos duomenys bei informaciją ar darbuotojas gali dirbti ar negali pagal nustatytas darbo funkcijas.

Taip pat tvarkyti duomenis būtina dėl viešojo intereso priežasčių visuomenės sveikatos srityje. Darbdavio pareiga užtikrinti saugias ir sveikatai nekenksmingas darbo sąlygas, įskaitant ir COVID – 19 prevenciją pagal Lietuvos Respublikos darbuotojų saugos ir sveikatos įstatymą. Tai reiškia, jog darbdavys turi pareigą rinkti tam tikrus duomenis epidemiologinės situacijos kontekste iš savo darbuotojų. Pavyzdžiui, siekiant apsaugoti darbuotojus nuo COVID-19 grėsmių sveikatai, darbdavys kas diena gali tikrinti darbuotojo temperatūrą darbo metu. Temperatūra gali būti tikrinama arba paties darbdavio paskirto atsakingo darbuotojo arba prie pagrindinio įėjimo į ofisą, gali būti įrengtas stovintis bekontaktis termometras, kuris prieš darbuotojui patenkant į patalpą, pamatuoja konkrečią darbuotojo kūno temperatūrą.

Be to, gali būti numatytas pagrindas, kad tvarkyti darbuotojo duomenis būtina, kad būtų apsaugoti gyvybiniai darbuotojo interesai, kai darbuotojas dėl fizinių ar teisinių priežasčių negali duoti sutikimo. Pavyzdžiui, kai po avarijos arba nelaimės darbuotojas yra nesąmoningas ir darbdaviui reikia surinkti informaciją apie darbuotojo sveikatą. Tokiu atveju sutikimas gali būti duodamas artimų giminaičių.

Paminėtina, kad darbdavys privalo sudaryti ir tvarkyti duomenų tvarkymo veiklos įrašus pagal BDAR 30 str. Tai būtina tam, kad darbdavys turėtų nuolatinę ir aktualią informaciją apie savo vykdomos duomenų tvarkymo veiklos apimtį, joje dalyvaujančius asmenis, naudojamas tvarkymo priemones. Tvarkymo veiklos įrašas yra pagrindinis dokumentas, kuriuo pradedamas darbdavio vykdomos tvarkymo veiklos atitikties taikomiems reikalavimams įvertinimas, todėl yra būtinas tinkamas tvarkymo veiklos įrašų sudarymo, keitimo ar atnaujinimo organizavimas nustatytoms procedūroms ar taisyklėms. Pavyzdžiui, darbdavys ketina sudaryti darbuotojų sąrašą dėl savanoriško sutikimo skiepytis AstraZeneca vakcina pagal Lietuvos Respublikos sveikatos ministro 2020 m. gruodžio 23 d. įsakymą Nr. V-3006 1.15 (įmonės turinčios daugiau negu 100 darbuotojų) arba 1.20 (darbuotojai, kurie tiesiogiai dirba su klientais) papunkčio pagrindu. Tokiu atveju turi būti įvertinta, kokius duomenis darbuotojas turi nurodyti sąrašė, kad būtų pasiektas darbdavio nustatytas tikslas.

Vadinasi, specialių kategorijų duomenų rinkimui turi būti numatyta apsauga, duomenų tvarkymo procesas bei informuoti darbuotoją, kaip sveikatos duomenys bus renkami ir naudojami. Darbdaviui rekomenduojama centralizuoti specialių kategorijų duomenis pagal BDAR 30 str.

2.1.2. Darbuotojų biometrinių duomenų tvarkymas darbo vietoje

Dauguma vardų ir pavardžių nėra unikalūs, o nustatant asmens tapatybę gali prireikti papildomų žymenų, kurie padėtų nesupainioti asmenis, su kuriuo nors kitu asmeniu. Biometriniai duomenys, pavyzdžiui, pirštų atspaudai, duomenys apie akies rainelės atvaizdą, šiame technologijų amžiuje vis dažniau naudojami asmenų tapatybei nustatyti. (Europos duomenų apsaugos teisės vadovas, 2014, p. 38)

Pagal BDAR 9 str. 1 d. nurodyta, kad draudžiama tvarkyti biometrinius duomenis, nebent būtų BDAR 9 str. 2 d. numatytos sąlygos. Analizuojant biometrinių duomenų sąvoką, pagal BDAR 4 str. 14 p. biometriniai duomenys yra 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, pavyzdžiui, veido atvaizdai arba daktiloskopiniai duomenys.

Visgi, yra dvi pagrindinės biometrinių metodų kategorijos:

1. Fizinėmis ir fiziologinėmis savybėmis pagrįstas metodas, kuris padeda įvertinti asmens fizines ir fiziologines savybes ir apima: pirštų atspaudų tikrinimą, pirštų atvaizdo analizę, akies rainelės atpažinimą, tinklainės analizę, veido atpažinimą, delno kontūrų

išdėstymą, ausies formos atpažinimą, kūno kvapo nustatymą, balso atpažinimą, DNR mėginio analizę, prakaito liaukų analizę ir kt.;

2. Elgesiu pagrįstas metodas padeda įvertinti asmens elgesį ir apima ranka pasirašyto parašo tikrinimą, naudojimosi kompiuterio klaviatūra analizę, eisenos analizę, vaikščiojimo ar judėjimo manieras, ypatybes, atskleidžiančias mąstymą sąmonėje, pvz., melavimas ir kt. (29 straipsnio darbo grupės nuomonė Nr. 3/2012 dėl biometrinių technologijų pokyčių (WP193), 2012, p. 4).

Paminėtina, kad informacinėms technologijoms sparčiai judant į priekį, vis dažniau, darbdaviai darbo vietoje naudoja biometrinę informaciją. Darbdaviai biometrinius duomenis naudoja šioms prieigoms:

Pirma, laiko matavimui, pavyzdžiui, pirštų atspaudų naudojimas ar rankos nuskaitymas norint įspausti ir išjungti biometrinius laikrodžius.

Antra, elektroninė apsauga ir prieiga prie pastato. Pavyzdžiui, tinklainės nuskaitymo naudojimas, veido atpažinimas arba pirštų atspaudų technologija darbuotojo prieigai eiti į darbdavio fizines patalpas, užuot naudoję slaptažodžius ar tradicinės asmens tapatybės kortelės.

Trečia, prieigai prie darbdavio suteiktos darbo vietos įrangos, tokios kaip kompiuterių sistemos, kopijavimo aparatų ir nešiojamųjų kompiuterių, planšetinių kompiuterių, išmaniųjų telefonų, naudojamas veido atpažinimas ar pirštų atspaudų technologija. (Reuters, 2018, p. 2)

Lietuvos kontekste teismų praktika šiuo klausimu yra negausi. Dar 2020 m. balandžio 2 d. teisėjų kolegija byloje nurodė, kad darbdavys darbuotojų biometrinius duomenis tvarkė neturėdami darbuotojų sutikimų, kurie reikalingi pagal BDAR 6 str. 1 d. a p. Byloje nebuvo įrodymų, kad darbdavys turėjo sutikimus tvarkyti biometrinius duomenis ir (arba) buvo informavę savo darbuotojus apie jų pirštų atspaudų rinkimo ir tvarkymo tikslus, duomenų subjektų teises ir pan. Taip pat šios bylos kontekste, teisėjų kolegija padarė išvadą, darbdavys tvarkė biometrinius darbuotojų duomenis dėl patogumo ir ekonomiško. Atsižvelgia į tai, biometrinių duomenų naudojimas darbdavio nustatytam tikslui pasiekti, nelaikytinas teisėtu interesu net ir vykdant darbo laiko apskaitą, jeigu nebuvo gautas iš anksto rašytis ar žodinis darbuotojo sutikimas (Lietuvos vyriausiojo administracinio teismo 2020 m. balandžio 2 d. sprendimas administracinėje byloje Nr. A-3345-822/2020). Nors, BDAR nepateikia nuorodos, koku būdu turi būti gautas sutikimas dėl asmens duomenų tvarkymo, pavyzdžiui, raštu, žodžiu ar konkludentiniais veiksmais, tačiau darbdaviui rekomenduojama iš darbuotojo sutikimą gauti raštu. Ši rekomendacija pagrįsta per įrodinėjimo prizmę tam, kad jeigu paaiškėtų pažeidimai arba darbuotojas reikalautų

patvirtinimo, kokių pagrindų jo duomenys yra saugomi, renkami, kaupiami ir pan. Rašytinis darbuotojo sutikimas dėl biometrinių duomenų tvarkymo, pagelbėtų darbdaviui tvarkingai, aiškiai ir struktūrizuotai gintis teisiniuose ginčuose.

Kitoje byloje, nagrinėjamu atveju Amsterdamo teismas nustatė, kad biometriniai duomenys gali būti laikomi informacija, susijusia su fiziniu asmeniu, nes tai yra duomenys, kurie pagal savo pobūdį teikia informaciją apie konkretų asmenį. Naudojant biometrinius duomenis, tokius kaip pirštų atspaudai, asmuo gali būti atpažįstamas ir gali būti atskiriamas nuo kito asmens. Šioje byloje esminis momentas buvo tas, jog darbuotojų biometrinių duomenų tvarkymas buvo nustatytas darbdavio vienašališku sprendimu (darbuotojas negalėjo pasinaudoti teise nesutikti su biometrinių duomenų tvarkymu), todėl šios bylos kontekste darbuotojų sutikimo nebuvo. Teismas padarė išvadą, kad pirštų atspaudų autorizavimo sistema pažeidė BDAR (Amsterdamo apylinkės teismo sprendimas, 2019 m. rugpjūčio 12 d., Nr. 7728204 CV VERZ 19-9686).

Visgi, šios temos kontekste sutikimas yra esminis rodiklis, suteikiantis darbdaviui teisę rinkti, kaupti, saugoti darbuotojo biometrinius duomenis. BDAR griežtinami sutikimo, kaip vieno iš alternatyvių duomenų tvarkymo pagrindų, reikalavimai (Zaleckis, 2017, p. 47).

Vadinasi, darbdaviui pravartu turėti rašytinį darbuotojo sutikimą dėl biometrinių darbuotojo duomenų tvarkymo. Toliau bus aptariami sutikimo esminiai turinio elementai.

Pirmiausia, sutikime turėtų atsispindėti informacija apie darbuotoją, pavyzdžiui, vardas, pavardė, sutikimo pasirašymo data, parašas. Šiame dokumente duomenų subjektui turėti būti aišku, kas yra duomenų valdytojas. Pavyzdžiui, nurodyti įmonės, įstaigos, organizacijos pavadinimą, adresą bei kontaktinius duomenis.

Darbdaviui rekomenduojama nurodyti teisinį pagrindą ar interesą, dėl biometrinių duomenų panaudojimo darbe. Pavyzdžiui, vykdyti darbines funkcijas (biometriniai duomenys t. y. darbuotojo piršto antspaudas, bus naudojamas tam, kad darbuotojui būtų suteikta galimybė dirbti su labai konfidencialiais dokumentais) ir pan. Visgi darbdaviui tokiu būdu yra lengviau sekti, kokie darbuotojai prisijungia prie konkrečios sistemos. Jeigu bus padaryta darbdaviui žala, pavyzdžiui, atskleista labai konfidenciali informacija trečiosioms šalims, darbdavys pagal prisijungimo laiką ir biometrinius duomenis, galės patikrinti, kokie asmenys konkrečiu laiku jungėsi prie sistemos.

Be to, sutikime turėtų būti nurodytas sutikimo galiojimo terminas. Pavyzdžiui, iki darbo santykių pabaigos, iki kol darbuotojas neatšauks sutikimo ir pan. Atkreipiamas dėmesys, kad pagal BDAR 5 str. 1 d. e p. terminas negali būti neribotas.

Sutikime taip pat turėtų būti išvardinta bei suteikta galimybė darbuotojui žinoti informaciją apie sutikimo atšaukiamumą, teisę susipažinti su tvarkomais dokumentais, teisę pateikti skundą VDAI dėl duomenų pažeidimo ir pan.

Visgi, esminė problema biometrinių duomenų rinkimo kontekste yra darbuotojo prieštaravimas dėl biometrinių duomenų panaudojimu darbo vietoje. Pavyzdžiui, kad darbdavys galėtų tinkamai apskaičiuoti darbuotojo darbo laiką, darbuotojas gauna individualią kortelę, kurios pagalba žymisi laiko apskaitą: kada ateina į darbą, kada išeina į pietų pertrauką, kada išeina namo. Toks darbdavio biometrinių duomenų tikslas yra pagrindžiamas tinkamos apskaitos vedimu, pavyzdžiui, apskaičiuoti viršvalandžius ir pan. Kitas pavyzdys, kai darbuotojo biometriniai duomenys yra naudojami turint prieigą prie tam tikrų vietų, pastatų, paslaugų, produktų, informacinių ar darbo proceso sistemų. Pavyzdžiui, įkelti dokumentus į konkrečią sistemą reikalingas darbuotojo „SmartID“ prisijungimo kodas, kuris sugeneruojamas per darbuotojo bankininkystę. Vadinasi, biometriniai duomenys gali būti tvarkomi, jei tapatybė su šiais duomenimis yra reikalinga tapatybės patvirtinimo ar saugumo tikslais.

Daroma išvada, pagal BDAR 9 str. 1 d. biometriniai darbuotojų duomenys yra priskiriami prie draudžiamų duomenų tvarkymo kategorijos, nebent yra numatytos išimtys pagal BDAR 9 str. 2 p. Taip pat, darbdavys privalo turėti darbuotojo sutikimą bei kritiškai įvertinti, ar toks duomenų rinkimas yra būtinas pagal iš anksto nustatytą teisinį interesą. Vadinasi, toks duomenų rinkimas būtų teisėtas, jeigu darbdavys pagrįstai sugebėtų įrodyti, kad darbuotojas buvo tinkamai informuotas ir raštu supažindintas su darbdavio viduje galiojančiais lokaliniais aktais.

