Vilnius University Press

Contents lists available at Vilnius University Press

Teisė
2024, Vol. 133, pp. 103–117

ISSN 1392-1274 eISSN 2424-6050
DOI: https://doi.org/10.15388/Teise.2024.133.7

Darbuotojų stebėjimas panaudojant algoritminį valdymą, grįstą dirbtinio intelekto sistemomis

Ineta Breskienė

Vilniaus universiteto Teisės fakulteto
Privatinės teisės katedros doktorantė
Saulėtekio al. 9, I rūmai, LT-10222 Vilnius, Lietuva
Tel.: (+370 5) 236 61 70
El. paštas: ineta.breskiene@tf.vu.lt

Employee Surveillance Using Algorithmic Management Based on Artificial Intelligence Systems

Ineta Breskienė

(Vilnius University (Lithuania))

Summary. The article analyses the legal regulation of employee surveillance managed by employers carried on algorithmic management based on artificial intelligence systems. Employers observe employees and their work so that to smoothly organize work processes at workplaces, ensure efficient use of resources, and manage risks. Through the process of surveillance, personal data of employees are collected, which are later analysed; hence, employees may experience direct legal consequences (for example, termination of employment, violations of work duties, adjusted wages, etc.). Algorithmic management based on artificial intelligence systems generates various risks to employees. Before starting their application, employers have to evaluate various requirements. The key requirements arise from the *Artificial Intelligence Act*, the *General Data Protection Regulation* and the practice formed by the European Court of Human Rights which has been established regarding employee surveillance. Also, the employer has the obligation to ensure the employee's privacy rights, since, when applying algorithmic management, artificial intelligence systems can sometimes make hardly predictable insights and reveal extremely sensitive facts about the employee. The issue of informing and consulting employees and their representatives regarding the implementation and use of algorithmic management based on artificial intelligence systems in the work environment is analysed.
Keywords: algorithmic management, artificial intelligence systems, surveillance, personal data, privacy, employees, employees' representatives.

Darbuotojų stebėjimas panaudojant algoritminį valdymą, grįstą dirbtinio intelekto sistemomis

Ineta Breskienė

(Vilniaus universitetas (Lietuva))

Santrauka. Straipsnyje nagrinėjamas darbuotojų stebėjimo, darbdavio atliekamo algoritminiu valdymu, grįstu dirbtinio intelekto sistemomis, teisinis reguliavimas. Darbdaviai norėdami sklandžiai organizuoti darbo procesus darbovietėse, užtikrinti efektyvų išteklių naudojimą, valdyti rizikas, stebi darbuotojus ir jų atliekamą darbą. Stebėjimo metu renkami

Received: 30/11/2024. **Accepted:** 12/12/2024

darbuotojų asmens duomenys, kurie vėliau analizuojami ir darbuotojai gali patirti tiesiogines teisines pasekmes (pavyzdžiui, nutraukti darbo santykiai, nustatytas darbo pareigų pažeidimas, koreguojamas darbo užmokestis ir pan.). Algoritminis valdymas, grįstas dirbtinio intelekto sistemomis, kelia įvairias rizikas darbuotojams. Darbdaviai prieš pradėdami jį naudoti turi atlikti įvairių teisinių reikalavimų analizę. Pagrindiniai reikalavimai kyla iš Dirbtinio intelekto akto, Bendrojo asmens duomenų apsaugos reglamento, Europos Žmogaus Teisių Teismo suformuotos praktikos, skirtos darbuotojų stebėjimui. Taip pat darbdaviui tenka prievolė užtikrinti darbuotojo teisę į privatų gyvenimą, kadangi algoritminio valdymo metu dirbtinio intelekto sistemos gali atlikti kartais sunkiai prognozuojamų įžvalgų ir apie darbuotoją atskleisti itin jautrių faktų. Analizuojamas darbuotojų ir jų atstovų informavimo ir konsultavimo klausimas dėl algoritminio valdymo, grįsto dirbtino intelekto sistemomis, diegimo ir naudojimo darbo aplinkoje.
Pagrindiniai žodžiai: algoritminis valdymas, dirbtinio intelekto sistemos, stebėjimas, asmens duomenys, privatumas, darbuotojai, darbuotojų atstovai.

Įvadas

Darbdaviai norėdami sklandžiai organizuoti darbo procesus darbovietėse, užtikrinti efektyvų išteklių naudojimą, valdyti rizikas, pasitelkia įvairias priemones, kurių pagalba gali stebėti darbuotojus ir jų atliekamą darbą. Algoritminis valdymas[1] (angl. *algorithmic management*), grįstas dirbtinio intelekto sistemomis, gali būti lengvai pritaikomas darbuotojų stebėjimui darbo vietoje ir jų atliekamo darbo analizei. Dar visai neseniai nė viena technologija negalėjo įvertinti daug duomenų arba padaryti naudingų išvadų (Europos duomenų apsaugos teisės..., 2021, p. 362), tačiau dirbtinio intelekto sistemos geba itin greitai apdoroti didžiulius duomenų kiekius, kuriuos generuoja darbuotojai, juos savarankiškai, be žmogaus įsikišimo analizuoti ir daryti išvadas, teikti rekomendacijas ir pan. Panaudodami algoritminį valdymą, grindžiamą dirbtinio intelekto sistemomis, darbdaviai gali stebėti darbuotojus, jų atliekamą darbą, rinkti jų asmens duomenis, analizuoti darbuotojų rezultatyvumą, produktyvumą darbe ir, jeigu reikia, imtis atitinkamų veiksmų, sukeliančių tiesiogines teisines pasekmes patiems darbuotojams (pavyzdžiui, nutraukti darbo santykius, nustatyti darbo pareigų pažeidimus, koreguoti darbo užmokestį ir pan.). Darbdavio siekis stebėti dirbančius darbuotojus ir naudoti algoritminį valdymą, grįstą dirbtinio intelekto sistemomis, privalo atitikti teisinius reikalavimus, kurių turinys atskleidžiamas šiame straipsnyje.

Temos *aktualumą* pagrindžia algoritminio valdymo, grįsto dirbtinio intelekto sistemomis, naudojimo darbuotojų atžvilgiu problematika. Algoritminis valdymas, grįstas dirbtinio intelekto sistemomis, yra viena iš naujų darbdavio pasitelkiamų priemonių, pastaruoju metu pradedamų vis dažniau naudoti atliekamo darbo ir darbuotojų stebėjimui, todėl jos panaudojimo teisėtumą reikia analizuoti ir iš teisinės perspektyvos.

Algoritminio valdymo, grįsto dirbtinio intelekto sistemomis, panaudojimo tematiką darbo teisėje pastaruoju metu nagrinėjo Valerio De Stefano, Jeremias Adamsas-Prasslas, Ernesto Klengelis, Adrianas Todolis-Signes, Mohammadas Hosseinas Jarrahis ir kt. Lietuvoje atliktų tyrimų nagrinėjama tema nėra, todėl ją galima laikyti *originalia ir nauja*. Lietuvos autorių didesnis dėmesys skiriamas darbo santykių ir duomenų apsaugos temai – darbuotojų asmens duomenų apsaugos klausimai nagrinėjami Tomo Davulio (Davulis, 2018, p. 113–120), Juliaus Zaleskio (Zaleskis, 2018, p. 255–260), Rasos Grigonienės (Grigonienė, 2020, p. 346–369) moksliniuose darbuose, privatumo darbe klausimui – Tomo Bagdanskio, Pauliaus Sartatavičiaus (Bagdanskis, Sartatavičius, 2012, p. 697–713), Eglės Štareikės (Štareikė, 2021, p. 221–235). Gintarė Tamašauskaitė-Janickė yra nagrinėjusi informacinių technologijų poveikį darbuotojų privatumui, technologijų panaudojimo darbo vietoje klausimus (Tamašauskaitė, 2013, p. 195–210;

[1] Algoritminis valdymas šiame straipsnyje suprantamas kaip darbdavio veiklos (darbuotojų stebėjimo, kontrolės, valdymo ir kita) funkcijų delegavimas algoritmams, kurie yra pagrįsti dirbtinio intelekto sistemomis.

2016, p. 1–310), tačiau G. Tamašauskaitės-Janickės tyrimas atliktas iki 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (toliau – BDAR) ir naujojo Lietuvos Respublikos darbo kodekso (toliau – Darbo kodeksas) įsigaliojimo bei jis neapima algoritminio valdymo, grįsto dirbtinio intelekto sistemomis, temos.