2.1.3. Kiti darbuotojų tvarkomi duomenys darbo vietoje

Daugelis organizacijų naudoja duomenų bazes sudėtingiems duomenims saugoti. Duomenų bazės dažniausiai grindžiamos debesimis (angl. *cloud-based*) ir yra labai efektyvūs vykdant ataskaitas ir vizualizuojant duomenis. Žmogiškųjų išteklių skyriuje ar departamente saugomi duomenys apima išsamią informaciją apie darbuotoją atostogas, darbo valandas, rotaciją ir kt. (Nocker, Sena, 2019, p. 4)

Darbo sutarčių sudarymo, vykdymo, apskaitos ir duomenų valstybės institucijoms teikimo tikslais yra tvarkomi darbuotojų: vardai, pavardės, asmens ir kiti identifikaciniai kodai, gimimo datos, socialinio draudimo numeriai, pareigos, kontaktiniai duomenys (gyvenamosios vietos adresai, telefono numeriai ir asmeninio elektroninio pašto adresai), duomenys apie šeiminę padėtį (dėl mokestinės lengvatos), duomenys apie priėmimą

(perkėlimą) į pareigas, atleidimą iš pareigų, duomenys apie mokymą, atostogas, darbo užmokestį, išeitines išmokas, kompensacijas, pašalpas, informacija apie dirbtą darbo laiką, skatinimus ir nuobaudas, banko sąskaitų numerių duomenis, reikalingus atlyginimams ir kitoms išmokoms darbuotojams pervesti. Teisės aktuose nustatytų įmonės pareigų tinkamo vykdymo tikslu yra tvarkomi darbuotojų: asmens kodai, informacija apie išsilavinimą, informacija apie darbuotojų šeiminių padėtį (darbuotojui pageidaujant mokestinės lengvatos).

Taip pat personalo skyriui ar departamentui yra žinomi tokie darbuotojų duomenys, kaip informacija apie buvimą santuokoje, ankstesnė darbuotojos pavardė, skatinimų programos duomenys (kuro limitas, pokalbių ryšio limitas, stovėjimo aikštelės pultelis ir pan.), sveikatos draudimo kortelės numeris, darbo laiko grafikas, informacija apie nedarbingumą, mokymosi kursuose darbuotojų atlikti veiksmai (kurso pavadinimas, kurso peržiūra, testo atlikimas, įvertinimo gavimas, veiksmo atlikimo laikas, trukmė), atskaitomybės, veiklos vertinimas, praėjusių metų atskaitomybės tikslai ir pan.

Paminėtina, kad pagal Lietuvos Respublikos darbo kodeksą 125 str. išvardintos atostogų rūšys, kurios darbuotojas gali pasinaudoti darbo laikotarpiu. Tai reiškia, kad žmogiškųjų išteklių specialistas registruoja ir tvarko prašymus gautus dėl atostogų sutrikimo. Po to, ši informacija apie atostogų trukmę perduodama buhalterijos skyriui, kuri apskaičiuoja ir išmoka atlygį už kasmetinių atostogų panaudojimą. Tai reiškia, kad ir buhalterijos skyriui yra žinomi darbuotojo duomenys apie banko sąskaitą (banko pavadinimas, kodas, sąskaitos numeris)

Be to, pagal Lietuvos Respublikos darbo kodekso 148 str. 1 d. darbdavys ne rečiau kaip kartą per mėnesį raštu ar elektroniniu būdu privalo darbuotojui pateikti informaciją apie jam apskaičiuotas, išmokėtas ir išskaičiuotas sumas ir apie dirbto darbo laiko trukmę, atskirai nurodydamas viršvalandinių darbų trukmę. Pavyzdžiui, buhalterija kiekvieną mėnesį darbuotojo asmeniniu arba darbinio elektriniu paštu atsiunčia atsiskaitymo lapelį. Ataskaitiniame lapelyje buhalterija pateikia, tokius duomenis, kaip darbuotojo vardas, pavardė, pareigos, tabelio numerį, informaciją apie priėmimo datą, darbo užmokestį, nepanaudotų atostogų likutį ir pan. Tai reiškia, kad vidaus administravimo tikslu (struktūros tvarkymas, personalo valdymas, turimų materialinių ir finansinių išteklių valdymas ir naudojimas, raštvedybos tvarkymas ir kt.) gali būti tvarkomi darbuotojui būdingi fizinio, fiziologinio, psichologinio, ekonominio ar socialinio pobūdžio duomenys, turintys įtaką darbo funkcijoms ir galimybei jas vykdyti, kuriuos reikia tvarkyti dėl įmonės siekiamų teisėtų interesų, jei darbuotojo interesai nėra svarbesni.

Paminėtina, kad darbuotojų duomenys gali būti žinomi ne tik darbdavio vidiniams skyriams ar departamentams, tačiau ir tretiesiems asmenims. Tretiesiems asmenims duomenys teikiami tik įstatymų ir kitų teisės aktų nustatytais atvejais ir tvarka:

1. Darbuotojų duomenys: socialinio draudimo mokesčio administravimo tikslu – Valstybinio socialinio draudimo fondo valdybai prie Socialinės apsaugos ir darbo ministerijos, mokesčių administravimo tikslu – Valstybinei mokesčių inspekcijai prie Lietuvos Respublikos finansų ministerijos;

2. Kitiems tretiesiems asmenims, kuriems asmens duomenis teikti įmonę įpareigoja įstatymai ar kiti teisės aktai;

3. Darbuotojų duomenys taip pat gali būti teikiami įmonės atžvilgiu veikiantiems kitiems duomenų tvarkytojams (pvz., įmonėms, kurios yra įmonės naudojamų informacinių sistemų valdytojos ir turi prieigą prie asmens duomenų), kurie teikia paslaugas įmonei ir jos vardu tvarko asmens duomenis. Duomenų tvarkytojai tvarko asmens duomenis tik pagal įmonės nurodymus ir tik tokia apimtimi, kuri yra būtina tikslų įgyvendinimui.

Vadinasi, darbuotojų duomenis turi teisę tvarkyti tik tie asmenys, kuriems jie yra būtini darbo funkcijų vykdymui, ir tik tuomet, kai tai yra būtina atitinkamiems tikslams pasiekti.

2.2. Darbuotojo sutikimas dėl atvaizdo išviešinimo

Įsigaliojus darbo sutarčiai darbdaviui gali iškilti poreikis fotografuoti, filmuoti darbuotojus individualiai ar bendrame įmonės darbuotojų kontekste. Pavyzdžiui, įvairių įmonės švenčių, renginių, seminaro ar mokymų metu. Taip pat įmonės internetiniuose puslapiuose galima pastebėti ir portretines darbuotojų nuotraukas, po kuriomis pateikiama darbuotojo kontaktinė informacija ir pan. Reprezentavimas gali būti išreiškiamas įvairiomis formomis, tačiau darbdavys neturėtų pamiršti apie darbuotojo sutikimą dėl atvaizdo išviešinimo. Paminėtina, kad ESTT byloje teismas išdėstė poziciją, kad užfiksuotas asmens atvaizdas yra asmens duomuo (Europos Sąjungos Teisingumo Teismo 2014 m. gruodžio 11 d. sprendimas byloje C-212/13 František Ryneš v. Úřad pro ochranu osobních údajů).

Teisės į atvaizdą apibrėžtį galime rasti Lietuvos Respublikos civilinio kodekso 2.22 str. 1 d. kuriame nurodoma, kad fizinio asmens nuotrauka (jos dalis), portretas ar kitoks atvaizdas gali būti atgaminami, parduodami, demonstruojami, spausdinami, taip pat pats asmuo gali būti fotografuojamas tik jo sutikimu (Lietuvos Respublikos civilinis kodeksas, 2000).

Paminėtina, jog visada būtina gauti sutikimą prieš tai, kai duomenų valdytojas pradeda tvarkyti asmens duomenis, dėl kurių reikia sutikimo. Savo nuomonėse ES 29 str. darbo grupė nusprendė, kad sutikimas turėtų būti duodamas prieš pradedant duomenų

tvarkymo veiklą. Nors BDAR 4 str. 11 d. nėra pažodžiui nurodyta, kad sutikimas turi būti duodamas iki duomenų tvarkymo veiklos pradžios, tai aiškiai turima omenyje. Tokį aiškinimą patvirtina 6 str. 1 d. įvadinė frazė ir formuluotė „davė“ (sutikimą) 6 str. 1 d. a punkte. Iš 6 str. ir 40 konstatuojamosios dalies nuostatų logiškai seka tai, kad galiojantis teisėtas pagrindas turi būti nustatytas prieš pradedant tvarkyti duomenis (Europos duomenų apsaugos valdyba, 2020, p. 20).

Kadangi teisė į atvaizdą yra sudėtinė teisės į privatų gyvenimą dalis (Lietuvos Aukščiausiojo teismo Civilinių bylų skyriaus 2008 m. sausio 1 d. nutartis civilinėje byloje Nr.3K-7-2/2008), tais atvejais, kai darbdavys nori viešinti darbuotojo atvaizdą socialiniuose tinkluose, įmonės, įstaigos ar organizacijos vidiniuose tinklapiuose ar kitoje marketingo medžiagoje, darbdavys privalo iš anksto gauti darbuotojo rašytinį sutikimą dėl atvaizdo panaudojimo pagal BDAR 6 str. 1 d.

Šiuo nagrinėjamu aspektu galima paminėti Vilniaus apygardos teismo bylą, kurioje buvo analizuojamas klausimas dėl darbuotojo nuotraukos prieinamumo socialiaame tinkle „Facebook“. Teismas nurodė, kad darbuotojo nuotraukos patalpinimas ir jos prieinamumas socialiniame tinkle „Facebook“ pats savaime nereiškia, jog asmuo konkludentiniais veiksmais sutinka, kad jo atvaizdas būtų naudojamas atgaminant ir platinant jį masinės informacijos priemonėse (Vilniaus apygardos teismo Civilinių bylų skyriaus 2019 m. kovo 18 d. nutartis civilinėje byloje Nr. e2A-588-656/2019). Paminėtina, kad sutikimas gali būti duotas tiek žodžiu, tiek raštu, tiek ir konkludentiniais veiksmais (Lietuvos vyriausiojo administracinio teismo 2021 m. sausio 13 d. nutartis administracinėje). Pasitaiko situacijų, kai darbuotojas dėl atvaizdo panaudojimo sutikimą išreiškia konkludentiniais veiksmais. Vis dėlto, atsakomybė ir įrodinėjimo našta dėl sutikimo egzistavimo išlieka darbdaviui. Siekiant palengvinti įrodinėjimo našta, darbdaviui rekomenduojama turėti rašytinį darbuotojo sutikimą dėl atvaizdo panaudojimo.

Kiekvienas asmuo turi teisę į tai, kad būtų gerbiamas jo privatus ir šeimos gyvenimas, būsto neliečiamybė ir komunikacijos slaptumas, kiekvienas asmuo turi teisę į savo asmens duomenų apsaugą (Vilniaus apygardos teismo Civilinių bylų skyriaus 2018 m. lapkričio 20 d. nutartis civilinėje byloje Nr. 2A-1417-614/2018).

Visgi tam, kad būtų galima suvokti teisės į atvaizdą reikšmę šiame skaitmeniniame pasaulyje, paminėtina, jog technologijų pagalba jau yra generuojamos veido atpažinimo sistemos. Veido atpažinimas yra automatinis skaitmeninių vaizdų, kuriuose yra asmenų veidai, apdorojimas, siekiant identifikuoti ar patikrinti tuos asmenis, naudojant veido šablonus. Iš esmės, veido atpažinimo sistemos veikimo principą galima būtų suskirstyti į tris žingsnius: veido aptikimą (sistema atpažįsta ir suranda žmogaus veidą vaizdiniuose ar

vaizdo įrašuose), veido fiksavimą (žmogaus veidas, jo veido bruožai yra transformuojami į skaitmeninės informacijos (duomenų) rinkinį) ir veidų atitikimo procesą (šio proceso metu tikrinama, ar du veidai priklauso tam pačiam asmeniui). Paminėtina, kad veido atpažinimo priemonių naudojimas turi būti įvertintas atsižvelgus į proporcingumą tikslui ir poveikiui duomenų subjekto teisėms. Skaitmeninių vaizdų, patalpintų internete, įskaitant socialinę mediją, ar iš nuotraukų tvarkymo svetainių internete, ar tų, kurie buvo užfiksuoti per stebėjimo kameras, naudojimas negali būti laikomas teisėtu remiantis tik tuo, kad tokie asmens duomenys buvo aiškiai prieinami (TeisėPro, 2021). Paminėtina, kad ir šiais atvejais privalo būti rašytinis darbuotojo sutikimas dėl automatizuotų priemonių būvimo ir naudojimo darbe.

Šios temos kontekste didžiausia problema yra tuomet, kai darbdavys nežino, kad dėl kiekvieno atvaizdo panaudojimo būdo turi būti gautas atskiras darbuotojo sutikimas. Pavyzdžiui, kai vyksta įmonės vasaros šventės, renginiai, konkursai, ar kai darbdavys socialiniame tinkle nori „pažymėti“ darbuotoją, taip atskleisdamas jo socialinių tinklų paskyrą ir pan. Todėl, dėl kiekvieno iš šių veiksmų, turi būti gaunamas individualus rašytinis darbuotojo sutikimas. Paminėtina, kad prieš duodant darbuotojui sutikimo dokumentą, darbuotojas turi būti supažindinamas su sutikimo turiniu pagal BDAR 13 str. Tai atvejais, kai darbdavys neturėdamas išankstinio darbuotojo sutikimo, paviešina nuotrauką socialiniuose tinkluose, internetiniuose puslapiuose ir pan. darbdavys pažeidžia darbuotojo teisę į privatumą. Šiuo atveju, darbuotojui pareikalavus darbdavys privalo nedelsiant ištrinti arba pašalinti nuotrauką. Bet kuriuo atveju, darbdavys negali reikalauti iš darbuotojo paaiškinimo dėl atvaizdo panaudojimo nesutikimo.

Pirmiausia, sutikimo turinyje turėtų būti nurodytas duomenų tvarkymo tikslas. Pavyzdžiui, darbuotojo portretinės nuotraukos viešinimas darbdavio internetinėje svetainėje, tikslas yra informuoti klientus apie paslaugą teikiančio asmens profilį: kompetenciją, kontaktinius duomenis.

Taip pat sutikime turėtų būti nuoroda, kas yra nuotraukų ar vaizdo įrašų gavėjai. Pavyzdžiui, įmonės, įstaigos, organizacijos darbuotojai, duomenų valdytojai, tretieji asmenys ir pan.

Atitinkamai, sutikime turėtų būti apibrėžtas terminas, kiek tokie duomenys bus saugojami ir naudojami. Pavyzdžiui, iki darbuotojo darbo sutarties pabaigos, sutikimo atšaukimo ir pan.

Galiausiai, dokumente turėtų būti suteikta galimybė darbuotojui tiek sutikti, tiek nesutikti su tokio pobūdžio duomenų tvarkymu. Pagal BDAR 7 str. 3 d. duomenų subjektui bet kuriuo metu turėtų būti suteikta teisė ir atšaukti duotą sutikimą. Pavyzdžiui, darbuotojas

įvertinęs prieš tai buvusio renginio nuotraukas nusprendžia, kad nebenori, jog jo atvaizdas būtų viešinamas socialinėje erdvėje. Tokiu atveju darbuotojas kreipiasi į darbdavį ir prašo atšaukti jo sutikimą dėl atvaizdo naudojimo šios temos kontekste. Darbuotojas neprivalo nurodyti priežasčių dėl tokio apsisprendimo, kadangi atvaizdas yra darbuotojo duomuo.

Paminėtina, kad kai planuojami renginiai, įmonės šventės ir kt., kuriuose dalyvauja didelis kiekis darbuotojų, darbdavys prieš darbuotojui patenkant į renginio patalpą, privalo iš anksto informuoti, kad renginys bus filmuojamas ar fotografuojamas. Pavyzdžiui, prieš renginį el. paštu ar kitais darbuotojui priimtinais būdais nusiųsti informacinį pranešimą, kad renginys / šventė konkrečioje vietoje ir konkrečiu laiku bus filmuojamas ar fotografuojamas. Tokiu atveju, darbuotojas atvykdamas į renginį / šventę, konkludentiniais veiksmais sutinka dėl filmavimo ar fotografavimo.

Taigi, sutikimas privalo būti aiškus, suprantamas ir apibrėžtas. Darbdaviams rekomenduojama šį dokumentą pridėti, kaip priedą prie darbo sutarties arba šias nuostatas apibrėžti darbo sutartyje, leidžiant darbuotojai turėti pasirinkimo teisę dėl sutikimo arba nesutikimo. Akcentuojama, kad darbdavys privalo ypač didelį dėmesį skirti sutikimo turiniui, kad ateityje kilus ginčui sugebėtų įrodyti sutikimo teisėtumą.

2.3. Darbuotojų stebėjimas vaizdo ir garso priemonėmis

Šiandieninis pasaulis sparčiai juda į priekį: naujos technologijos keičia mūsų gyvenimą akimirksniu, o profesinėje srityje darbas tampa efektyvesnis ir modernesnis. Pabrėžiama, kad nors techninės priemonės, tokios kaip stebėjimo kameros ar garso įrašymo įranga, palengvina darbdaviui galimybę stebėti, kaip darbuotojas atlieka darbo funkcijas, kaip tausoja ir saugo darbdavio suteiktas darbo priemonės, tačiau kartu jų pasitelkimas gali kelti rimtą pavojų darbuotojo privačiam gyvenimui.

Remiantis Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo 5 str. 3 d. 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, pateikiant Reglamento (ES) 2016/679 13 str. 1 ir 2 d. nurodytą informaciją (Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas, 1996). Vadinasi, Lietuvos teisės aktuose ši nuostata tik patvirtina, kad vaizdo ir garso stebėjimas yra neatsiejamas nuo darbdavio pareigos informuoti darbuotoją apie šiuo vykdomus veiksmus. Iš principo egzistuojanti darbdavio teisei vykdyti vaizdo ar garso stebėjimą, svarbu išsiaiškinti, dėl ko egzistuoja ši darbdavio pareiga.

Pirmiausia, darbuotojų stebėseną turėtų būti suderinta su duomenų tvarkymo tikslo apribojimo principu, kuriuo remiantis reikalaujama, kad duomenys būtų renkami nustatytais tikslais, aiškiai apibrėžti bei teisėtais tikslais ir toliau netvarkomi su tais tikslais nesuderintu būdu (BDAR 5 str. 1 d. b p.). Pavyzdžiui, vaizdo stebėjimas ir garso įrašymas darbo vietoje turėtų būti vykdomas tada, kai dėl darbo specifikos būtina užtikrinti asmenų, turto ar visuomenės saugumą ir kitais atvejais, kai kiti būdai ar priemonės yra nepakankamai ir (arba) netinkami siekiant išvardytųjų tikslų. Vadovaujantis atskaitomybės principu, duomenų valdytojas turėtų įvertinti, ar darbo vietoje atliekant vaizdo ar garso įrašymą atitinka minėtuosius bendrojo pobūdžio reikalavimus, ir gebėti tai įrodyti (BDAR 5 str. 2 d.). Turėtų būti paisoma principų būtinumo, tikslo apribojimo, skaidrumo, duomenų subjektų teisių, proporcingumo, duomenų tikslumo, saugumo ir saugojimo trukmės apribojimo reikalavimai. Specialieji reikalavimai padeda detalizuoti, kaip bendrieji duomenų subjektų informavimo apie duomenų tvarkymą reikalavimai (BDAR 13 ir 14 str.) turėtų būti įgyvendinami vykdant darbuotojų stebėseną (Zaleckis, 2019, p. 259).

Pagal BDAR 35 str. 4 d. išdėstyta, kad priežiūros institucija sudaro ir viešai paskelbia tų rūšių duomenų tvarkymo operacijas, kurioms taikomas reikalavimas atlikti poveikio duomenų apsaugai vertinimą.

Valstybinės duomenų apsaugos inspekcijos įsakyme Nr. 1T-35 dėl Duomenų tvarkymo operacijų, kurioms taikomas reikalavimas atlikti poveikio duomenų apsaugai vertinimą, sąrašo patvirtinimo nurodoma, kad darbdavys turėtų atlikti poveikio duomenų apsaugai vertinimą dėl „<...> asmens vaizdo ir (ar) garso duomenų tvarkymas darbo vietoje <...>“ (Valstybinė duomenų apsaugos inspekcija, 2019). Tai reiškia, kad, esant poreikiui, Valstybinė duomenų apsaugos inspekcija gali patikrinti bendrovę, kaip yra laikymąsi šių nuostatų. Pažeidus privalomas teisės aktų nustatytas nuostatas, pagal BDAR 83 str. 5 d. 6 p. bendrovei gali būti skiriama bauda. Toliau darbo autorė plačiau analizuos darbuotojų stebėjimą vaizdo ir garso stebėjimą darbo vietoje problematiką bei sprendimo būdus.

2.3.1. Darbuotojų stebėjimas vaizdo priemonėmis

Darbuotojų darbo stebėjimas ir kontrolės klausimas šiandieniniame pasaulyje nėra naujas. Tačiau ši tema yra įgavusi visiškai naują prasmę, nes stebėjimo mastai ir elektroninės kontrolės galimybės yra labai išaugusios.

EŽTT byloje Amann prieš Šveicariją Nr. 27798/95 pasisakė, kad bet kokia informacija, susijusi su nustatytu asmeniu ar asmeniu, kurį būtų galima nustatyti, yra laikoma asmens duomenimis. Taigi vaizdo stebėjimo kameromis užfiksuota informacija, net ir netiesiogiai liečianti asmenį, kuris pagal ją galėtų būti identifikuotas, yra laikoma

asmens duomenimis. Taip pat Teismas yra pasakęs, kad net ir vieša informacija apie asmenį gali papulti į privataus gyvenimo sferą, jei ji yra sistemiškai kaupiama ir saugoma. Tam, kad nebūtų pažeista teisė į privatų gyvenimą, informacijos apie asmenį tvarkymui yra taikomi asmens duomenų apsaugos reikalavimai, paremti teisės į privatų gyvenimą principais (Žmogaus teisių stebėjimo institutas, 2005, p. 4).

Kitoje EŽTT byloje pasisakyta, kad asmens stebėjimas vaizdo priemonėmis viešoje vietoje nepažeidžia asmens teisės į privatų gyvenimą (Europos Žmogaus teisių teismo sprendime 2003 m. sausio 28 d. byloje Peck prieš Jungtinę Karalystę Nr. 44647/98).

Amman prieš Šveicariją byloje teismas išskyrė sąvokos „privatus gyvenimas“ ribas ir nurodė, jog šis apibrėžimas neturi būti aiškinamas siauriai. Kitos bylos pavyzdys aprėpia atvejus dėl apsauginių vaizdo kamerų, kurios yra aptinkamos duomenų subjektui patekus į prekybos centrus, parduotuves ir pan. Tai, kad tos vaizdo kameros stebi asmenis viešoje erdvėje, nepažeidžia asmens teisės į privatumą, tačiau ir nesuteikia duomenų valdytojui nesant teisiniam pagrindui disponuoti šiais duomenimis viešoje erdvėje be duomenų subjekto sutikimo.

Lietuvos teismų praktikoje teismas yra aiškinęs vaizdo kamerų paskirtį. Pavyzdžiui, vienoje byloje teismas nurodė, kad vaizdo kameros yra reikalingos dėl saugumo, tiek darbuotojų, tiek klientų, tiek darbo proceso bei turto saugumo tikslais (Vilniaus apygardos administracinio teismo 2020 m. gruodžio 3 d. sprendimas administracinėje byloje Nr. e12-4192-811/2020). Kitoje byloje teismas pabrėžia, kad vaizdo stebėjimas darbo vietoje gali būti vykdomas, kai dėl darbo specifikos būtina užtikrinti asmenų, turto ar visuomenės saugumą ir kitais atvejais, kai kiti būdai ar priemonės yra nepakankamos ir (arba) netinkamos, siekiant išvardytų tikslų. Teismas išdėstė poziciją, kad teisės į privatų gyvenimą pažeidimas gali būti suprantamas kaip privataus asmens filmavimas jo privačioje valdoje be jo sutikimo, vaizdo įrašo, kuriame užfiksuotas privatus asmuo, platinimas ar pavišinimas be jo sutikimo ir pan. Nagrinėjamos bylos atveju filmavimas buvo atliekamas atsakovui priklausančiose parduotuvės patalpose – prekybos salėje, t. y. viešoje vietoje, buvo filmuojami asmenys, susiję darbo santykiais su atsakovu ir materialiai atsakingi už atliekamą darbą. Toks filmavimas neturi būti laikomas privataus asmens teisių pažeidimu, todėl vaizdo įrašė esanti informacija turi būti pripažinta tinkamu įrodymu, nagrinėjant darbo pareigų pažeidimą (Klaipėdos apylinkės teismo Klaipėdos miesto rūmų 2013 m. birželio 21 d. nutarimas Nr. A2.11.-2002-512/2013).

Kitas atvejis, ar tikrai visuomet darbuotojas žino ir supranta, kad darbdavys jį stebi darbo vietoje prieš tai neinformavęs. Byloje teisėjų kolegija rėmėsi BDAR preambulės 47 punktu ir vertino, ar egzistuoja teisėtas interesas, kuriuo grindžiamas duomenų tvarkymas.

Paminima, kad visuomet turi būti atsižvelgiama, ar duomenų subjektas gali pagrįstai tikėtis, kad jis bus stebimas. Pripažįstama, kad darbuotojas dažniausiai nesitiki, kad darbdavys jį stebės darbo vietoje (Vilniaus apygardos administracinio teismo 2020 m. gruodžio 3 d. sprendimas administracinėje byloje Nr. eI2-4192-811/2020). Didžiausios problemos kyla tuomet, kai darbdavys pradeda tikrinti ir stebėti, kiek darbuotojas laiko užtrunka kalbant telefonu su artimiausiais ar draugais, kiek laiko darbuotojas geria kavą ir bendrauja su kolegomis, kiek kartų per darbo dieną darbuotojas išeina į lauką parūkyti, kiek laiko praleidžia rūkydamas, kiek kartų per dieną eina į tualetą ir pan. Kita vertus, tokie nuoseklūs ir konkretūs stebėjimo atvejai, kurie visiškai nėra suderinamas su darbdavio teisėtų interesu, pažeistų darbuotojo teisę į privatumą. Gali pasitaikyti atveju, kai patys darbuotojai piktnaudžiauja fiduciariniais santykiais su darbdaviu, tačiau net ir tuo atveju darbdavys turėtų imtis proporcingų priemonių nustatant pažeidimą.

Bet koku atveju apie vaizdo stebėjimą konkrečioje erdvėje, pavyzdžiui, darbo vietoje, koridoriuje, sandėlyje ir pan. būtina informuoti darbuotoją pagal BDAR 13 str. Autorė pateikia darbdaviui du informacinius būdus, kurie įspėja darbuotojus apie vaizdo stebėjimą konkrečioje erdvėje ar patalpoje.

Pirmas būdas, tai darbuotojui prieš įeinant į patalpą, kurioje yra vaizdo kamera (-os), matomoje vietoje turėtų būti informacinis pranešimas ir paveikslėlis su vaizdo kamera. Tam, kad informacinį pranešimą neapkrauti tekstu, rekomenduojama pateikti internetinę nuorodą į privatumo politiką. Pavyzdžiui, pranešime gali būti nurodyta, kad „Asmenų ir turto apsaugos tikslais yra vykdomas vaizdo stebėjimas“. Po šiuo tekstu, rekomenduojama pateikti internetinę nuorodą, leidžiančią konkrečiau susipažinti su vaizdo stebėjimo tikslais, apimtimi bei duomenų saugojimo terminais.