Straipsnio *tyrimo objektas* yra darbuotojų stebėjimo panaudojant algoritminį valdymą, grįstą dirbtinio intelekto sistemomis, teisinis reguliavimas[2] ir suformuota teismų praktika (darbuotojų stebėjimo srityje). Šio straipsnio *tikslas* – sistemiškai išanalizuoti teisės aktų nuostatas, teismų praktiką, teisės doktriną ir nustatyti darbuotojų stebėjimo panaudojant algoritminį valdymą, grįstą dirbtinio intelekto sistemomis, teisėtumo reikalavimus. Siekiant įvardyto tikslo, keliami šie *uždaviniai: pirma,* aptarti algoritminio valdymo, grindžiamo dirbtinio intelekto sistemomis, panaudojimą darbuotojų atžvilgiu; *antra*, išanalizuoti teisinius reikalavimus, keliamus darbuotojų stebėjimui BDAR ir asmens teisės į privatumą gynimo kontekstuose; *trečia,* ištirti procedūrinius reikalavimus dėl darbdavio sprendimo stebėti darbuotojus darbo vietoje algoritminiu valdymu, grįstu dirbtinio intelekto sistemomis.

Atliekamas tyrimas grindžiamas sisteminės analizės, teleologiniu, precedentiniu, istoriniu *metodais*. Sisteminės analizės metodu naudotasi siekiant ištirti teisės doktriną ir joje pateikiamą diskursyvų požiūrį į algoritminį valdymą, grįstą dirbtinio intelekto sistemomis; teleologinis metodas leido atskleisti naujai priimto, su dirbtinio intelekto sistemomis susijusio, teisės akto siekiamus tikslus, kai kurių straipsnių turinio prasmę; istorinis metodas naudotas siekiant atskleisti dirbtinio intelekto sąvokos, kuri reikšminga algoritminio valdymo naudojimui, įteisinimo aplinkybes; precedentiniu metodu buvo remiamasi analizuojant Europos Žmogaus Teisių Teismo (toliau - EŽTT) suformuotą praktiką. Tyrime didelę reikšmę turėjo šie *šaltiniai ir literatūra*: Europos Sąjungos duomenų apsaugos direktyvos 29 straipsniu įsteigtos darbo grupės asmenų apsaugai tvarkant asmens duomenis (toliau - ES 29 straipsnio duomenų apsaugos darbo grupė) nuomonės ir gairės (ypač Nuomonė 2/2017 dėl duomenų tvarkymo darbe), V. De Stefano, Aude Cefaliello, Miriam Kullmann, T. Davulio ir kitų mokslininkų darbai.

1. Algoritminio valdymo, grįsto dirbtinio intelekto sistemomis, panaudojimas darbuotojų atžvilgiu

Dirbtinio intelekto sistemų terminą pirmą kartą 1956 m. pavartojo mokslininkas J. McCarthy, tačiau ši technologija buvo žinoma daug anksčiau (George, Thomas, 2019, p. 5069). Ilgus dešimtmečius nerasta kompromiso dėl dirbtinio intelekto sistemų sąvokos apibrėžties ir įteisinimo teisės aktu, tačiau Europos Komisija baltojoje knygoje nurodė, jog dirbtinio intelekto sistemų sąvoka turi atsirasti ir kad ji turės būti gana lanksti, kad būtų galima atsižvelgti į technikos pažangą, ir kartu gana tiksli, kad būtų užtikrintas būtinas teisinis tikrumas (Baltoji knyga dirbtinis intelektas..., 2020). 2024 m. rugpjūčio 1 d. įsigaliojo DI aktas, jame įtvirtinant ir dirbtinio intelekto sistemos apibrėžtį[3]. Autorės A. Cefaliello ir

[2] Teisinis reguliavimas tiriamas nacionaliniu (t. y. Darbo kodeksas, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas (toliau – ADTAĮ)) ir Europos Sąjungos mastu galiojančių (BDAR ir 2024 m. birželio 13 d. Europos Parlamento ir Tarybos reglamentas (ES) 2024/1689 kuriuo nustatomos suderintos dirbtinio intelekto taisyklės ir iš dalies keičiami reglamentai (EB) Nr. 300/2008, (ES) Nr. 167/2013, (ES) Nr. 168/2013, (ES) 2018/858, (ES) 2018/1139 ir (ES) 2019/2144 ir direktyvos 2014/90/ES, (ES) 2016/797 ir (ES) 2020/1828 (Dirbtinio intelekto aktas) (toliau – DI aktas)) teisės aktų apimtyje.

[3] Dirbtinio intelekto sistema apibrėžiama kaip mašina grindžiama sistema, suprojektuota veikti įvairiais autonomijos lygiais, kuri po diegimo gali veikti prisitaikydama ir kuri, siekiant aiškių ar numanomų tikslų, iš gautos įvesties duomenų daro išvadą, kaip generuoti išvedinius, pavyzdžiui, predikcijas, turinį, rekomendacijas ar sprendimus, kurie gali turėti įtakos fizinei ar virtualiai aplinkai (DI akto 3 str. 1 p.).

M. Kullmann yra išskyrusios tokias esmines dirbtinio intelekto sistemų savybes: 1) duomenų rinkimą, kuris techniniu požiūriu gali būti begalinis, t. y. jis gali sekti beveik viską 24 valandas per parą, 7 dienas per savaitę; 2) duomenų tvarkymo galią ir gebėjimą akimirksniu įvairiais tikslais analizuoti didžiuosius duomenis; 3) algoritmų gebėjimą prognozuoti, teikti pasiūlymus, daryti išvadas; 4) techninį pajėgumą automatizuoti sprendimų priėmimą ir tam tikru mastu bendrauti su darbuotojais (Cefaliello, Kullmann, 2022, p. 544). Nurodytos savybės koreliuoja su DI akte įtvirtinta apibrėžtimi; ji papildomai akcentuoja, jog dirbtinio intelekto sistemos pasižymi tam tikro lygio autonomiškumu nuo sistemos kūrėjo ir gebėjimu savarankiškai pasiekti numatytus tikslus.

Darbdaviai dirbtinio intelekto sistemas pasitelkia su darbuotojų darbu susijusiuose procesuose algoritminiam valdymui atlikti. Algoritminis valdymas apibrėžiamas kaip įvairių technologinių priemonių ir metodų rinkinys, skirtas nuotoliniu būdu valdyti darbo jėgą, remiantis duomenų rinkimu ir darbuotojų stebėjimu, kad būtų galima automatizuoti arba nepilnai automatizuoti sprendimų priėmimą (Explainer: Algorithmic Management in the Workplace, 2019). Jis itin paplitęs tarp pavežėjų ir maisto išvežiotojų platformų, tačiau pandeminiu ir po pandeminiu laikotarpiu vis dažniau pradėtas naudoti ir tradicinėse darbo vietose (The Algorithmic Management of work..., 2022; Jarrahi et al., 2021, p. 2; The platformisation of work, 2023; Technical workshop on Practices..., 2021). Algoritminis valdymas yra socialinis – techninis procesas, apimantis techninę (technologijų pritaikymą) ir socialinę, organizacinę pusę (tikslai ir būdai, kaip ir kam technologijos naudojamos) (Jarrahi et al., 2021, p. 2; The Algorithmic Management of work..., 2022). Algoritminis valdymas, grindžiamas dirbtinio intelekto sistemomis, darbdavių naudojamas planuojant, organizuojant, paskirstant darbuotojų darbus, taip pat stebint jų atliekamą veiklą (De Stefano, 2019, p. 2; Todoli-Signes, 2021, p. 3), vertinant darbuotojų produktyvumą, priimant sprendimus dėl darbo santykių nutraukimo ar pakeitimo (Ebert et al., 2021, p. 3; Data and algorithms at..., 2021), darbo pareigų pažeidimo.