Antras būdas – pasirašytinai informuoti darbuotoją apie vaizdo stebėjimą darbo vietoje. Rašytiniame pranešime privaloma nurodyti tikslą. Pavyzdžiui, informuoti darbuotoją, kad siekiant užtikrinti darbuotojų bei trečiųjų asmenų turto saugumą, užkirsti kelią daromoms nusikalstamoms veikloms bei palengvinti nelaimingų atsitikimų darbe tyrimus darbo vietoje yra įdiegiamos vaizdo kameros. Kaip bebūtų, gali pasitaikyti situacijų, kai darbuotojas nesutinka dėl vaizdo stebėjimo darbo vietoje. Tokiu atveju, darbdavys privalo gauti iš darbuotojo paaiškinimą, kuriame turi būti išdėstyti nesutikimo motyvai. Stebėjimas vaizdo kameromis yra teisėtas, jeigu jis būtinas siekiant su duomenų valdytojo arba trečiosios šalies teisėtais interesais susijusio tikslo, išskyrus atvejus, kai už tokius interesus yra viršesni duomenų subjekto interesai arba pagrindinės teisės ir laisvės (Europos duomenų apsaugos valdyba, 2020, p. 9). Pavyzdžiui, darbdavys įrengia vaizdo

kamera šalia tualetu. Šiuo atveju, duomenų subjekto interesas bus viršesnis už duomenų valdytojo interesą, todėl darbdavys privalės nutraukti vaizdo stebėjimą šioje erdvėje.

Darbdaviui siūloma nurodyti, kokiose konkrečiai vietose darbuotojas gali aptikti vaizdo kameras. Pavyzdžiui, sandėlio patalpose, administracinėse patalpose, biuro patalpose, prie įėjimų, automobilių stovėjimo aikštelėse ir pan.

Taip pat, šiame pranešime darbdaviui rekomenduojama nurodyti vaizdo saugojimo trukmę. Pavyzdžiui, įrašytas vaizdo stebėjimas saugomas 14 kalendorinių dienų, vėliau vaizdo įrašas ištrinamas automatiškai. Darbdavys pranešime gali nusimatyti atvejus, kai vaizdo įrašas bus saugomas ilgiau dėl svarbių priežasčių. Pavyzdžiui, ikiteisminio tyrimo metu, nelaimingo atsitikimo metu, draudiminio įvykio administravimo tikslu ir pan.

Paminėtina, kad darbdavys gali ir raštu turi informuoti atskirai kiekvieną darbuotoją pateikdamas informaciją, kas gali peržiūrėti vaizdo įrašus. Pavyzdžiui, vadovas, teisės skyriaus / departamento darbuotojas / vadovas, asmens duomenų apsaugos pareigūnas, personalo departamento vadovas, tačiau tik tiek kiek reikalinga šių darbuotojų funkcijoms vykdyti.

Vadinasi, iš bylų analizės darytina išvada, kad vaizdo stebėjimas turėtų būti naudojamas kaip kraštutinė priemonė, siekiant apsaugoti paties darbdavio turtą, siekiant užtikrinti darbų saugą ir pan. Tai reiškia, kai darbdavio interesas turi būti viršesnis nei darbuotojo tam, kad toks stebėjimas būtų teisėtas. Dėl stebėjimo vaizdo kameromis darbuotojo sutikimo nereikia. Svarbiausia pateikti informacinį pranešimą bei supažindinti darbuotoją su vaizdo stebėjimu darbo metu. Darbo autorė rekomenduojama darbdaviui informuoti darbuotoją apie vaizdo stebėjimą pranešimu arba informaciniais ženklais prieš įeinant į patalpą.

2.3.2. Darbuotojų stebėjimas garso priemonėmis

Dažnai garso priemonės darbdaviui pasitarnauja tokiais atvejais, kai pagal darbuotojo darbo specifiką reikalaujama įrašinėti pokalbius tarp darbuotojo ir kliento. Tokios priemonės leidžia užtikrinti darbdaviui efektyviau gerinti, vertinti ir analizuoti darbuotojo kalbėseną, bendravimo manieras. Tačiau pasitaiko atvejų, kai tokiomis priemonėmis darbdavys peržengia ribas ir pažeidžia darbuotojo teisės į privatumą. Šioje dalyje darbo autorė toliau nagrinės telefoninių pokalbių įrašėjimo apimtį ir problematiką.

Paminėtina, kad net ir darbdaviui turint teisėtą interesą bei laikantis asmens duomenų apsaugos principų gali imtis darbuotojo kontrolės funkcijų. Tęsiant analizę svarbu išsiaiškinti, ar darbuotojas apskritai yra faktinis paslaugos naudotojas.

Šis atsakymas pateikiamas Lietuvos Respublikos elektroninių ryšių įstatymo 3 str. 25 punkte, kuriame nurodoma, kad faktinis elektroninių ryšių paslaugų naudotojas – fizinis asmuo, asmeniniams ar verslo tikslams naudojantis viešąsias elektroninių ryšių paslaugas. Šis asmuo nebūtinai turi būti šių paslaugų abonentas. To paties įstatymo 61 str. 4 d. pateikia, kad saugoti informaciją arba suteikti galimybę naudotis jau saugoma informacija abonto ar faktinio elektroninių ryšių paslaugų naudotojo galiniame įrenginyje leidžiama tik su sąlyga, kad atitinkamam abonentui ar faktiniam elektroninių ryšių paslaugų naudotojui vadovaujantis Asmens duomenų teisinės apsaugos įstatymu suteikus aiškią ir išsamią informaciją, įskaitant informaciją apie tvarkymo tikslus, jis davė sutikimą. Šios nuostatos nedraudžia techninio saugojimo ar naudojimosi duomenimis, kurio vienintelis tikslas yra perduoti informaciją elektroninių ryšių tinklu, taip pat būtiniais atvejais teikiant informacines visuomenės paslaugas, kurias užsako abonentas ar faktinis elektroninių ryšių paslaugų naudotojas (Lietuvos Respublikos elektroninių ryšių įstatymas, 2004). Minint šį įstatymą turima galvoje atvejį, kai darbuotojas naudojasi darbo priemonėmis, t. y. telefonu, kuris yra prijungtas prie viešojo ryšio tinklo. Dėl šios priežasties darbuotoją galima laikyti faktiniu elektroninių ryšių paslaugų naudotoju ir neatsiejamai jam garantuojama teisė į ryšio slapumą.

Analizuojant teisminę praktiką šios temos kontekste, pažymima, kad EŽTT nurodė, kad „privatus gyvenimas“ ir „susirašinėjimas“ apima taip pat ir telefoninius pokalbius darbo vietoje (Europos Žmogaus teisių teismo byla Halford v. The United Kingdom, App. 20605/92, Judgment of 25 June, 1997. EHRR 523). Taip pat nustatyta, kad telefono skambučiams iš įmonės patalpų taikoma privataus gyvenimo ir susirašinėjimo sąvokos apibrėžtis (Europos Žmogaus teisių teismo byla 2007 m. liepos 3 d. Copland prieš Jungtinę Karalystę Nr. C-70/10). Darytina išvada, kad pokalbiai telefonu, susirašinėjimas trumposiomis žinutėmis patenka į komunikacijos slaptumo bei darbuotojo privatumo apsaugos sritį. Darbdavys, norėdamas teisėtai stebėti, pasiklausyti ar kontroliuoti darbuotojo pokalbius, turi laikytis tam tikrų reikalavimų. Europos Žmogaus Teisių Teismas precedentiniuose sprendimuose: Halford prieš Jungtinę Karalystę ir Copland prieš Jungtinę Karalystę suformulavo poziciją dėl komunikacijos darbo vietoje stebėsenos (Tamašauskaitė-Janickė, 2016, p. 106).

Toliau Lietuvos teismų praktiką, teisėjų kolegija vienoje iš bylų nurodė, kad teismas pagrįstai sprendė, kad aplinkybė, jog asmuo galėjo suprasti, kad pokalbis įrašinėjamas, tačiau prieštaravimo neišreiškė, negali būti vertinama kaip duotas sutikimas, jei būtų remiamasi ADTAĮ 2 str. 12 d. Taip pat žvelgiant į šios bylos pavyzdį, paminėtina, kad darbuotoja nebuvo įspėta dėl garso įrašo darymo, nežinojo pokalbio įrašymo tikslo

(Lietuvos vyriausiojo administracinio teismo 2018 m. sausio 24 d. nutartis administracinėje byloje Nr.eA-3-822/2018).

Iš bylų analizės darytina išvada, kad darbdaviui privaloma informuoti darbuotoją dėl pokalbių įrašinėjimo pagal BDAR 13 str. tam, kad būtų sumažintos problemos dėl neinformavimo, darbdavys raštu privalo supažindinti darbuotoją dėl garso įrašymo darbo vietoje. Toliau darbo autorė pateiks preliminarų pranešimo turinį, kuriame rekomenduojama apibrėžti esminius pranešimo elementus.

Pirmiausia, pranešime svarbu apibrėžti asmens duomenų tvarkymo tikslą. Pavyzdžiui, gerinti komunikaciją ir bendravimą tarp klientų ir darbuotojų, stebėti darbuotojų klaidas teikiant konsultacijas klientams ir pan.

Pranešime svarbu apibrėžti tvarkomų duomenų ir duomenų subjektų kategorijas. Pavyzdžiui, garso įrašai įrašinėjami tarp klientų ir darbuotojų. Paminėtina, kad tais atvejais, kai telefoninius pokalbius įrašoma vadovaujantis teisėtų interesu, darbuotojo sutikimo nereikia. Ne išimtis ir kliento statusas. Kadangi prieš pradedant pokalbį su konsultantu, klientui nurodoma „Siekiant užtikrinti pokalbio ir aptarnavimo kokybę, pokalbis gali būti įrašytas. Jeigu sutinkate, prašome palaukti“. Tai reiškia, jog pats klientas konkludentiniais veiksmais sutinka su pokalbio įrašu.

Taip pat pranešime privalo būti apibrėžtas ir asmens duomenų gavėjas. Pavyzdžiui, kolegos, įmonės, įstaigos, organizacijos komandų / skyriaus vadovai ir pan.

Paminėtinas ir saugojimo termino būtinumas. Pavyzdžiui, pranešime nurodoma, jog darbdavys duomenis saugos 6 mėnesius, nebent duomenų saugojimas būtų reikalingas ilgesniam laikotarpiui dėl teisinių tyrimų ar ginčo atvejų.

Šį pranešimą galima pateikti darbuotojams nuorodos principu į darbdavio privatumą politiką arba prieš pasirašant darbo sutartį supažindinti su šiuo pranešimu. Pavyzdžiui, jeigu darbuotojas pagal darbo specifiką įsidarbinta kliento aptarnavimo specialistu, tai natūralu, kad pokalbiai su klientais bus įrašomi ir analizuojami. Dažnai klientų aptarnavimo specialistų konsultacijos yra vertinamos pačių klientų, bendrovės vadovų ir pan. Tokie vertinimai skatinami piniginėmis premijomis. Dėl šios priežastis, vienintelis būdas patikrinti darbuotojo darbo kokybę – pokalbių įrašų perklausa.

Visgi darbuotojai, kurių darbo funkcijos nėra susijusios su kliento aptarnavimo sritimi, pokalbių įrašinėjimas nėra leidžiamas, kadangi pokalbio metu gali būti pažeista darbuotojo teisė į privatumą. Pavyzdžiui, prekybos centre įrašinėti salės darbuotojų, kasininkų pokalbių negalima, nes darbuotojai komunikuoja ne tik darbo santykių ribose, bet ir asmeninio gyvenimo srityje. Jeigu darbdavys siektų įrašinėti pokalbius šių darbuotojų

kontekste, tai turi būti pagrįsta teisės aktais ar kompetentingų institucijų pavedimu, kai siekiama išsiaiškinti nusikaltimo aplinkybes.

Darytina išvada, kad egzistuoja darbdavio pareiga informuoti darbuotoją apie telefoninių pokalbių įrašinėjimo tvarkymą ir pagrindą. Autorė pastebi, kad Lietuvoje nėra pakankamai daug teismų praktikos šiuo klausimu. Vadinasi, telefoninių pokalbių įrašinėjimas būtų svarbus ir aktualus tik tuo atveju, jeigu darbuotojas dirba konsultacijų skyriuje, kur tiesiogiai yra bendraujama su klientais ir teikiamos konsultacijos.

2.4. Darbuotojų stebėjimas ir sekimas kitomis priemonėmis

Lietuvos Respublikos darbo kodekso 24 str. 4 d. nurodoma, kad darbdaviui priklausančias darbo priemones darbuotojas turi naudoti darbo reikmėms, išskyrus atvejus, kai darbo sutarties šalys susitaria dėl darbdaviui priklausančių priemonių naudojimo kitais tikslais sąlygų ir tvarkos. Ši specialioji nuostata skirta aptarti darbdavio darbo priemonių (pavyzdžiui, kompiuterio, išmaniojo telefono, planšetės, automobilio, fotokameros, taip pat programinės įrangos ar technologijų), kurias darbuotojas turi darbo reikmėms, naudojimą. Darbuotojo reikmėms jos gali būti naudojamos tik darbdavio ar darbuotojo susitarimu. Kai kuriam materialiniam turui (automobiliui) naudoti gali būti sudaromi atskiri susitarimai, bet tinkama ir labiausiai paplitusi praktika yra tokią tvarką patvirtinti darbdavio vietos teisės aktais. Juose aptariami turto naudojimo ne darbo reikmėms atvejai, bet darbdavio sutikimas naudoti asmeninėms reikmėms jo turtą gali būti duodamas konkludentiniais veiksmais (Davulis, 2018, p. 98).

Vadinasi tam, kad būtų galima tiksliau išsiaiškinti darbuotojo stebėjimo teisėtumą kitų priemonių pagalba, darbo autorė plačiau analizuos GPS ir elektroninių ryšių problematiką darbo santykiuose.

2.4.1. Darbuotojų automobilio sekimas GPS priemonėmis

ES 29 str. duomenų apsaugos darbo grupės nuomonėje nurodoma, kad darbdavys gali būti įpareigotas transporto priemonėse įrengti sekimo technologiją, kad galėtų įrodyti, jog laikosi kitų teisinių įpareigojimų. Darbdavio teisėti interesai gali turėti galimybę bet kuriuo metu nustatyti transporto priemonių buvimo vietą. Net jeigu darbdaviai turi teisėtų interesų pasiekti šiuos tikslus, pirmiausia turėtų būti įvertinama, ar duomenų tvarkymas šiais tikslais yra reikalingas ir ar faktinis jų įgyvendinimas atitinka proporcingumo ir subsidiarumo principus. Kai darbinę transporto priemonę leidžiama naudoti asmeniniais tikslais, svarbiausia priemonė, kurios darbdavys gali imtis šių principų laikymuisi užtikrinti, yra pasiūlyti galimybę pasirinkti: darbuotojui iš esmės turėtų būti suteikta galimybė laikinai

išjungti sekimą, kai šis išjungimas pateisinamas ypatingomis aplinkybėmis, pavyzdžiui, lankantis pas gydytoją. Taip darbuotojas gali savo iniciatyva tam tikrus buvimo vietos duomenis apsaugoti kaip privačius. Taip pat darbdavys turi užtikrinti, kad renkami duomenys nebūtų naudojami siekiant toliau neteisėtai juos tvarkyti, pavyzdžiui, sekti ir vertinti darbuotojus. Be to, darbdavys turi aiškiai informuoti darbuotojus, kad įmonės transporto priemonėje, kurią jie vairuoja, yra sumontuotas sekimo įrenginys ir kad jų judėjimas įrašinėjamas tol, kol jie naudoja tą transporto priemonę (taip pat, kad gali būti įrašinėjami ir vairuotojo veiksmai). Pageidautina, kad tokia informacija būtų aiškiai nurodyta kiekviename automobilyje, vairuotojo regėjimo lauke (ES 29 straipsnio duomenų apsaugos..., 2017, p. 22).

Visgi GPS sekimas darbdavio atveju padeda apsaugoti įmonės turtą bei užtikrinti, jog darbuotojai naudotų šias priemones pagal paskirtį. Pavyzdžiui, vienoje iš bylų GPS priemonės pagalba darbdavys išsiaiškino, jog darbuotojas pasinaudojo įmonės automobiliu ir darbo metu atliko veiksmus, kurie nesusiję su darbine veikla (Lietuvos apeliacinio teismo 2011 m. rugsėjo 5 d. nutartis civilinėje byloje Nr. 2A–1502/2011). Kitoje byloje taip pat GPS pagalba darbdavys nustatė, kad darbuotoja ne visą darbo laiką skyrė darbo sutartyje numatytoms pareigoms atlikti (Šiaulių apygardos teismo 2011 m. lapkričio 2 d. nutartis civilinėje byloje Nr. 2A–666-368/2011). Pavyzdžiui, darbuotojas darbo metu važiuodamas iš vieno miesto į kitą, pasiima pakeleivį. Darbuotojas nėra pervežimo paslaugas teikiantis darbuotojas. Individas nuvežą pakeleivį į atitinkamą vietą ir už tai gauną piniginį atlygį. Tai reiškia, jog darbuotojas naudodamasis darbdavio automobiliu, atlieka veiksmus, kurie nėra suderinami su darbdavio tikslais. Tokie darbuotojo veiksmai, pažeidžia darbdavio interesus.

Šios temos kontekste keliamas kitas klausimas, o kokia GPS paskirtis ir kaip plačiai ši priemonė gali stebėti ir kėsinti į darbuotojo privatų gyvenimą? Šį klausimą gvildeno LAT ir išaiškino, kad tokios priemonės kaip GPS pagal pobūdį skiriasi nuo kitų vaizdo ir garso stebėjimo priemonių, kurios atskleidžia daugiau informacijos apie asmens elgesį, mintis ar jausmus ir dėl to gali labiau apriboti asmens teisę į privataus gyvenimo gerbimą. Vis dėlto sistemingas informacijos apie asmenį rinkimas naudojant GPS įrangą gali apriboti asmens teisę į privatumą (Lietuvos Aukščiausiojo teismo 2013 m. balandžio 23 d. nutartis baudžiamojoje byloje Nr. 2K–198/2013). Pavyzdžiui, kitoje byloje LAT citavo EŽTT praktiką byloje U. prieš Vokietiją. Šiame sprendime teismas pažymėjo, kad asmens stebėjimas panaudojant GPS priemones dėl savo pobūdžio turi būti skiriamas nuo kitų vaizdo ir garso stebėjimo metodų, kurie paprastai gali labiau apriboti asmens teisę į privataus gyvenimo gerbimą, nes atskleidžia daugiau informacijos apie jo elgesį, pažiūras

ar jausmus, tačiau, atsižvelgdamas į konkrečias bylos aplinkybes, nurodė, kad, nepaisant to, jog GPS stebėjimas taikytas pareiškėjo automobiliui, juo aiškiai siekta gauti informacijos ir apie pareiškėjo judėjimą bei nusprendė, kad dėl šio stebėjimo ir jį taikant gautų duomenų tvarkymo bei panaudojimo pareiškėjo teisė į privatų gyvenimą buvo apribota (Lietuvos Aukščiausiojo teismo 2014 m. gegužės 6 d. nutartis baudžiamojoje byloje Nr. 2k-213/2014).

Ne išimtis šiuo atveju yra ir darbuotojo informavimo apie tokių duomenų tvarkymą. Pavyzdžiui, vienoje iš bylų dėl GPS priemonių naudojimo ir sekimo teismas nurodė, kad duomenų subjektai turėjo būti supažindinti su duomenų subjektų teisėmis bei teise nesutikti, kad jų asmens duomenys būtų tvarkomi (Lietuvos vyriausiojo administracinio teismo 2016 m. gruodžio 7 d. nutartis administracinėje byloje Nr. eA-2333-525/2016).

Iš teismų praktikos darytina išvada, kad GPS priemonės labiau palengvina darbdavio situaciją, kadangi darbuotojai naudodamiesi padėtimi dažniausiai piktnaudžiauja savo teisėmis. Juk darbdavys suteikia darbo priemones darbuotojams. GPS įrangos diegimas transporto priemonėje reikalinga darbdavio siekiant apsaugoti darbdavio turtą nuo vagysčių. Tai reiškia, kad darbdavių interesas stebėti darbuotojus GPS priemonių pagalba yra suprantama. Naudojant GPS įrangą visgi darbdavys privalo informuoti apie GPS įrenginio būvimą bei gauti darbuotojo sutikimą dėl tokių priemonių naudojimo. Žinoma, gali pasitaikyti situacijų, kai darbuotojas nesutinka su šios įrangos įdiegimu transporto priemonėje. Net ir tokiu atveju darbuotojui nesutinkant, darbdavys įvertinęs būtinumą, gali GPS pagalbą stebėti transporto priemonių maršrutus, pavyzdžiui, darbuotojas turi iš vieno miesto į kitą, pervežti įmonės steigimo dokumentus. Toks informacijos praradimas vagystės atveju, būtų įmonės konfidencialios informacijos atskleidimo rizikos rate.

Valstybinės duomenų apsaugos inspekciją 2019 m. kovo 15 d. yra išleidusi direktoriaus įsakymą NR.1T-35 (1.12.E), kuriame 10 punkte nurodoma, kad darbdavys privalo atlikti poveikio duomenų apsaugai vertinimą dėl „<...> asmens duomenų, susijusių su darbuotojų, komunikacijos, elgesio, vietos ar judėjimo stebėsena, tvarkymas <...>“ (Valstybinės duomenų apsaugos inspekcijos direktoriaus įsakymas NR.1T-35 (1.12.E), 2019, 10 punktas). Tai reiškia, kad šie duomenys turi būti saugomi, o jų prireikus pateikti Valstybinei duomenų apsaugos inspekcijai pareikalavus.

Vadinasi, siekiant išvengiant piktnaudžiavimo darbdaviui rekomenduojama, nusistatyti transporto priemonės vidinio naudojimo taisykles. Pavyzdžiui, pasibaigus darbo valandoms automobilio rakteliai turėtų būti grąžinami darbdaviui ir pan. Taip pat darbdaviui rekomenduojama apsibrėžti duomenų apsaugos politikoje konkrečius duomenų

subjektus, kurie yra padidintos rizikos apsuptyje dėl vagysčių. Pavyzdžiui, tolimųjų reisų vairuotojai, kurie gabena alkoholį, tabaką, automobilius, dujas ir pan.

2.4.2. Darbuotojo elektroninių ryšių stebėjimas

Darbuotojų susirašinėjimo elektroniniu paštu ir kitų elektroninių ryšių pagalba, tokių kaip naršymas internete, stebėjimas yra opus dalykas, nes kyla klausimų, kokia ir kokia turėtų būti darbuotojų teisė į privatumą darbdavio atžvilgiu. (Eklund, 2019, p. 121)

Dėl susirašinėjimo pasisakyta Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos 8 str., jog asmenims garantuoja teisę į privataus ir šeimos gyvenimo gerbimą, būsto neliečiamybę ir susirašinėjimo slaptumą (Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija, 1995). Vienoje iš EŽTT byloje teismas išaiškino, jog bet kokiuose darbo santykiuose turi būti erdvės privatumui (Europos Žmogaus teisių teismo 1992 m. gruodžio 16 d. sprendimas byloje Niemietz prieš Vokietiją Nr. 13710/88).

Kitoje EŽTT byloje darbdavys buvo informavęs darbuotoją, jog šis gali naudoti darbo priemonės darbo vietoje tik darbo tikslams. Pirminiame sprendime teismas nustatė, kad darbdavys tikrinęs darbuotojo „Yahoo Messenger“ paskyros susirašinėjimą, nepažeidė teisės į privatumą. Toliau tęsiantis šios bylos aiškinimui Didžioji kolegija pakeitė nuomonę ir situacijos kontekste įžvelgė pažeidimų. Nors šioje byloje ir buvo užtektinai informacijos, kad darbdavys buvo informavęs darbuotoją, jog darbo priemonės būtina naudoti tik darbo tikslais, tačiau darbdavys nebuvo tinkamai informavęs darbuotoją apie susirašinėjimo stebėjimą. Visgi šioje byloje tam tikri darbuotojo interesai buvo pažeisti (Europos Žmogaus Teisių Teismo 2016 m. sausio 12 d. sprendimas byloje Bărbulescu v. Romania Nr. 61496/08). Pavyzdžiui, didžiausia grėsmė darbdaviams, turintiems komercines paslaptis, kyla ne iš išorės (pvz., kibernetinės atakos ar kompiuterio kenkėjiškos programos), bet iš darbuotojų (Eklund, 2019, p. 121). Pavyzdžiui, dėl žinių ir kompetencijos stokos, darbuotojas gali nesugebėti identifikuoti internetinių sukčių, kurie informacinių technologijų pagalba gali sukurti darbuotojui iš pirmo žvilgsnio saugią, elektroniniame laiške sukurtą nuorodą. Darbuotojas elektroniniame laiške paspaudęs sukčių pateiktą nuorodą, tokiu būdu sukčiams gali suteikti prieigą prie ne tik prie asmeninės, bet ir prie darbdavio konfidencialios informacijos.

EŽTT praktikoje pabrėžiama, kad darbdavio atliekamas darbuotojo susirašinėjimas ir kitokios komunikacijos sekimas yra suderintas su darbuotojo teise į privatumą, jeigu laikomasi proporcingumo reikalavimo ir užtikrinamos procedūrinės garantijos, apsaugančios nuo darbdavio savivalės. Šiuo požiūriu svarbu ar darbuotojas yra informuojamas apie sekimo galimybę, sekimo apimtį, ar darbdavys nurodo konkrečias

sekimo pateisinančias teisėtas priežastis, ar galima apriboti mažiau darbuotojo privatumo ribojančiomis priemonėmis, kokių padarinių darbuotojas gali patirti ir kokių garantijų jam suteikiama dėl vykdymo sekimo (Zaleckis, 2019, p. 259). Pavyzdžiui, 29 str. darbo grupė nurodo, kad praktiškai gali būti laikoma darbuotojų elektroninio pašto stebėsena siekiant gauti patvirtinimą ar įrodymus apie tam tikrus veiksmus. Pavyzdžiui, nusikalstamą veiklą, kad būtų galima apginti savo darbdavio interesus. Taip pat gali būti laikoma būtina stebėti darbuotojų el. pašto susirašinėjimą siekiant nustatyti virusus ar bet kokią darbdavio vykdomą veiklą, kad būtų garantuotas jo sistemų saugumas (Eklund, 2019, p. 129).

Direktyva dėl asmens duomenų apsaugos reikalauja, kad bet kokia darbuotojo stebėjimo forma būtų būtina konkrečiam, aiškiai išreikštam ir racionaliam tikslui pasiekti. Darbdaviai visais atvejais prieš imdamiesi darbuotojų elektroninio pašto, turėtų įsitikinti, kad pageidaujamam tikslui pasiekti nėra galimybės panaudoti kitas priemones, mažiau besikišančias į darbuotojų privatų gyvenimą. Tokių priemonių darbdaviai dažniausiai imasi norėdami apsaugoti savo verslo konfidencialią informaciją arba įrodyti, kad darbuotojas darbo metu atlieka neleistinus veiksmus. Atkreiptinas dėmesys į tai, kad elektroninio pašto stebėjimas turėtų apsiriboti duomenų srauto peržiūra ir ryšio laiko bei datos fiksavimu, vengiant susirašinėjime esančios informacijos fiksavimo ir analizavimo. Stebint darbuotojų elektroninį paštą, naršymą internete ar kitaip atliekant darbuotojų elektroninės darbo vietos stebėjimą, darbdavys neturėtų pamiršti ir kitų bendrųjų principų, tokių kaip: tikslingumas (duomenys surinkti stebėjimo metu yra surinkti konkrečiam tikslui ir negali būti panaudoti jokiame kitame tikslui), skaidrumas (draudžiamas slaptas darbuotojų el. pašto stebėjimas), duomenų tikslumas ir saugojimo terminas (reikalaujama, kad teisėtai surinkti ir saugomi duomenys būtų tikslūs ir saugomi ne ilgiau negu protingą saugojimo terminą) (Maliauskaitė, Šilkūnaitė, 2015).

Lietuvos Respublikos teisės aktų kontekste susirašinėjimo išaiškinimo apimtį analizavo Lietuvos Respublikos Konstitucijos nutarime, kuriame išdėstyta, kad Konstitucijos 22 str. 2 d. įtvirtinta asmens teisė į susirašinėjimo neliečiamumą nėra absoliuti; teisę į susirašinėjimo neliečiamumą galima apriboti tik įstatymu, kuriame turi būti nurodyti tokio ribojimo pagrindai ir tvarka; ribojimas turi būti toks, kad tarp pasirinktų priemonių ir siekiamo teisėto ir visuotinai svarbaus tikslo būtų protingas santykis (Lietuvos Respublikos Konstitucinio teismo nutarimas 2015 m. vasario 26 d. Nr. KT8-N4/2015).