Algoritminis valdymas, grįstas dirbtinio intelekto sistemomis, gali būti ir labai naudingas tiek pačiam darbuotojui, tiek darbdaviui, pavyzdžiui, siekiant išvengti profesinės rizikos pavojų (Todoli-Signes, 2021, p. 4). Tačiau mokslinėje literatūroje ypač akcentuojamos grėsmės darbuotojams: intensyvus darbuotojų atliekamo darbo stebėjimas ir darbuotojų patiriama įtampa dėl terminų laikymosi, darbo kokybės gali sumažinti darbuotojų pasitenkinimą darbu ir sukelti emocinį išsekimą (The Algorithmic Management of work..., 2021); esanti diskriminacijos ir šališkumo tikimybė dirbtinio intelekto sistemų algoritmų priimamuose sprendimuose (Technical workshop on Practices..., 2021); algoritmų sprendimų priėmimo skaidrumo trūkumas ir sudėtingumas (Jarrahi et al., 2021, p. 8; Explainer: Algorithmic Management in the Workplace, 2019); darbuotojo privatumo ribų peržengimas, kai iš surinktų duomenų ir jų kombinacijų sužinoma itin jautri informacija (Data and algorithms at..., 2021); nepakankamas ir nevientisas darbuotojų teisių užtikrinimo mechanizmas, kai jų atžvilgiu taikomi algoritmais grįsti sprendimai (The platformisation of work, 2023). Be to algoritmai atmeta žmogiškuosius faktorius, skaičiuodami tik tikslius matematinius duomenis ir pateikdami rezultatus (Newlands, 2021, p. 730).

DI akte dirbtinio intelekto sistemos skirstomos į tris rizikos kategorijas[4]. Dirbtinio intelekto sistemos, kurios naudojamos užimtumo, darbuotojų valdymo ir galimybės dirbti savarankiškai srityse[5],

[4] Rizikų kategorijos yra šios: nepriimtina rizika, kuri yra draudžiama (pavyzdžiui, manipuliatyvus dirbtinis intelektas, socialinio vertinimo sistemos) (DI akto preamb. 26 p., 31 p., 46 p., 5 str.); didelė rizika (jai skiriama didžioji dalis DI akto); nedidelė rizika (DI akto preamb. 27 p.; 53 p. 50 str. 1 d.).

[5] DI akto III priedo 4 d. išskiriami tokie didelės rizikos atvejai: a) dirbtinio intelekto sistemos, skirtos naudoti fizinių asmenų įdarbinimui arba atrankai, visų pirma siekiant teikti tikslinius darbo skelbimus, analizuoti ir filtruoti darbo prašymus ir vertinti kandidatus; b) dirbtinio intelekto sistemos, skirtos naudoti priimant sprendimus, darančius poveikį darbo santykių sąlygoms**,** paaukštinimui arba darbo santykių nutraukimui, siekiant paskirstyti užduotis remiantis

klasifikuojamos kaip didelės rizikos sistemos, nes jos gali daryti apčiuopiamą poveikį tų asmenų būsimoms karjeros galimybėms, pragyvenimo šaltiniams ir darbuotojų teisėms (DI aktas, preamb. 57 p.). Ši klasifikacija užtikrina griežtus reikalavimus didelės rizikos dirbtinio intelekto sistemoms, įskaitant ir darbuotojų stebėsenai naudojamą algoritminį valdymą. Darbdaviui (diegėjui[6]), norinčiam darbo aplinkoje naudoti didelės rizikos dirbtinio intelekto sistemas, teks[7] prievolė laikytis DI akte numatytų atitikties įsipareigojimų[8], taip pat užtikrinti žmogaus vykdomą priežiūrą. Žmogiškasis veiksnys ir žmogaus atliekama priežiūra reiškia, kad, *pirma*, dirbtinio intelekto sistemos kuriamos ir naudojamos kaip priemonė, kuri tarnauja žmonėms, *antra*, gerbiamas žmogaus orumas ir asmens autonomiškumas, *trečia*, dirbtinio intelekto sistemos veikia taip, kad jas galėtų kontroliuoti ir prižiūrėti žmonės (DI akto preamb. 27 p., 14 str.). Asmuo, kuris darbe būtų atsakingas už algoritminį valdymą, grįstą didelės rizikos dirbtinio intelekto sistema, turėtų būti apmokytas ir turėti specialiųjų žinių kaip elgtis su atitinkama sistema; kompetentingas asmuo turėtų stebėti tokios sistemos veikimą, pernelyg nepasikliauti ir sugebėti teisingai interpretuoti generuojamus išvedinius (predikcijas, turinį, išvadas, rekomendacijas); tam tikrais atvejais nuspręsti nenaudoti algoritminio valdymo ar jo metu sukurto rezultato; taip pat gebėti sustabdyti, pakeisti ar ištaisyti sukurtus rezultatus (DI akto 14 str., 4 d.; 26 str. 2 d.).

Apibendrinant galima teigti, kad dirbtinio intelekto sistemos, kuriomis grindžiamas algoritminis valdymas, pasižymi tokiomis savybėmis: gebėjimu per itin trumpą laiką autonomiškai surinkti ir išanalizuoti didelius duomenų kiekius, pateikti išvedinius (išvadas, rekomendacijas, predikcijas, turinį) darbdaviui (diegėjui). Algoritminis valdymas, grįstas dirbtino intelekto sistemomis, yra patogi priemonė darbdaviams, gebanti sutaupyti jų skiriamą laiką rutininiams darbams, tokiems kaip darbų paskirstymas, darbuotojų drausmės kontrolė, darbuotojų kompetencijų vertinimas (o tai gali būti atliekama tik stebint darbuotojus) ir pan., tačiau jo panaudojimas DI akto priskiriamas prie didelės rizikos sistemų, dėl to algoritminio valdymo, grįsto dirbtinio intelekto sistemomis, panaudojimui darbuotojų atžvilgiu keliami griežti reikalavimai bei yra reikalinga žmogaus atliekama priežiūra.

2. Algoritminiu valdymu, grįstu dirbtinio intelekto sistemomis, atliekamo darbuotojų stebėjimo BDAR atitikties reikalavimai

Paprasčiausias būdas stebėti darbuotojus yra rinkti su jais susijusius duomenis. Surinktus duomenis galima panaudoti įvairiais tikslais, pavyzdžiui, sumokėti už darbo laiką, kokybę, sąnaudas, tačiau ir priimti kitokius sprendimus, kaip sprendimą dėl darbo sutarties nutraukimo arba darbo pareigų pažei-

individualiu elgesiu arba asmenybės bruožais ar savybėmis arba stebėti bei įvertinti tokiuose santykiuose dalyvaujančių asmenų rezultatus ir elgesį (DI aktas, III priedas, 4 d. a) ir b) p.).

[6] DI akte diegėjas apibrėžiamas kaip fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, naudojantys DI sistemą pagal savo įgaliojimus, išskyrus atvejus, kai DI sistema naudojama asmeniniais neprofesinės veiklos tikslais (DI akto 3 str. 4 p.)

[7] DI aktas turėtų būti taikomas nuo 2026 m. rugpjūčio 2 d., su tam tikromis išlygomis.

[8] Darbdavys (diegėjas) naudodamas didelės rizikos dirbtinio intelekto sistemas turi: 1) imtis tinkamų techninių ir organizacinių priemonių tam, kad dirbtinio intelekto sistemos būtų naudojamos pagal instrukcijas (DI akto 26 str. 1 d.); 2) užtikrinti, kad įvesties duomenys į dirbtinio intelekto sistemas būtų aktualūs ir reprezentatyvūs (DI akto 26 str. 4 d.); 3) stebėti dirbtinio intelekto sistemų veikimą, o apie incidentus informuoti tiekėją ar platintoją ir atitinkamą rinkos priežiūros instituciją, sustabdyti sistemos naudojimą, jeigu reikalinga (DI akto 26 str. 5 d.); 4) saugoti bent šešis mėnesius dirbtinio intelekto sistemų sugeneruotus žurnalus (DI akto 26 str. 6 d.); 5) įdiegti ir dokumentuoti rizikos valdymo sistemą (DI akto 9 str.); 6) atlikti poveikio pagrindinėms teisėms vertinimą DI akto numatytais atvejais (DI akto 27 str.).

dimo. Rinkoje yra daugybė darbuotojams stebėti skirtų produktų[9], o kai kurie iš jų yra grįsti dirbtinio intelekto sistemomis. Kaip teigia Gemma Newlands, būtina algoritminiu valdymu, grįstu dirbtinio intelekto sistemomis, atliekamo stebėjimo sąlyga yra ta, kad dirbtinio intelekto sistemoms reikalingi dideli kiekiai duomenų, susijusių su darbuotojų veikla (Newlands, 2021, p. 723). Kuo daugiau duomenų surenkama apie atskirus darbuotojus, tuo vertingesni šie duomenys tampa prognozėms, pagrįstoms dirbtinio intelekto sistemų metodais (Ebert et al., 2021, p. 3). Kai algoritminio valdymo, grįsto dirbtinio intelekto sistemomis, metu stebint darbuotojus surenkami duomenys, kuriuos vėliau dirbtinio intelekto sistema analizuoja ir apdoroja rezultatams gauti, yra susiję su fizinių asmenų asmens duomenimis, turi būti taikomos BDAR nuostatos (BDAR 1 str. 1 d.). Nustačius, jog darbdavys renka darbuotojų asmens duomenis, atsiranda papildomi reikalavimai, kuriuos numato BDAR.