Visgi ir Lietuvos Respublikos darbo kodekse 27 str. 2 d. užsiminta apie tai, kad darbdaviui, įgyvendinant nuosavybės ar valdymo teises į darbo vietoje naudojamas informacines ir komunikacines technologijas, negali būti pažeidžiamas darbuotojų asmeninio susižinojimo slaptumas.

Tam, kad lengviau suprasti su kokiomis situacijomis yra susiduriama Lietuvoje šia tema buvo paanalizuota teismų praktika. Pavyzdžiui, vienoje iš bylų 2010 m. teisėjų kolegija manė, kad darbdavys turi teisę žinoti, kokiam tikslui yra naudojamos darbo priemonės ir kuo užsiima darbuotojas darbo metu. Teisėjų kolegija konstatavo, kad darbdavys teisėtai tikrina darbuotojo pokalbius „Skype“ programoje. Teismas neįžvelgė teisės į privataus gyvenimo neliečiamumą pažeidimo (Vilniaus apygardos teismo Civilinių bylų skyriaus 2010 m. gegužės 6 d. nutartis civilinėje byloje Nr. 3K-3-177/2010).

Po daugiau nei dviejų metų Lietuvos vyriausiasis administracinis teismas kitoje byloje nustatė, kad darbdavys, suteikęs darbuotojai kompiuterį ir mobiliojo ryšio telefoną darbo funkcijoms atlikti, tačiau nenustatęs darbo priemonių naudojimosi tvarkos apribojimų (lokalinių teisės aktų), iš jų ir dėl draudimo „Skype“ programa naudotis asmeniniais tikslais, neįspėjęs dėl to, kad susirašinėjimas ar lankymasis internetiniuose tinklapiuose bus tikrinami, slapta nurašęs kompiuterio atmintyje esančius programas „Skype“ ir lankytų internetinių svetainių adresų duomenis, pažeidė ieškovės privatumą, juolab, kad ieškovei buvo leista kompiuteriu naudotis ir asmeniniais tikslais po darbo (Vilniaus apygardos teismo Civilinių bylų skyriaus 2012 m. gruodžio 28 d. nutartis civilinėje byloje Nr. 2A-3217-781/2012).

Dar vienoje byloje šios temos kontekste, darbuotojui buvo skirta drausminė nuobauda už tai, kad iš darbui suteikto kompiuterio ir jam priskirto elektroninio pašto adreso elektroniniais laiškais bendravo su tiesiogiai konkuruojančia bendrove. Susirašinėjimai darbuotojo kompiuteryje parodė, kad darbuotojas konkuruojančios bendrovės darbuotojams atskleidė komercines paslaptis apie bendrovės klientus, vykdomų pervežimų maršrutus, krovinių siuntėjus ir gavėjus, ekspedijavimo kainas (Kauno apygardos teismo 2011 m. lapkričio 24 d. nutartis civilinėje byloje Nr. 2A-2130-555/2011).

Darytina išvada, kad darbuotojų elektroninių ryšių stebėjimas gali būti pateisinamas, tik tuomet, kai kyla pavojus darbdavio konfidencialios, ar net paties darbuotojo asmeninės informacijos atskleidimo galimybėms. Visgi, tikrinti darbuotojo elektroninio pašto gautus ir išsiųstus laiškus, internetinius tinklapius, kur darbuotojas lankėsi darbo metu ir pan., galima tik turint objektyvių ir pateisinamų priežasčių.

3. Duomenų tvarkymas pasibaigus darbo santykiams

Šiandieniniame dinamiškame pasaulyje darbuotojų kaita yra natūralus procesas. Dėl šios priežasties, darbo santykių pabaigos etapas gali priklausyti tiek nuo darbuotojo valios, tiek nuo darbdavio valios, arba dėl kitų Darbo kodekse nurodytų priežasčių. Lietuvos Respublikos darbo kodekso 65 str. yra įtvirtintos taisyklės dėl darbo sutarties pasibaigimo įforminimo. Tačiau nepriklausomai nuo darbdavio ir darbuotojo pasibaigusios darbo sutarties priežasties, svarbu išsiaiškinti, buvusio darbuotojo duomenų saugojimo trukmės elementus bei kokias teises turi duomenų subjektas nutraukus darbo sutartį.

3.1. Buvusio darbuotojo duomenų saugojimo trukmė

Analizuojant šį klausimą, paminėtinas duomenų saugojimo trukmės ribojimo principas. Taikant duomenų saugojimo trukmės apribojimo principą reikalaujama, jog duomenys būtų laikomi tokia forma, kad duomenų subjektų tapatybę būtų galima nustatyti ne ilgiau, nei tai būtina, ir tik tais tikslais, kuriais asmens duomenys yra tvarkomi (BDAR 5 str. 1d. d p., ET duomenų apsaugos konvencija 5 str. 4 d. e p.) (Zaleckis, 2019, p. 126).

Paminėtina, kad darbo santykių pradžioje darbdavys renka duomenis, kurie yra reikalingi įdarbinimo ir darbo sutarties vykdymo tikslais. Po to darbo santykiams pasibaigus darbdavys konkrečią informaciją saugo savo vidinėse duomenų bazėse. Pavyzdžiui, informaciją apie kontaktinius duomenis (adresą, telefono numeris (darbo), darbo el. paštas, asmenimis telefono numeris ir pan.), su kvalifikacija susijusius duomenis (išsilavinimo įstaiga, išsilavinimo tipas ir pan.), darbo sutarties sąlygų duomenys (darbo vieta, informacija apie sutartį (terminuota / neterminuota), darbo užmokestis (bruto), priėmimo į darbą data ir pan.), darbo sutarties pasibaigimo duomenys (atleidimo iš darbo data, darbuotojo išėjimo iš darbo priežastys, atleidimo iš darbo pagrindas ir pan.), kiti duomenys (apdovanojimai, pasiekimai, darbuotojo pažymėjimo numeris, tabelio numeris, Sodros pažymėjimo numeris ir pan.) ir t. t.

ESTT išaiškino, kad duomenų valdytojas turi užtikrinti, kad asmens duomenys būtų „tvarkomi teisingai ir teisėtai“, „surinkti įvardintais, aiškiai apibrėžtais ir teisėtais tikslais, o po to [ne]tvarkomi su šiais tikslais [ne]suderintais būdais“, būtų „adekvatūs, susiję ir savo apimtimi neviršijantys tikslų, kuriems jie renkami ir (arba) vėliau tvarkomi“, būtų „tikslūs ir, jei būtina, nuolat atnaujinami“ ir, galiausiai, būtų saugomi „tokio pavidalo, kad duomenų subjektų tapatybes būtų galima nustatyti ne ilgiau, nei tai yra reikalinga tais tikslais, dėl kurių duomenys buvo surinkti arba po to tvarkomi“. Šiais atvejais duomenų valdytojas turi imtis visų reikalingų priemonių, kad duomenys, kurie neatitinka šioje nuostatoje nurodytų reikalavimų, būtų ištrinti arba ištaisyti (Europos Sąjungos Teisingumo Teismo 2014 m.

gegužės 13 d. sprendimas byloje Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González Nr. C131/12).

Kitoje ESTT byloje konstatuojama, kad valstybės narės garantuoja kiekvienam duomenų subjektui teisę reikalauti, kad duomenų valdytojas: tinkamai ištaisytų, ištrintų arba blokuotų duomenis, kurie tvarkomi nesilaikant šios direktyvos nuostatų, o ypač, kai tie duomenys yra neišsamūs ar netikslūs, o 6 str. 1 d. e punktas nurodo, kad Valstybės narės turi numatyti, kad asmens duomenys būti laikomi tokio pavidalo, kad duomenų subjektų tapatybės būtų galima nustatyti ne ilgiau, nei tai yra reikalinga tais tikslais, dėl kurių duomenys buvo surinkti arba paskui tvarkomi (Europos Sąjungos Teisingumo Teismo 2017 m. kovo 9 d. sprendimas byloje Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni Nr.C-398/15). Gali pasitaikyti situacijų, kai darbo santykių pradžioje darbo sutartys bus saugomos vienu teisiniu pagrindu, o darbo santykių pabaigoje darbo sutartys gali būti saugomos kitu teisiniu pagrindu. Pavyzdžiui, darbo santykių pabaigoje duomenų saugojimo tikslas privalomas pagal norminius teisės aktus. Tai reiškia, kad teisės aktai nustato ir įpareigoja darbdavį vadovautis minimaliais duomenų saugojimo terminais. Deja, BDAR nereguliuoja, kaip turėtų būti nustatytas ir apskaičiuotas saugojimo terminas, todėl atsakymo reikia ieškoti nacionaliniuose teisės aktuose.

Lietuvoje minimalūs saugojimo terminai pateikiami Lietuvos vyriausiojo archyvaro įsakyme Nr. V-100 dėl bendrųjų dokumentų saugojimo terminų rodyklės patvirtinimo (toliau – rodyklė). Rodyklėje nustatyti minimalūs saugojimo terminai taikomi ir nevalstybinių organizacijų, privačių juridinių asmenų veiklos dokumentams, kurių rengimą nustato teisės norminiai aktai. Pavyzdžiui, 7.3 punkte nurodoma, kad darbo sutarties ir jų priedai (susitarimai dėl papildomų darbo sutarties sąlygų ir kt.) saugomi mažiausiai 50 metų (pasibaigus sutarčiai). Taip pat šiame įsakyme nurodoma, kad sutikimai dėl asmens duomenų tvarkymo saugomi mažiausiai 1 metus (pasibaigus asmens duomenų, dėl kurių tvarkymo buvo duotas sutikimas, saugojimo laikotarpiui) ir pan. (Lietuvos Vyriausio archyvaro įsakymą dėl bendrųjų dokumentų saugojimo terminų rodyklės patvirtinimo, 2011).

Visgi, autorės nuomone toks darbo sutarčių saugojimo terminas yra kritikuotinas. Pirmiausia, pats BDAR preambulės 39 p. nustato, kad duomenys privalo būti tvarkomi ir saugomi turint teisėtą tikslą, tačiau ar 50 metų terminas yra tikrai proporcingas nustatytiems tikslams? Pavyzdžiui, darbuotojas įsidarbina įmonėje specialistu, tačiau po dviejų savičių nusprendžia, jog darbo funkcijos neatitinka jo lūkesčių. Galiausiai nutraukia darbo sutartį ir pereina dirbti į kitą įmonę. Iš to seka klausimas, kam gi darbdaviui reikia 50 metų saugoti tokio darbuotojo duomenis, jeigu asmuo net nepraeina bandomojo laikotarpio? Ar tikrai

įstatymų leidėjas nustatydamas tokį ilgą periodą nepažeidžia buvusio darbuotojo teisės į privatumą?

Toliau analizuojant rodyklėje nustatytus terminus darbo autorei kritikuotina, kad, pavyzdžiui, informaciją dėl priėmimo į pareigas, perkėlimo, pavadavimo, atleidimo iš pareigų, darbo užmokesčio, atostogų vaikui prižiūrėti, tėvystės atostogų dokumentai saugomi taip pat 50 metų. Autorė pakartotinai kritikuoja šio saugojimo termino periodą. Pavyzdžiui, kodėl darbdaviui yra reikalinga saugoti darbuotojo naujagimio gimimo liudijimą ar kitus dokumentus 50 metų? Kokią vertę šie dokumentai turės net po 20 metų? Kam darbdaviui reikia tokį ilgą terminą saugoti duomenis apie vaiką, kuris net nėra jų darbuotojas? Visgi, darbo autorės nuomone 50 metų terminas tokių dokumentų saugojimui pažeidžia kitų šeimos narių teisę į privatumą.

Dėl kasmetinių, nemokamų, mokymosi ir kitų atostogų, dėl komandiruočių, papildomų poilsio dienų, sutrumpinto darbo laiko dokumentai pagal rodyklės normatyvus saugomi net 10 metų. Autorės nuomone, tokių dokumentų saugojimas 10 metų yra perteklinis. Pavyzdžiui, kam darbdaviui yra reikalingi dokumentai apie papildomas poilsio dienas ir pan. tokį ilgą laiko tarpą? Autorės nuomone tokio pobūdžio dokumentų saugojimas paprasčiausiai apkrauna darbdavio saugojimo duomenų bazes iš tiesų neaktualia informacija. Kokią naudą ir svorį šie dokumentai suteiks darbdaviui 10 metų laikotarpyje?

Be to, drausminės atsakomybės dokumentacija (tarnybiniai pranešimai, reikalavimai pasiaiškinti, darbuotojų pasiaiškinimai, įspėjimai ir t. t.) saugomi 5 metus pagal Lietuvos vyriausiojo archyvaro įsakymą Nr. V-100 dėl bendrųjų dokumentų saugojimo terminų rodyklės patvirtinimo. Paminėtina, kad ne visų saugomų dokumentų terminai gali būti nurodyti Lietuvos vyriausiojo archyvaro įsakyme Nr. V-100. Visgi, Lietuvos Respublikos darbo kodekso 15 str. 2 d. pateikiamas bendrasis trijų metų ieškinio senaties terminas. Tai reiškia, kad darbdavys gali savarankiškai nusistatyti konkrečių dokumentų saugojimo terminus, kurie nenurodyti Lietuvos vyriausiojo archyvaro įsakyme Nr. V-100. Pavyzdžiui, darbuotojo įdirbio planai, registracija į kalbų kursus, kurie rengiami įmonės viduje ir pan. Vadinasi, kadangi tokio pobūdžio dokumentai nėra nurodyti Lietuvos vyriausiojo archyvaro įsakyme Nr. V-100, tai šių dokumentų saugojimo terminas bus trys metai pagal Darbo kodeksą.