Stebėjimo tikslą (-us) svarbu identifikuoti ir apibrėžti dar prieš pradedant rinkti darbuotojų asmens duomenis. BDAR 5 str. 1 d. b p. apibrėžia tokias tikslo apribojimo principo sąlygas: 1) aiškus teisėto tikslo nurodymas ir 2) suderinamas naudojimas (Biega, Finck, 202, p. 48). Tai suponuoja, kad bet koks darbuotojo asmens duomenų tvarkymo tikslas turi būti aiškus, konkretus, teisėtas; kartu darbuotojams turi būti suprantama, kokiais tikslais jų asmens duomenys bus renkami ir kokiems tikslams naudojami, ypač kai tai atlieka ne žmogus, o dirbtinio intelekto sistema. Teisėtumo reikalavimas turėtų būti suprantamas plačiai ir apimti visas rašytinės ir bendrosios teisės formas, pirminius ir antrinius teisės aktus <...> t. y. kaip tokią „teisę“ aiškintų ir ja remtųsi kompetentingi teismai (Nuomonė Nr. 03/2013 dėl.., 2013). Be to reikėtų atsižvelgti ir į srities, kurioje norima nustatyti tikslus, specifiką. Antroji sąlyga lemia tai, kad draudžiamas bet koks tolesnis asmens duomenų panaudojimas, kuris savo esme prieštarauja pirminiam tikslui. Pastebėtina, kad dėl algoritminio valdymo metu naudojamos dirbtinio intelekto sistemos autonomiškumo savybės visuomet išlieka rizika, jog pirminis stebėjimo tikslas ilgainiui gali pasikeisti, nes ši sistema geba persiprogramuoti, ir tam tikrais atvejais bus sudėtinga nustatyti, kuriame dirbtinio intelekto sistemos veiklos etape tas konkretus pirminis tikslas baigėsi ir prasidėjo naujas (De Stefano, 2019, p. 15).

Darbdavys privalo įvertinti darbuotojų stebėjimui pasirinktų priemonių būtinumą ir ar jos proporcingos siekiant užsibrėžto tikslo. Kuo labiau trikdantis, intensyvus yra darbuotojo stebėjimas ir jo duomenų rinkimas, tuo mažesnė tikimybė, kad darbdavys galės proporcingai pagrįsti šią veiklą: fiksuojant klavišų paspaudimus ar pelės judesius, su algoritminiu valdymu, grįstu dirbtinio intelekto sistemomis, susijęs duomenų tvarkymas yra netinkamas; labai mažai tikėtina, kad darbdavys turės teisinį pagrindą ir pagal teisėtą interesą (Adams-Prassl, 2022, p. 39). Šiame algoritminio valdymo, grindžiamo dirbtinio intelekto sistemomis, panaudojimo kontekste reikšminga ES 29 straipsnio duomenų apsaugos darbo grupės nuomonė dėl biometrinių technologijų pokyčių. Ne visi asmens duomenys, kurie būtų tvarkomi algoritminio valdymo, grįsto dirbtinio intelekto sistemomis, metu bus biometriniai duomenys, bet, atliekant poveikio duomenų apsaugai vertinimą pagal BDAR 35 str., tie patys aspektai, padedantys darbdaviui nustatyti tokios priemonės būtinumą, proporcingumą tinka ir nagrinėjamam klausimui. Pirma, reikia atsižvelgti ar algoritminis valdymas, grįstas dirbtinio intelekto sistemomis, yra būtinas nustatytam poreikiui patenkinti, ar pasirenkama ne dėl ekonomiškumo ar patogumo; antra, tikimybė, kad algoritminis valdymas, grįstas dirbtinio intelekto sistemomis, padės

[9] Pavyzdžiui „ActivTrack“ stebi programas, kurias naudoja darbuotojai ir praneša jų vadovams, jeigu naudojami socialiniai tinklai; „Interguard“ minučių tikslumu sudaro grafiką, kuriame atsispindi visi darbuotojo veiklos duomenys jo kompiuteryje, siunčia pranešimus vadovams, jeigu darbuotojų atliekama veikla nėra įprastinė jų darbo veiklai (Aloisi, De Stefano, 2022, p. 298); „Zonar“ sistema leidžia darbuotojų vadovams ir jų kolegoms įvertinti darbuotojų darbą, kai toks įvertinimas gali turėti įtakos išmokant premijas ar svarstant pareigų paaukštinimo galimybes (Employee Evaluation Sytem may..., 2020).

pasiekti tikslą; trečia, ar darbuotojų privatumo ribų susiaurinimas atsvers siekiamos naudos gavimą; ketvirta, ar norimą tikslą galima pasiekti mažiau darbuotojų privatumą ribojančiomis priemonėmis (Nuomonė Nr. 3/2012 dėl biometrinių technologijų..., 2012). Intensyvus darbuotojo darbo stebėjimas algoritminiu valdymu, grįstu dirbtinio intelekto sistemomis, kai darbuotojas stebimas visą jo dirbamą darbo laiką, daromos ekrano nuotraukos, skaičiuojamos atsitraukimo nuo ekrano minutės ir pan., gali būti laikomas netinkamai pasirinkta darbuotojo darbo stebėjimo priemone ir, priešingai: įvertinus darbuotojo pareigybės aprašymą, jo atliekamų funkcijų svarbą, nustačius adekvačią stebėjimo apimtį bei intensyvumą, stebėjimas algoritminiu valdymu, grįstu dirbtinio intelekto sistemomis, galėtų būti tinkamas ir proporcingas.

Kitas svarbus aspektas, kad bet koks asmens duomenų tvarkymas turi būti pagrįstas bent viena teisėto tvarkymo sąlyga iš BDAR 6 str.: 1) duomenų subjekto sutikimas, 2) siekiant įvykdyti sutartį tarp darbuotojo ir darbdavio, 3) reikia įvykdyti darbdaviui taikomą teisinę prievolę, 4) siekiant apsaugoti gyvybinius darbuotojo ar kito fizinio asmens interesus, 5) siekiant atlikti užduotį viešojo intereso labui, 6) siekiant teisėtų darbdavio arba trečiosios šalies interesų; ir, kai reikalinga (esant poreikiui tvarkyti specialių kategorijų asmens duomenis, pavyzdžiui, sveikatos duomenis, narystės profesinėje sąjungoje duomenis), BDAR 9 str. įtvirtintų pagrindų. BDAR neišskiria, kada ir kokiu teisiniu pagrindu gali ar turi būti remiamasi tvarkant darbuotojų asmens duomenis (Grigonienė, 2020, p. 348), tai turi nuspręsti pats darbdavys (duomenų valdytojas[10]). Sutikimo pagrindas darbo teisiniuose santykiuose turi būti vertinamas itin kritiškai, kadangi jis turi atitikti tam tikras sąlygas (turi būti duotas laisva valia, konkretus, informacija pagrįstas, nedviprasmiškas valios išreiškimas) (BDAR 7 str., preamb. 32 p.). Įprastai laikoma, kad darbuotojas yra silpnesnioji darbo santykių šalis ne tik dėl to, kad jis yra ekonomiškai priklausomas nuo darbdavio pajamų, bet ir dėl to, kad yra teisiškai jam pavaldus (Zekic, 2019 cituota Mačernytė-Panomariovienė ir kt., 2023, p. 130), o darbo sutarties šalims pačioms nustatant tarpusavio teisių ir pareigų apimtį darbdavys gali daryti įtaką darbuotojo valiai, primesdamas jam nepriimtinas darbo sąlygas (Davulis, 2018, p. 44). Todėl laisvos valios elementas sutikimo ir darbo santykių kontekste tampa kontroversiškas.