Lyginant darbo sutarčių saugojimo terminą su kitos rūšies, pavyzdžiui, turto panaudos, prekių, darbų, paslaugų, nuomos sutarčių saugojimo terminais, pagal Lietuvos vyriausiojo archyvaro įsakymą Nr. V-100 dėl bendrųjų dokumentų saugojimo terminų rodyklės patvirtinimo, minėtos turto panaudos, prekių, darbų, paslaugų, nuomos sutartys

yra saugomos 10 metų. Remiantis 2020 metų civilinių bylų nagrinėjimo ataskaita (apeliacinės instancijos teismuose) pagal bylų kategorijas išvelgiama, kad iš viso apeliacinės instancijos teismuose gauta 150 647 bylų. Paminėtina, kad dėl darbo teisinių santykių gautos 890 bylų, o su prievolių teise susijusių gauta 49 132 bylų. Nemažą dalį civilinių bylų sudaro būtent ginčai dėl sutarčių, pavyzdžiui, pirkimo – pardavimo, įmonės, žemės, transporto nuomos ir pan. Tai reiškia, kad bylų tarp darbuotojų ir darbdavių apeliacinės instancijos teisme per 2020 metus apytiksliai buvo išnagrinėta vos 0,6 % iš visų nagrinėtų bylų. Tuo tarpu civilinių sutarčių kontekste per 2020 metus gauta net 33 % iš 150 647 bylų (Civilinių bylų nagrinėjimo ataskaita (apeliacinės instancijos teismuose), 2020). Darbo autorė pažymi, kad dažniausiai ginčas tarp darbuotojų arba darbdavių atsiranda darbo santykių nutraukimo momentu. Vadinasi, toks ilgas darbo sutarčių saugojimas yra perteklinis ir nepagrįstas.

Darytina išvada, kad BDAR nurodo, kad pats duomenų valdytojas turi apibrėžti saugojimo terminus, tačiau būtina atsižvelgti į nacionalinius teisės aktus, kurie nustato minimalius saugojimo terminus. Darbo autorės nuomone saugojimo terminai yra pakankamai per ilgi ir neproporcingi, todėl siūlytina įstatymų leidėjui pakartotinai peržiūrėti terminų standartus ir įvertinti besikeičiančios darbo rinkos tendencijas ir pokyčius. Paminėtina, kad prieš 10, 20 metų ilgalaikiai ir stabilūs darbo santykiai – buvo standartas. Visgi, Y karta yra labiau savarankiškesnė, lankstesnė, greitai priprantanti prie pokyčių ir siekianti naujovių, todėl šiai kartai darbo pokytis yra judėjimas į priekį, o duomenų saugojimas apkrauna darbdavio informacinės sistemas bergždžia informacija.

3.2. Buvusio darbuotojo teisės BDAR kontekste

Kai yra nutraukiama darbo sutartis, buvęs darbuotojas nepraranda BDAR numatytų duomenų subjektų teisių. Toliau bus plačiau analizuojama darbuotojo teisė būti pamirštam bei teisė į duomenų perkėlimą.

Remiantis duomenų apsaugos teise nustatoma, kad tam tikrais atvejais duomenų subjektas turi teisę reikalauti, jog duomenų valdytojas nepagrįstai nedelsdamas ištrintų su juo susijusius duomenis, o šis įpareigotas tai padaryti (BDAR 17 str. 1d., ET duomenų apsaugos konvencijos 9 str. 1 d. e p.). EBPO privatumo gairėse numatoma abstraktesnė duomenų subjekto teisė ginčyti su juo susijusius duomenis ir, jeigu prieštarašavimas yra priimamas, reikalauti juos ištrinti (Zaleckis, 2019, p. 185). BDAR 17 str. 1 d. a p. detalizuoja, kad teisė reikalauti ištrinti duomenis atsiranda, kai asmens duomenys nebėra reikalingi, kad būtų pasiekti tikslai, kuriais jie buvo renkami arba kitaip tvarkomi.

Duomenų subjektui turėtų būti taikoma teisė reikalauti, kad jo asmens duomenys būtų ištrinti ir toliau nebetvarkomi, kai šių duomenų nebereikia tiems tikslams, kuriems jie buvo renkami ar kitaip tvarkomi (BDAR 17 str. 1 d. a p.) (Zaleckis, 2019, p. 185).

Taigi, teisė būti pamirštam taikoma esant bent vienam BDAR 17 str. esančiam pagrindui. Pirmiausia, duomenų valdytojas gavęs prašymą apie reikalavimą ištrinti su buvusiu darbuotoju susijusius duomenis, darbdavys turi įvertinti ir patikrinti, ar prašymas atitinka bent vieną BDAR 17 str. nurodytą sąlygą. Darbdavys įvertinęs, kad duomenų subjekto prašymą neatitinka šio straipsnio – prašymą gali atmesti. Pavyzdžiui, darbuotojas reikalauja, kad darbdavys ištrintų duomenis apie pasikeitusi gyvenamosios vietos adresą. Tai atvejai, kai darbuotojas atskiru prašymų būdamas darbo santykiuose informuoja darbdavį apie pasikeitusią lokaciją. Šiuo atveju darbdavys įvertinęs, kad toks priedas prie sutarties iš tiesų neturi teisinės reikšmės (nėra inicijuotas teisinis ginčas, pavyzdžiui, po 5 metų nuo darbo sutarties nutraukimo), galėtų iš dalies įgyvendinti darbuotojo teisę būti pamirštam.

ESTT vienoje iš bylų nurodė, kad išskyrus specialiose nuostatose, kurias valstybės narės gali priimti dėl duomenų tvarkymo istoriniais, statistiniais ar moksliniais tikslais, numatytus atvejus duomenų valdytojas turi užtikrinti, kad asmens duomenys būtų „tvarkomi teisingai ir teisėtai“, „surinkti įvardintais, aiškiai apibrėžtais ir teisėtais tikslais, o po to [ne]tvarkomi su šiais tikslais [ne]suderintais būdais“, būtų „adekvatūs, susiję ir savo apimtimi neviršijantys tikslų, kuriems jie renkami ir (arba) vėliau tvarkomi“, būtų „tikslūs ir, jei būtina, nuolat atnaujinami“ ir, galiausiai, būtų saugomi „tokio pavidalo, kad duomenų subjektų tapatybes būtų galima nustatyti ne ilgiau, nei tai yra reikalinga tais tikslais, dėl kurių duomenys buvo surinkti arba po to tvarkomi“. Šiais atvejais duomenų valdytojas turi imtis visų reikalingų priemonių, kad duomenys, kurie neatitinka šioje nuostatoje nurodytų reikalavimų, būtų ištrinti arba ištaisyti (Europos Sąjungos Teisingumo teismas (didžioji kolegija) 2014 m. gegužės 13 d. sprendimas byloje Google Spain SL ir Google Inc. prieš Agencia Española de Protección de Datos (AEPD) ir Mario Costeja González Nr. C131/12). Darbo santykiams pasibaigus darbdavys įvertinęs kompetentingų institucijų užklausas privalo pateikti duomenis apie buvusį darbuotoją tik esant teisiniam pagrindui. Pavyzdžiui, policijai, teismas suteikti informaciją apie nelaimingo atsitikimo metu darbe įvykusį incidentą; Sodrai, Valstybinei duomenų apsaugos inspekcijai suteikti informaciją mokesčių deklaravimo tikslais ir pan.

Paminėtina, kad gali būti teikiamos rekomendacijos apie buvusį darbuotoją. Pavyzdžiui, informuojant buvusį darbuotoją, darbdavys gali teikia rekomendaciją teikia raštu. Rekomendacijoje nurodomi tokie duomenys kaip vardas, pavardė, darbo laikotarpis,

pareigos, rekomendacija, darbo kokybę ir pan. Vadinasi, kad tam tikrų duomenų saugojimas apie buvusį darbuotoją yra aktualūs ne tik darbdaviui bet išimtiniais atvejais ir platesniam subjektų ratui.

Kita darbuotojo teisę į teisę į duomenų perkėlimą. BDAR duomenų subjektui suteikiama teisė gauti su juo susijusius asmens duomenis, kuriuos jis pateikė duomenų valdytojui susistemintu, įprastu naudojamu ir kompiuterio skaitomu formatu, ir teisę persiųsti šiuos duomenis kitam duomenų valdytojui, kuriam asmens duomenys buvo pateikti, tam turi nesudaryti jokių kliūčių (Zaleckis, 2019, p. 175). Pavyzdžiui, darbuotojas šia teise gali pasinaudoti tuomet, kai dokumentai darbovietėje yra tvarkomi automatizuotu būdu. Tai neturi būti atvejai, kai darbuotojas prašo darbdavio nuskenuoti rankiniu būdu visus dokumentus ir nusiųsti būsimam darbdaviui. Vadinasi, šia teise darbuotojas gali pasinaudoti tuomet, kai darbdavys surinktą informaciją saugo duomenų bazėse, pavyzdžiui, apie darbuotojo kvalifikacijos kėlimo mokymus, seminarus ir pan. Teigiama, kad tuomet darbuotojas gali kreiptis į darbdavį ir jam turėtų būti suteikta teisė pasinaudoti į duomenų perkėlimą.

Teisė į duomenų perkėlimą yra Europos Sąjungoje sukurta teisė, kaip naujovė BDAR, atsižvelgiant, kai vis daugiau paslaugų perkeliamos į elektroninę erdvę. Vadinasi, tai papildoma garantija, kuri sustiprina darbuotojo teisę susipažinti su duomenimis bei kontroliuoti savo duomenis. Teisine prasme tai reiškia, kad darbuotojas ne tik turi žinoti apie duomenų tvarkymą, gauti kopijas, bet ir turi teisę gauti visus savo duomenis, kuriuos pats pateikė darbdaviui darbo santykiu metu.

Darytina išvada, kad tuomet kai tarp darbdavio ir darbuotojo yra nutraukiama darbo sutartis, darbuotojas turi teisę prašyti, kad darbdavys ištrintų asmens duomenis pasibaigus saugojimo terminui, kuris yra iš anksto nustatytas vidiniuose įmonės, įstaigos ar organizacijos dokumentuose. Pabrėžtiną momentą, kad tuomet, kai darbuotojas išreiškia prieštaravimą, kad nesutinka su savo asmens duomenų tvarkymu, o darbdavys negali pagrįsti savo pirminio intereso, tai suveiks ne tik teisė prieštarauti bet ir teisė būti pamirštam pagal BDAR 17 str. Šiuo atveju visa įrodinėjimo našta tenka darbdaviui. Taip pat teisė į duomenų perkėlimą pagal BDAR 20 str. gali būti įgyvendinta tuomet, kai informacija saugoma skaitmeniniu formatu paties darbdavio.

IŠVADOS

1. Asmens tinkamumo eiti konkrečias darbo funkcijas įvertinimo ir priėmimo į laisvą darbo vietą tikslais gali būti tvarkomi pretendentų (kandidatų) į darbuotojus: vardai, pavardės, gimimo datos, kontaktiniai duomenys (gyvenamosios vietos adresai, telefono numeriai ir asmeninio elektroninio pašto adresai), informacija apie pareigas, į kurias pretenduojama, duomenys apie išsilavinimą ir kvalifikaciją bei kiti paties asmens pateikti duomenys.
2. Įmonės darbuotojai ar kiti atsakingi asmenys, kuriems suteikta teisė tvarkyti darbuotojų duomenis turi laikytis konfidencialumo principo ir laikyti paslapyje bet kokią su asmens duomenimis susijusią informaciją, su kuria jie susipažino eidami savo pareigas, nebent tokia informacija būtų vieša pagal galiojančių teisės aktų nuostatas. Pareiga saugoti asmens duomenų paslaptį taip pat galioja įmonės darbuotoją paskyrus į kitas pareigas bei pasibaigus darbo santykiams.
3. Specialių kategorijų duomenims pagal BDAR 9 str. turi būti numatyta apsauga, duomenų tvarkymo procesas bei suteikta darbuotojui informacija, kaip sveikatos duomenys renkami ir naudojami darbdavio vietoje.
4. Pagal BDAR 9 str. 1 d. biometriniai darbuotojų duomenys yra priskiriami prie draudžiamų duomenų tvarkymo kategorijos, nebent yra numatytos išimtys pagal BDAR 9 str. 2 p. Taip pat darbdavys privalo turėti darbuotojo sutikimą bei kritiškai įvertinti, ar toks duomenų rinkimas yra būtinas pagal iš anksto nustatytą teisinį interesą.
5. Darbuotojų duomenis turi teisę tvarkyti tik tie asmenys, kuriems jie yra būtini darbo funkcijų vykdymui, ir tik tuomet, kai tai yra būtina atitinkamiems tikslams pasiekti.
6. Darbuotojo sutikimas dėl atvaizdo išviešinimo privalo būti aiškus, suprantamas ir apibrėžtas. Darbdavys šį dokumentą gali pridėti, kaip priedą prie darbo sutarties arba šias nuostatas apibrėžti darbo sutartyje, leidžiant darbuotojai turėti pasirinkimo teisę dėl sutikimo arba nesutikimo.
7. Vaizdo stebėjimas turėtų būti naudojamas kaip kraštutinė priemonė, siekiant apsaugoti paties darbdavio turtą, siekiant užtikrinti darbų saugą ir pan. Tai reiškia, kai darbdavio interesas turi būti viršesnis nei darbuotojo tam, kad toks stebėjimas būtų teisėtas. Dėl stebėjimo vaizdo kameromis darbuotojo sutikimo nereikia.
8. Egzistuoja darbdavio pareiga informuoti darbuotoją apie telefoninių pokalbių įrašinėjimo tvarkymą ir pagrindą. Visgi, Lietuvoje nėra pakankamai daug teismų praktikos šiuo

klausimu. Paminėtina, kad pagal darbo pobūdį, pokalbių įrašinėjimas būtų privalomas, kad užtikrinti kokybišką darbo funkcijų įgyvendinimą.

9. Darbuotojo automobilio sekimas GPS priemonėmis galimas net ir tuomet, kai siekiama išvengiant darbuotojo ar trečiųjų šalių piktnaudžiavimo, vagystės ir pan. Kitais atvejais reikalaujamas darbuotojo sutikimas ir informavimas.
10. Darbuotojų elektroninių ryšių stebėjimas gali būti pateisinamas, tik tuomet, kai kyla pavojus darbdavio konfidencialios, ar net paties darbuotojo asmeninės informacijos atskleidimo galimybėms.
11. BDAR nurodo, kad pats duomenų valdytojas turi apibrėžti saugojimo terminus, tačiau būtina atsižvelgti į Lietuvos Vyriausiojo archyvaro įsakymą Nr. V-100 dėl bendrųjų dokumentų saugojimo terminų rodyklės patvirtinimo, kurie nustato minimalius saugojimo terminus.
12. Nutraukus darbo santykius, darbuotojas turi teisę prašyti, kad darbdavys ištrintų asmens duomenis pasibaigus saugojimo terminui pagal BDAR 17 str. Taip pat darbuotojas turi teisę į duomenų perkėlimą pagal BDAR 20 str.

ŠALTINIŲ SĄRAŠAS

Teisės norminiai aktai:

Tarptautiniai ir Europos Sąjungos teisės aktai:

1. Europos Parlamento ir Tarybos 2016 m. balandžio 27 d. reglamentas 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB. OJ L 119, 4.5.2016, p. 1–88.
2. Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija. Valstybės žinios, 1995, Nr. 40-987.

Lietuvos Respublikos teisės aktai:

3. Lietuvos Respublikos dokumentų ir archyvų įstatymas, *Valstybės žinios*, 1995-12-30, Nr. 107-2389.
4. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas, *Valstybės žinios*, 1996-07-03, Nr. 63-1479.
5. Lietuvos Respublikos civilinis kodeksas, *Valstybės žinios*, 2000-09-06, Nr. 74-2262.
6. Lietuvos Respublikos elektroninių ryšių įstatymas, *Valstybės žinios*, 2004-04-30, Nr. 69-2382.
7. Lietuvos Respublikos darbo kodeksas, *Valstybės žinios*, 2016-09-19, Nr. 23709.

Specialioji literatūra:

8. CIVILKA, Mindaugas; ŠLAPIMAITĖ, Lina. Asmens duomenų samprata elektroninėje erdvėje. *Teisė*, 2015, t. 96, p. 126-148.
9. DAVULIS, T. Lietuvos Respublikos darbo kodekso komentaras. Vilnius: VĮ *Registų centras*, 2018.
10. EKLUND, Mia Catharina. Monitoring employees' e-mail correspondence and Internet use – A Finnish perspective. *European Labour Law Journal*. 2019.
11. Maliauskaitė A., Šilkūnaitė M. (2015) Privatumas darbo vietoje: ar darbdavys gali skaityti Jūsų laiškus? [Interaktyvus]. Prieiga per internetą: <https://www.glimstedt.lt/publikacijos/privatumas-darbo-vietoje-ar-darbdavys-gali-skaityti-jusu-laiskus-lt-lt/>. [žiūrėta 2021 m. vasario 30 d.]

12. Ogriseg, Claudia. (2017) GDPR and Personal Data Protection in the Employment Context.
13. PETRAITYTĖ, Ilona. Asmens duomenų teisinės apsaugos principai: daktaro disertacija. Socialiniai mokslai, teisė (01S). Vilnius: Vilniaus universitetas, 2013.
14. Reuter T. (2018) Expert Q&A on Biometrics in the Workplace: Recent Developments and Trends. [Interaktyvus]. Prieiga per internetą: <https://www.ebglaw.com/content/uploads/2018/02/Sholinsky-Steinmeyer-Reuters-Expert-QA-Biometrics-February-2018.pdf>. [žiūrėta 2021 m. balandžio 10 d.]
15. TAMAŠAUSKAITĖ-JANICKĖ, Gintarė. Informacinių ir komunikacinių technologijų panaudojimas darbo vietoje darbo teisės požiūriu. Socialiniai mokslai, teisė (01 S). Vilnius: Vilniaus universitetas, 2016.
16. United Nations economic commission for Europe. (2013) Human Resources Management and Training. [Interaktyvus]. Prieiga per internetą: https://unece.org/DAM/stats/publications/HRMT_w_cover_resized.pdf. [žiūrėta 2021 m. balandžio 10 d.]
17. VU Teisės fakulteto Mokslinė teminė grupė. Veido atpažinimo technologijos – europietiško požiūrio formavimo procesas. [Interaktyvus]. Prieiga per internetą: <http://www.teise.pro/index.php/2021/02/28/veido-atpazinimo-technologijos-europietisko-poziuuro-formavimo-procesas/>. [žiūrėta 2021 m. vasario 28 d.]
18. ZALESKIS, Julius. Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė. Monografija. *Registru centras*, 2019.
19. Žmogaus teisių stebėjimo institutas (2005) Vaizdo stebėjimo kamerų panaudojimas ir žmogaus teisės. [Interaktyvus]. Prieiga per internetą: https://www.hrmi.lt/uploaded/PDF%20dokai/TYRIMAI/Vaizdo_stebejimo_kameru_panaudojimas_ir_zmogaus_teises_web.pdf. [žiūrėta 2021 m. kovo 4 d.]

Teismų praktika:

Tarptautinė ir Europos Sąjungos praktika:

20. Europos Žmogaus teisių teismo 1992 m. gruodžio 16 d. sprendimas byloje Niemietz prieš Vokietiją, Nr. 13710/88.

21. Europos Žmogaus teisių teismo byla Halford v. The United Kingdom, App. 20605/92, Judgment of 25 June, 1997. EHRR 523.
22. Europos Žmogaus teisių teismo 2003 m. balandžio 28 d. sprendimas byloje Peck prieš Jungtinę Karalystę, pareiškimo Nr.44647/98.
23. Europos Žmogaus teisių teismo byla 2007 m. liepos 3d. Copland prieš Jungtinę Karalystę, Nr. C-70/10.
24. Europos Sąjungos Teisingumo Teismo byla 2008 m. gruodžio 22 d. sprendimas byloje I-3889 College van burgemeester en wethouders van Rotterdam v. M. E. E. Rijkeboer, 2009.
25. Europos Sąjungos Teisingumo Teismo 2014 m. gegužės 13 d. sprendimas byloje C131/12 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González.
26. Europos Žmogaus Teisių Teismo 2016 m. sausio 12 d. sprendimas byloje Bărbulescu v. Romania, nr. 61496/08.
27. Europos Sąjungos Teisingumo Teismo 2017 m. kovo 9 d. sprendimas byloje C-398/15 Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni.

Lietuvos Respublikos Konstitucinis nutarimas:

28. Lietuvos Respublikos Konstitucinio teismo nutarimas 2015 m. vasario 26 d. Nr. KT8-N4/2015

Lietuvos Aukščiausiojo Teismo praktika:

29. Lietuvos Aukščiausiasis teismas nutartis Civilinių bylų skyriaus 2008 m. sausio 1d. nutartis civilinėje byloje Nr. 3K-7-2/2008
30. Lietuvos Aukščiausiojo teismo 2013 m. balandžio 23 d. nutartis baudžiamojoje byloje Nr. 2K-198/2013.
31. Lietuvos Aukščiausiojo teismo 2014 m. gegužės 6 d. nutartis baudžiamojoje byloje Nr. 2K-213/2014.

Lietuvos vyriausiojo administracinio teismo praktika:

32. Lietuvos vyriausiojo administracinio teismo 2012 m. liepos 26 d. sprendimas administracinėje byloje Nr. A⁸⁵⁸-2133/2012.

33. Lietuvos vyriausiojo administracinio teismo 2016 m. gruodžio 7 d. nutartis administracinėje byloje Nr. eA-2333-525/2016.
34. Lietuvos vyriausiojo administracinio teismo 2018 m. sausio 24 d. nutartis administracinėje byloje Nr. eA-3-822/2018.
35. Lietuvos vyriausiasis administracinis teismas 2020 m. liepos 1 d. nutartis administracinėje byloje Nr. eA-2601-629/2020.

Kita Lietuvos teismų praktika:

36. Vilniaus apygardos teismo Civilinių bylų skyriaus 2010 m. gegužės 6 d. nutartis civilinėje byloje Nr. 3K-3-177/2010
37. Lietuvos apeliacinio teismo 2011 m. rugsėjo 5 d. nutartis civilinėje byloje Nr. 2A-1502/2011.
38. Šiaulių apygardos teismo 2011 m. lapkričio 2 d. nutartis civilinėje byloje Nr. 2A-666-368/2011.
39. Kauno apygardos teismo 2011 m. lapkričio 24 d. nutartis civilinėje byloje Nr. 2A-2130-555/2011.
40. Vilniaus apygardos teismo Civilinių bylų skyriaus 2012 m. gruodžio 28 d. nutartis civilinėje byloje Nr. 2A-3217-781/2012.
41. Klaipėdos apylinkės teismo 2013 m. birželio 21 d. nutarimas Nr. A2.11.-2002-512/2013.
42. Vilniaus apygardos teismo Civilinių bylų skyriaus 2018 m. lapkričio 20 d. nutartis civilinėje byloje Nr. 2A-1417-614/2018.
43. Vilniaus apygardos teismo Civilinių bylų skyriaus 2019 m. kovo 18 d. nutartis civilinėje byloje Nr. e2A-588-656/2019.
44. Vilniaus apygardos administracinio teismo 2020 m. gruodžio 3 d. sprendimas administracinėje byloje Nr. eI2-4192-811/2020.

Kita teismų praktika:

45. Amsterdamo teismo 2019 m. rugpjūčio 5 d. sprendimas Nr. 7728204 CV VERZ 19-9686. [Interaktyvus]. Prieiga per internetą: <https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2019:6005>. [žiūrėta 2021 m. balandžio 2 d.]

Kita praktinė medžiaga:

46. Lietuvos Vyriausiojo archyvaro įsakymas dėl bendrųjų dokumentų saugojimo terminų rodyklės patvirtinimo, *Valstybės žinios*, 2011-03-17, Nr. 32-1534.
47. Valstybinė duomenų apsaugos inspekcijos direktoriaus įsakymas dėl duomenų tvarkymo operacijų, kurioms taikomas reikalavimas atlikti poveikio duomenų apsaugai vertinimą, sąrašo patvirtinimo Nr. 1T-35 (1.12.E), *TAR*, 2019-03-14, Nr. 4104.
48. Europos duomenų apsaugos valdyba, Gairės 05/2020 dėl sutikimo pagal Reglamentą 2016/679. [Interaktyvus]. Prieiga per internetą: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_lt_0.pdf. [žiūrėta 2021 m. kovo 13 d.]
49. Civilinių bylų nagrinėjimo ataskaita (apeliacinės instancijos teismuose), 2020. [Interaktyvus]. Prieiga per internetą: <https://www.teismai.lt/lt/visuomenei-ir-ziniasklaidai/statistika/106> . [žiūrėta 2021 m. kovo 21 d.]
50. Interviu su Valstybinės duomenų apsaugos inspekcijos Teisės skyriaus patarėja, 2021.

Soft law šaltiniai:

51. ES 29 straipsnio duomenų apsaugos darbo grupė. 2007 m. birželio 20 d. Nuomonė Nr. 4/2007 dėl asmens duomenų apsaugos sąvokos Nr. 01248/07/LT WP 136. [Interaktyvus]. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_lt.pdf. [žiūrėta 2021 m. kovo 3 d.]
52. ES 29 str. duomenų apsaugos darbo grupė. 2014 m. balandžio 9 d. Nuomonė Nr. 06/2014 dėl duomenų valdytojo teisėtų interesų sampratos pagal Direktyvos 95/46/EB 7 straipsnį. Nr. 06/2014, 844/14/LT WP 217. [Interaktyvus]. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_lt.pdf. [žiūrėta 2021 m. kovo 3 d.]
53. ES 29 straipsnio duomenų apsaugos darbo grupė. 2017 m. birželio 8 d. Nuomonė Nr. 2/2017 dėl duomenų tvarkymo darbe Nr. 17/LT WP 249. [Interaktyvus]. Prieiga per internetą: [https://vdai.lrv.lt/uploads/vdai/documents/files/Nuomonedelduomenutvarkymodrabe20170608wp249lt\(2\).pdf](https://vdai.lrv.lt/uploads/vdai/documents/files/Nuomonedelduomenutvarkymodrabe20170608wp249lt(2).pdf). [žiūrėta 2021 m. kovo 3 d.]

SANTRAUKA

BDAR ir darbo teisė

Paula Juchnevič

Magistro darbe analizuojama BDAR ir darbo teisės tema, kurioje nagrinėjama reikšmingi tarptautiniai teisės aktai, Europos Žmogaus teisių teismo, Europos Sąjungos teisingumo teismo formuojama praktika. Lygiagrečiai Lietuvoje atsakymu šia tema galima rasti įstatymuose ir kituose poįstatyminiuose aktuose. Šios temos kontekste reikšminga vaidmenį atlieka savo gausiomis gairėmis, rekomendacijomis, kuriamais projektais ir organizuojamais mokymais / konferencijomis Valstybinė duomenų apsaugos inspekcija.

Darbe analizuojama asmens duomenų kelio pradžia nuo kandidato gyvenimo aprašymo išsiuntimo potencialiam darbdaviui santykis su BDAR principais, atvejai dėl kandidato sutikimo dėl asmens duomenų tvarkymo. Detaliau darbo temoje aiškiai išskiriamos temos, kurios atvaizduoja realią situaciją su kuriomis dažniausiai susiduriama darbo santykių eigoje asmens duomenų apsektu.

Darytina išvada, kad šiame asmens duomenų kupiname pasaulyje reikia šviesti, mokyti darbuotojus ginti teisę į privatumą, o darbdaviams kurti strategijas ir semtis žinių, kaip nepažeidžiant duomenų subjekto teisių, sugebėti sukurti teisėtą ir proporcingą sistemą duomenų rinkimui bei stebėjimui.

SUMMARY

GDPR and Labour Law

Paula Juchnevič

The master's thesis analyzes the topic of GDPR and labor law, in which international legal instruments, the case law of the European Court of Human Rights and the Court of Justice of the European Union are relevant. At the same time, the answer to this topic in Lithuania can be found in laws and other by-laws. In the context of this topic, the State Data Protection Inspectorate plays an important role in providing many guidelines, recommendations, projects and trainings / conferences.

The work analyzes the beginning of the personal data path from the sending of the candidate's CV to the potential employer in relation to the GDPR principles, cases of the candidate's consent to the processing of personal data. The detailed topic of the work clearly distinguishes the topics that reflect the real situation that is most often encountered in the course of the employment relationship in terms of personal data.

It can be concluded that in this world full of personal data, there is a need to educate, train employees to protect the right to privacy, and for employers to develop strategies and knowledge on how to create a legitimate and proportionate system for data collection and monitoring without violating data subjects' rights.