Apibendrinant pasakytina, kad darbdavys būdamas atsakingas už sprendimo stebėti darbuotojus atliekamo algoritminio valdymo metu, grindžiamo dirbtinio intelekto sistemomis, teisėtumą, rinkdamas duomenis, turi nustatyti (ir esant ginčui ar kompetentingos institucijos reikalavimui – pagrįsti) darbuotojų stebėjimo tikslą (ko siekiama darbuotojų stebėjimu ir ar surinkti asmens duomenys tikrai naudojami nurodytam tikslui įgyvendinti), teisėto tvarkymo sąlygą (-as) ir įrodyti, kad toks rinkimas yra būtinas ir proporcingas.

3. Algoritminis valdymas, grįstas dirbtinio intelekto sistemomis, ir darbuotojo teisės į privatumą apsauga darbuotojų stebėjimo kontekste

DI akte konstatuojama, kad dirbtinio intelekto sistemos, naudojamos darbuotojų veiklos rezultatams ir elgesiui stebėti, gali pažeisti darbuotojų pagrindines teises į duomenų apsaugą ir privatumą (DI akto preamb. 57 p.). Daugelis autorių (Ebert et al., 2021, p. 10; Aloisi, De Stefano, 2022, p. 306) kaip vieną pagrindinių algoritminio valdymo, grįsto dirbtinio intelekto sistemomis, panaudojimo stebėjimui problemų darbuotojų atžvilgiu taip pat įvardija grėsmę jų privačiam gyvenimui. Stebėjimas naudojant dirbtinio intelekto sistemas atveria naujas galimybes darbdaviams kontroliuoti darbuotojus ir jų darbo

[10] Duomenų valdytojas šio straipsnio apimtyje ir BDAR sąvokų prasme (BDAR 4 str. 7 p.) suprantamas kaip darbdavys, kuris nustato asmens duomenų tvarkymo tikslus ir priemones.

aplinką daug intensyviau, nei kada nors iki šiol (Mole, 2022, p. 88). Algoritminis valdymas, grįstas dirbtinio intelekto sistemomis, gali veikti itin intervenciškai. Dėl dirbtinio intelekto sistemų gebėjimo su surinktais duomenimis atlikti įvairias kombinacijas didėja tikimybė sužinoti itin asmenišką informaciją apie darbuotoją, pavyzdžiui, apie nėštumo tikimybę, ketinimą stoti ar steigti profesinę sąjungą, darbo tarybą (Data and algorithms at..., 2021), darbuotojo ketinimą nutraukti darbo santykius (Ssudhan, 2023) ir pan.

Teisė į privatų gyvenimą yra pasyvioji teisė, nes asmuo savo paties elgesiu negali jos įgyvendinti, bet turi teisę reikalauti, kad kiti asmenys veiktų atitinkamu būdu (Davulis, 2018, p. 115). Darbdavio siekis stebėti darbuotojus negali būti pateisinamas vien tik darbdavio interesais, o turi būti užtikrintas darbdavio ir darbuotojo interesų pusiausvyros balansas, darbuotojo duomenų apsauga bei privatumas. Žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos 8 str. (toliau – Konvencija) užtikrina, kad kiekvienas turi teisę į tai, kad būtų gerbiamas jo privatus ir šeimos gyvenimas, būsto neliečiamybė ir susirašinėjimo slaptumas. Darbo kodeksas taip pat numato, kad darbdavys privalo gerbti darbuotojų teises į privatų gyvenimą ir į asmens duomenų apsaugą, darbdaviui įgyvendinant nuosavybės ar valdymo teises į darbo vietoje naudojamas informacines ir elektroninių ryšių technologijas, negali būti pažeidžiamas darbutojų asmeninio susižinojimo slaptumas (Darbo kodekso 27 str. 1 d., 2 d., 52 str. 6 d.). Todėl darbdaviui tenka atsakomybė nustatyti, ar jo planuojamas darbuotojų stebėjimas pasitelkiant algoritminį valdymą, grįstą dirbtinio intelekto sistemomis, yra suderinamas su imperatyvia darbuotojo teise į privatų gyvenimą.

Dėl darbuotojų stebėjimo kriterijų ir jų privatumo ribų nustatymo profesiniame kontekste yra suformuota svarbi Europos Žmogaus Teisių Teismo (toliau – EŽTT) praktika. Analizuojant darbuotojų stebėjimo algoritminiu valdymu, grįstu dirbtinio intelekto sistemomis, atvejį, reikšmingas EŽTT Didžiosios kolegijos sprendimas *Barbulescu prieš Rumuniją* byloje. Pareiškėjas naudojo paskyras „Yahoo Messenger“ ne tik darbo reikmėms, bet ir asmeniniams susirašinėjimo tikslams. Darbdavys stebėjo darbuotojo veiklą „Yahoo Messenger“ ir vėliau su pareiškėju, dėl jo asmeninių susirašinėjimų, nutraukė darbo santykius. Šioje byloje buvo pripažinta, kad darbuotojas išsaugo privatumą darbo metu ir darbdavio nurodymai negali sumažinti darbuotojo privataus socialinio gyvenimo darbo vietoje iki nulio (EŽTT Didžiosios kolegijos 2017 m. rugsėjo 5 d…, 80 p.). EŽTT Didžioji kolegija taip pat vertino, kad Konvencijos 8 straipsnis garantuoja teisę į „privatų gyvenimą“ plačiąja prasme, įskaitant teisę gyventi „privatų socialinį gyvenimą“, t. y. galimybę asmeniui plėtoti savo socialinę tapatybę (p. 70). Kitoje EŽTT byloje *Lobez Ribalda ir kt. prieš Ispaniją* buvo aiškinamasi ar vykdomas iš dalies slaptas darbuotojų vaizdo stebėjimas siekiant nustatyti atsakingus asmenis dėl atsirandančių piniginių trūkumų parduotuvėje pažeidė Konvencijos 8 str. Darbdavys ne apie visas filmuojančias vaizdo kameras informavo darbuotojus. Remiantis surinkta slapta filmuota medžiaga, pinigus iš kasos pasisavinę darbuotojai, buvo nustatyti ir su jais buvo nutrauktos darbo sutartys. Įvertinusi aplinkybių visumą EŽTT Didžioji kolegija šioje byloje nusprendė, kad Konvencijos 8 str. nebuvo pažeistas. *Barbulescu prieš Rumuniją* ir *Lobez Ribalda ir kt. prieš Ispaniją* suformavimo praktiką, kad vertinant darbuotojų stebėjimo teisėtumą turėtų būti atsižvelgta į: *pirma*, reikšminga tai, ar darbuotojui buvo pranešta, jog darbdavys gali imtis priemonių stebėti darbuotojo korespondenciją, kitą veiklą, stebėti jį vaizdo kameromis; pranešime paprastai turėtų būti aiškiai nurodytas stebėsenos pobūdis ir jis turėtų būti pateikiamas iš anksto; *antra*, svarbus darbdavio vykdomas darbuotojo stebėjimo mastas ir darbuotojo privatumo ribojimo laipsnis (reikėtų atskirti pranešimų srauto ir jų turinio stebėseną); reikėtų atsižvelgti į privatumo lygį stebimoje zonoje, taip pat į visus laiko ir erdvės apribojimus bei žmonių, kurie gali susipažinti su rezultatais, skaičių; *trečia*, darbdavys stebėjimą (ir jo mastą) turi pagrįsti teisėtomis priežastimis; kuo intensyvesnė stebėsena, tuo svaresnis bus reikalingas pagrindimas; *Lobez Ribalda ir kt. prieš Ispaniją* byloje EŽTT

Didžioji kolegija dėl slapto stebėjimo kaip reikšmingas aplinkybes vertino, kad buvo nustatytas didelis nuostolių mastas, kurį sukėlė ne pavienis darbuotojas, o suderintai veikdama jų grupė; ir priešingai, bet koks nedidelis įtarimas dėl darbuotojo elgesio ar pažeidimo negalėtų pateisinti slapto darbuotojo stebėjimo; *ketvirta*, ar įmanoma tuos pačius darbuotojo kontrolės tikslus pasiekti mažiau darbuotojo privatumą ribojančiais stebėjimo metodais ir priemonėmis; *penkta*, stebėjimo pasekmės darbuotojui ir tai, kam darbdavys naudos stebėjimo rezultatus (ar anksčiau deklaruotam tikslui pasiekti); *šešta*, ar darbuotojui buvo suteikti tam tikri saugikliai, ypač kai darbdavio taikomos stebėjimo priemonės riboja darbuotojo privatumą (darbdavys negalėtų susipažinti su faktiniu atitinkamų pranešimų turiniu, nebent darbuotojui apie tai būtų pranešta iš anksto); tokios apsaugos priemonės gali būti atitinkamų darbuotojų arba darbuotojų atstovų informavimas apie stebėsenos įdiegimą ir mastą, pareiškimas apie tokią priemonę nepriklausomai įstaigai arba galimybė pateikti skundą. (EŽTT Didžiosios kolegijos 2017 m. rugsėjo 5 d…, 121 p. *i-vi;* EŽTT Didžiosios kolegijos 2019 m. spalio 17 d…, 116 p., 124 p., 125 p., 128 p., 134 p.). Šie kriterijai atitinka ir anksčiau aptartus teisinius reikalavimus, kylančius iš BDAR, taip pat aiškiai indikuoja kokius kriterijus prieš pasitelkdamas algoritminį valdymą, grįstą dirbtinio intelekto sistemomis, darbuotojų stebėsenai darbdavys turėtų analizuoti ir nusprendus naudoti stebėsenai, taikyti praktikoje.

Florindo de Almeida Vasconcelos Gramaxo prieš Portugaliją byloje EŽTT prieštaringai pažvelgė į kai kuriuos aspektus, anksčiau suformuotus dėl darbuotojų stebėjimo. Šioje byloje į pareiškėjo darbinį automobilį buvo įdiegta geolokacijos sistema (toliau – GPS), apie kurios veikimą pareiškėjas buvo informuotas. Vėliau buvo įmontuota dar viena, tačiau slapta sistema, apie kurios buvimą pareiškėjas nežinojo. GPS veikė 24 val. ir 7 dienas per savaitę bei darbuotojas buvo stebimas trejus metus. Tai apėmė ir laiką po pareiškėjo darbo valandų. Pareiškėjas buvo atleistas dėl to, jog vadovaujantis surinktais iš kelių GPS sistemų duomenimis, buvo nustatytas tyčinis nuvažiuotų darbo metu rodmenų klastojimas, siekiant sumažinti ne darbo metu nuvažiuotų atstumų rodmenis; taip pat iš GPS duomenų buvo galima matyti, kad pareiškėjas dirbdavo mažiau nei 8 darbo valandas. EŽTT tik keturiais balsais prieš tris nusprendė, kad Konvencijos 8 str. nebuvo pažeistas. Įdomu tai, kad toks intensyvus (pavyzdžiui, byloje *Antović ir Mirković prieš Juodkalniją* buvo nuspręsta, kad apskritai darbuotojo vaizdo stebėjimas darbo vietoje, nesvarbu, ar jis slaptas, ar ne, turi būti laikomas dideliu kišimusi į darbuotojo privatų gyvenimą, o šiuo atveju, kita priemonė, t. y. GPS buvo itin intervencinė, nes rinko darbuotojo duomenis jo asmeninio gyvenimo po darbo valandų metu) ir ilgalaikis darbuotojo stebėjimas (pavyzdžiui, palyginimui, *Lobez Ribalda ir kt. prieš Ispaniją* byloje darbuotojai buvo slaptai stebimi dešimt dienų, o *Köpke prieš Vokietiją* – dvi savaites, įtariant kasininkę savinantis parduotuvės lėšas), dalį laiko vykęs net ne darbuotojo darbo metu, buvo laikomas tinkamai pasirinkta priemone, kuria darbdavys užtikrino tinkamą savo verslo funkcionavimą, atsižvelgdamas į teisėtą bendrovės interesą, t. y. užtikrindamas, kad tinkamai būtų kontroliuojamos įmonės išlaidos. Esant darbuotojo privataus gyvenimo gerbimo jo profesinėje veikloje ir darbdavio teisei užtikrinti tinkamą verslo vykdymą kolizijai, teismo dauguma nusprendė, kad pareiškėjo teisė į jo privatų gyvenimą buvo proporcingai sumažinta siekiant užtikrinti darbdavio interesą į jo verslo valdymą ir apskaitą. Vis dėlto, teismas neįvertino, kad naudotos priemonės darbuotojo stebėjimui ir jų panaudojimo būdas, mastas, intensyvumas, nebuvo tuo metu egzistavęs vienintelis tinkamas ir proporcingas pasirinkimas stebėjimo tikslui pasiekti. Kitaip tariant EŽTT *Barbulescu prieš Rumuniją* byloje suformuoto vieno iš kriterijų „ar įmanoma tuos pačius darbuotojo kontrolės tikslus pasiekti mažiau darbuotojo privatumą ribojančiais stebėjimo metodais ir priemonėmis“ neatitiko. EŽTT sprendimais *Köpke prieš Vokietiją, Lobez Ribalda ir kt. prieš Ispaniją, Florindo de Almeida Vasconcelos Gramaxo prieš Portugaliją,* aiškiai parodė, kad darbuotojai reikšmingai piktnaudžiaujantys savo teisėmis darbe negali tikėtis absoliutaus jų privataus gyvenimo gerbimo darbinėje aplinkoje.

Lietuvos Aukščiausiasis Teismas (toliau – LAT) 2024 m. spalio 8 d. nagrinėtoje byloje dėl nuotolinio darbo ir ieškovės, dirbusios nuotoliniu būdu, su kuria vėliau buvo nutraukta darbo sutartis dėl šiurkštaus darbo pareigų pažeidimo, išaiškino, kad darbdavys, turėdamas interesą kontroliuoti darbuotoją, turėtų tai daryti nepažeisdamas jo privatumo ir asmens duomenų apsaugos t.y. galėtų patikrinti, ar darbuotojas vykdo jam pavestas funkcijas, fiksuodamas darbuotojo prisijungimą prie tam tikrų sistemų, aktyvų ir pasyvų prisijungimo laiką, nustatydamas kitokias darbo valandas arba darbo funkcijų vykdymą kontroliuodamas ne pagal darbo laiko apskaitą, bet per atliktų darbų ir jų rezultatų fiksavimą (LAT 2024 m. spalio 8 d. nutartis civilinėje byloje..., 30 p.). LAT įvardija įvairias alternatyvas, kurios yra galimos ir reikalingos darbuotojo darbo kontrolei, tačiau visa tai iš darbdavio pusės turi būti atliekama nepažeidžiant darbuotojo privatumo. Be to atsakovės įmonėje, kurioje dirbo ieškovė, nebuvo reglamentuota nuotolinio darbo organizavimo tvarka, o būtent aiškios tvarkos nebuvimas ir sukūrė konfliktinę situaciją (LAT 2024 m. spalio 8 d. nutartis civilinėje byloje..., 33 p.). Atsivelgiant į tai įmonės, įstaigos, organizacijos turėtų turėti parengtus vidaus teisės aktus, kuriuose būtų detalizuojama darbuotojų stebėjimo algoritminiu valdymu, grįstu dirbtinio intelekto sistemomis, tvarka, įtraukiant ir anksčiau aptartus kriterijus, suformuotus bylose *Barbulescu prieš Rumuniją* ir *Lobez Ribalda ir kt. prieš Ispaniją.*

Apibendrinant, galima daryti išvadą, jog algoritminis valdymas, grindžiamas dirbtinio intelekto sistemomis, gali veikti ne visada nuspėjamu būdu; renkant asmens duomenis apie darbuotojus, gali padaryti itin asmens privatumą pažeidžiančių prognozių, įžvalgų. Išanalizavus EŽTT praktiką, susijusią su darbuotojų stebėjimu, galima daryti išvadą, kad darbuotojas darbo metu nepraranda teisės į privatumą, tačiau negali tikėtis absoliutaus jos gerbimo, jeigu ir pats itin pažeidžia darbdavio interesus. Darbdavys darbuotojo stebėjimą darbe atlikti gali, tačiau toks stebėjimas algoritminiu valdymu, grįstu dirbtinio intelekto sistemomis, turi atitikti EŽTT bylose *Barbulescu prieš Rumuniją* ir *Lobez Ribalda ir kt. prieš Ispaniją* suformuotus kriterijus, kurie turėtų būti perkelti į darbdavio vidaus teisės aktus.

4. Procedūriniai reikalavimai darbdavio sprendimui stebėti darbuotojus priėmimui – informavimo ir konsultavimo procedūros

Darbdavys, ketinantis naudoti darbo vietoje algoritminį valdymą, gristą dirbtinio intelekto sistemomis, visų pirma turi nustatyti, kokiai rizikos kategorijai tokios sistemos bus priskiriamos. DI aktas darbuotojų informavimo prasme numato skirtingus reikalavimus. Nedidelės rizikos dirbtinio intelekto sistemoms bus taikomi tik skaidrumo reikalavimai, t. y. darbuotojai turi būti tik informuoti, jog sąveikauja su dirbtinio intelekto sistema (pavyzdžiui, bendraujama su pokalbių robotu) (DI akto preamb. 27 p.; 50 str. 1 d.). Didelės rizikos dirbtinio intelekto sistemos atveju, DI aktas numato, kad prieš pradėdami naudoti arba prieš naudodami tokios rizikos dirbtinio intelekto sistemas darbo vietoje, diegėjai darbdaviai informuoja darbuotojų atstovus ir darbuotojus, kurie bus paveikti, kad jų atžvilgiu bus naudojamos didelės rizikos dirbtinio intelekto sistemos (DI akto 26 str. 7 d.). Informacija apie planuojamą didelės rizikos dirbtinio intelekto sistemų diegimą darbo vietoje turi būti teikiama vadovaujantis teisės aktais ir praktika dėl darbuotojų ir jų atstovų informavimo (DI akto preamb. 92, 26 str. 7 d.). Tai reikštų, kad darbdavys, prieš pradėdamas darbovietėje diegti algoritminį valdymą, grįstą didelės rizikos dirbtinio intelekto sistemomis, ir jo pagalba stebėti darbuotojus, visų pirma privalo atlikti informavimo ir (kai reikia) konsultavimo procedūras (DK 203, 204 str.). Informacijos pateikimo apimties ir turinio DI aktas nedetalizuoja, tačiau DI akte galima rasti nuorodą, kad Europos Sąjungai ar valstybėms narėms neužkertamas kelias toliau taikyti arba priimti darbuotojams palankesnius įstatymus ir kitus teisės aktus, kiek tai susiję su jų teisių apsauga, kai darbdaviai naudoja dirbtinio intelekto sistemas, arba skatinti ar

leisti taikyti darbuotojams palankesnes kolektyvines sutartis (DI aktas 2 str. 11 d.). Todėl papildomas teisinis reguliavimas gali atsirasti netolimoje perspektyvoje tiek Europos Sąjungos[11], tiek nacionaliniu mastu. Tačiau kol jo nėra, darbo teisinių santykių šalys tapusavyje bendru sutarimu sprendžia, kokia informacija reikalinga norint priimti objektyvius sprendimus dėl algoritminio valdymo grįsto didelės rizikos dirbtinio intelekto sistemomis diegimo ir naudojimo darbo aplinkoje. Vis dėlto, šia DI akto norma, buvo pasiektas esminis laimėjimas, t. y. tai, kad darbuotojai galės ir turės laiku gauti informaciją apie darbdavio ketinimą diegti algoritminį valdymą, grįstą dirbtinio intelekto sistemomis, darbovietėje ir stebėti darbuotojus, bei toks veiksmas negalės būti atliekama apie tai neinformavus.

Pareiga veikti skaidriai ir informuoti duomenų subjektą, t. y. šiuo atveju darbuotoją yra įtvirtinta ir BDAR bei ADTAĮ. Tinkamas informavimo procesas darbuotojo atžvilgiu visų pirma suprantamas kaip BDAR nustatyto skaidrumo principo užtikrinimas (Grigonienė, 2020, p. 353). Atsiradus naujoms technologijoms, skaidrumo poreikis tampa dar akivaizdesnis, nes šios technologijos suteikia galimybę slaptai rinkti ir toliau tvarkyti asmens duomenis, kurių kiekis gali būti milžiniškas ir jeigu nenustatomos duomenų tvarkymo ribos, kyla didelis pavojus, kad teisėti darbdavių interesai taps nepateisinamu, intervenciniu stebėjimu (Nuomonė Nr. 2/2017 dėl.., 2017). Darbuotojai, apie jų asmens duomenų tvarkymą (šiuo atveju stebėjimą), kai tai atliekama algoritminio valdymo, grįsto dirbtinio intelekto sistemomis, metu turi būti informuojami pasirašytinai ar kitu informavimo faktą įrodančiu būdu, nurodant stebėjimo tikslą, duomenų saugojimo laikotarpį, informuojant ar atliekamas profiliavimas, pateikiant ir kitą BDAR 13 str. 1 ir 2 dalyse įtvirtintą informaciją (ADTAĮ 5 str. 4 d.).

Apibendrinant pateiktus argumentus, darytina išvada, kad darbdaviui siekiant darbo aplinkoje įdiegti algoritminį valdymą, grįstą dirbtinio intelekto sistemomis, darbdavys prieš tokį žingsnį turės įvertinti kokiai rizikos kategorijai priklauso algoritminis valdymas, grįstas dirbtinio intelekto sistemomis. Atitinkamai pagal tai informuoja darbuotojus arba informuoja ir (kai reikia) konsultuojasi su darbuotojais ir darbuotojų atstovais. Taip pat darbdavys turi prievolę apie darbuotojų stebėjimą kiekvieną darbuotoją informuoti ir pagal ADTAĮ bei BDAR nuostatas.

Išvados

1. Algoritminis valdymas, grįstas dirbtinio intelekto sistemomis, darbdavių naudojamas planuojant, organizuojant, paskirstant darbuotojų darbus, darbuotojų darbo veiklos stebėjimui, produktyvumo vertinimui. Dėl stebėjimo metu surinktų duomenų darbdavys priima sprendimus dėl darbo santykių su darbuotojais nutraukimo, pakeitimo, darbo pareigų pažeidimo. DI aktas dirbtinio intelekto sistemas skirsto į tris rizikos kategorijas: nepriimtina rizika, kuri yra draudžiama, didelė rizika ir nedidelė rizika. DI aktas algoritminį valdymą, grįstą dirbtinio intelekto sistemomis, skirtą darbuotojų stebėjimui, klasifikuoja kaip didelės rizikos dirbtinio intelekto sistemas ir numato griežtus reikalavimus darbdaviui (pavyzdžiui, imtis tinkamų techninių ir organizacinių priemonių tam, kad dirbtinio intelekto sistemos būtų naudojamos pagal instrukcijas; užtikrinti, kad įvesties duomenys į dirbtinio intelekto sistemas būtų aktualūs, reprezentatyvūs; stebėti veikimą, informuoti apie incidentus ir kita) šių sistemų naudojimui. Algoritminiu valdymu, grįstu dirbtinio intelekto sistemomis, darbdaviui galima naudotis tik laikantis minėtų griežtų reikalavimų ir atliekant žmogaus vykdomą

[11] Europos profesinių sąjungų konfederacija „ETUC“, Europos profesinė sąjunga „Industriall Europ“ ragina priimti direktyvą dėl algoritminių sistemų darbe, motyvuojant tuo, kad dirbtinio intelekto sistemos vis plačiau naudojamos darbo vietoje (darbo teisiniuose santykiuose). Pasiūlymuose detalizuojama, kokia informacija turėtų būti teikiama darbuotojų atstovams ir darbuotojams, numatomi pagrindiniai dirbtinio intelekto sistemų naudojimo darbo vietoje principai ir kt. (ETUC Resolution calling for an..., 2022; AI at the workplace: Collective…, 2023).

priežiūrą, t. y. darbe paskirti kompetentintą asmenį, turintį kvalifikaciją ir įgaliojimus užtikrinti žmogaus priežiūrą, kuris stebėtų algoritminio valdymo, grįsto dirbtinio intelekto sistemomis, veikimą, turėtų žinių kaip elgtis su dirbtinio intelekto sistema, gebėtų interpretuoti generuojamus išvedinius (išvadas, rekomendacijas, predikcijas, turinį), gebėtų atitinkamai elgtis su gautais rezultatais (sustabdyti, pakeisti, ištaisyti), taip pat tam tikrais atvejais nuspręstų nenaudoti algoritminio valdymo ar jo metu suskurto rezultato.

2. Darbdaviui, siekiančiam stebėti darbuotojus panaudojant algoritminį valdymą, grįstą dirbtinio intelekto sistemomis, ir tvarkant darbuotojų asmens duomenis, atsiranda prievolė atsižvelgti į teisinius reikalavimus, kylančius iš BDAR: 1) darbdavys nustato aiškų, konkretų, teisėtą darbuotojų stebėjimo tikslą; 2) darbdavys, prieš siekdamas naudoti algoritminį valdymą, grįstą dirbtinio intelekto sistemomis, sprendžia ar nustatytam tikslui pasiekti pasirenkama priemonė yra būtina ir proporcinga, t. y. ar algoritminis valdymas, pagrįstas dirbtinio intelekto sistemomis yra būtinas tikslui pasiekti, ar norimo tikslo negalima pasiekti kitomis, mažiau darbuotojų privatumą ribojančiomis priemonėmis, ar galimas darbuotojo privatumo ribojimas atsvers siekiamą naudą; 3) darbuotojų stebėjimas turi būti pagrįstas bent viena teisėto tvarkymo sąlyga, o jeigu tokios sąlygos nėra, stebėti darbuotojus draudžiama.
3. Algoritminio valdymo, grįsto dirbtinio intelekto sistemomis, naudojimas gali pasireikšti kaip intervencinė ir skvarbi stebėjimo priemonė, naudojama darbuotojų atžvilgiu, ir atskleisti jautrią bei privačią informaciją apie juos (dėl gebėjimo su surinktais duomenimis atlikti įvairias kombinacijas gali prognozuoti darbuotojų darbo santykių pasibaigimą, ketinimą stoti į darbo tarybą, nėštumo tikimybę ir pan.). Todėl darbdaviui sprendžiant algoritminio valdymo, grįsto dirbtinio intelekto sistemomis, panaudojimo darbuotojų stebėjimui ir jų teisės į privatumą ribų išsaugojimo klausimui, reikia atsižvelgti į suformuotą su darbuotojų stebėjimu susijusią EŽTT praktiką ir bylose *Barbulescu prieš Rumuniją, Lobez Ribalda ir kt. prieš Ispaniją* suformuotus kriterijus. Darbavys siekdamas nepažeisti darbuotojo teisės į privatumą algoritminio valdymo, grįsto dirbtinio intelekto sistemomis, panaudojimo kontekste turi: informuoti darbuotoją apie atliekamą stebėjimą; nustatyti tinkamą darbuotojo stebėjimo mastą; nustatyti teisėtas stebėjimo priežastis; pagrįsti algoritminio valdymo, veikiančio dirbtinio intelekto sistemų pagrindu, naudojimą darbuotojų stebėjimui kaip vienintelės tam atvejui tinkamos priemonės; detalizuoti darbuotojų stebėjimo pasėkmes ir kam bus naudojami stebėjimo rezultatai; kokios apsaugos priemonės taikomos darbuotojams dėl atliekamo jų stebėjimo algoritminiu valdymu, grįstu dirbtinio intelekto sistemoms. Tokius kriterijus darbdavys turėtų įtvirtinti ir išsamiau detalizuoti darbovietės vidiniuose teisės aktuose. Iš EŽTT bylų analizės, susijusios su darbuotojų stebėjimu, taip pat galima daryti išvadą, kad darbuotojas darbe taip pat turi laikytis bendrosios tvarkos, o atlikdamas teisei priešingas veikas (pavyzdžiui, neteisėtai savindamasis darbdavio turtą) negali tikėtis, jog jo teisė į privatumą išliks absoliuti.
4. DI aktas, ADTAĮ ir BDAR numato pareigą informuoti darbuotojus, kai yra atliekamas jų stebėjimas algoritminiu valdymu, grįstu dirbtinio intelekto sistemomis. Algoritminiam valdymui, grindžiamam nedidelės rizikos dirbtinio intelekto sistemomis, taikomi tik skaidrumo reikalavimai, t. y. darbdavys informuoja darbuotojus, jog šie sąveikauja su dirbtinio intelekto sistema ir pateikia detalesnę informaciją, susijusią su jų renkamais asmens duomenimis, vykdomo stebėjimo metu. Informavimo ir (kai reikia) konsultavimo prievolė darbdaviui atsiranda, kai šis darbovietėje planuoja diegti ir naudoti algoritminį valdymą, grįstą didelės rizikos dirbtinio intelekto sistemomis. Apie algoritminio valdymo, grįsto didelės rizikos dirbtinio intelekto sistemomis, diegimą ir naudojimą darbovietėje turi būti pranešama darbuotojams ir darbuotojų atstovams iki algoritminio valdymo, grįsto didelės rizikos dirbtinio intelekto sistemomis, naudojimo darbuotojų stebėjimui pradžios.

Literatūra

Teisės norminiai aktai

Europos Sąjungos teisės aktai

Žmogaus teisių ir pagrindinių laisvių apsaugos konvencija (1950). *Valstybės žinios,*1995 , Nr. 40-987. TAR, 2022, nr. 2432.

Europos Parlamento ir Tarybos 2016 m. balandžio 27 d. 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). *OL* L 119, 2016 5 4, p. 1.

2024 m. birželio 13 d. Europos Parlamento ir Tarybos reglamentas (ES) 2024/1689 kuriuo nustatomos suderintos dirbtinio intelekto taisyklės ir iš dalies keičiami reglamentai (EB) Nr. 300/2008, (ES) Nr. 167/2013, (ES) Nr. 168/2013, (ES) 2018/858, (ES) 2018/1139 ir (ES) 2019/2144 ir direktyvos 2014/90/ES, (ES) 2016/797 ir (ES) 2020/1828 (Dirbtinio intelekto aktas). *OL* L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj

Nacionaliniai teisės aktai

Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas (1996). *Valstybės žinios*, 1996, Nr. 63-1479.

Lietuvos Respublikos darbo kodekso patvirtinimo, įsigaliojimo ir įgyvendinimo įstatymas (2016). TAR, 23709.

Specialioji literatūra

Adams-Prassl, J. (2022). Regulating Algorithms at Work: Lessons for a "European Approach to Artificial Intelligence". *European Labour Law Journal,* 13 (1), p. 30–50, https://doi.org/10.1177/20319525211062558.

Aloisi, A., De Stefano, V. (2022). Essential jobs, remote work and digital surveillance: Addressing the COVID-19 pandemic panopticon. *International Labour Review*, 161, p. 289–314, https://doi.org/10.1111/ilr.12219.

Bagdanskis, T.; Sartatavičius, P. (2012). Workplace privacy: different views and arising issues. *Jurisprudencija,* 19 (2), p. 697–713.

Biega, A. J., Finck, M. (2021). Reviving Purpose Limitation and Data Minimisation in Data – Driven Systems. *Technology and Regulation*, 2021, p. 44–61, https://doi.org/10.26116/techreg.2021.004.

Cefaliello, A., Kullmann, M. (2022). Offering false security: How the draft artificial intelligence act undermines fundamental workers rights. *European Labour Law Journal*, 13 (4), p. 542–562, https://doi.org/10.1177/20319525221114474.

Davulis, T. (2018). *Lietuvos Respublikos darbo kodekso komentaras.* Vilnius: Registrų centras.

De Stefano, V. (2019). "Negotiating the algorithm": Automation, Artificial intelligence and Labour protection. *Comparative Labour Law & Policy Journal*, 41 (1), 1–31 [interaktyvus]. Prieiga per internetą: https://ssrn.com/abstract=3403837 [žiūrėta 2023 m. balandžio 2 d.].

Ebert, I., Wildhaber, I. and Adams-Prassl, J. (2021). Big Data in the workplace: Privacy Due Diligence as a human rights – based approach to employee privacy protection. *Big Data & Society*, January–June, p. 1–14, https://doi.org/10.1177/2053951721101.

Fernadez-Macias, E.; Urzi Brancati, C.; Wright, S.; Pesole, A. *The platformisation of work. Evidence from the JRC Algorithmic Management and Platform Work survey (AMPWork),* Publications Office of the European Union, Luxembourg, 2023, https://doi:10.2760/801282, JRC133016.

Europos Sąjungos pagrindinių teisių agentūra ir Europos Taryba. (2021). *Europos duomenų apsaugos teisės vadovas: 2018 m. redakcija.* Liuksemburgas: Europos Sąjungos leidinių biuras.

George, G., Thomas, M. R. (2019). Integration of Artificial Intelligence in Human Resource. *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, 9(2), p. 5069–5073, https://doi. 10.35940/ijitee.L3364.129219.

Grigonienė, R. (2020). Darbuotojų asmens duomenų apsaugos užtikrinimo teisinio reguliavimo ypatumai. *Jurisprudencija*, 27 (2), p. 346–369, DOI: 10.13165/JUR-20-27-2-06.

Jarrahi, M. H. *et al*. (2021). Algorithmic management in a work context. *Big Data & Society*, July–December, p. 1–14, https://doi: 10.1177/20539517211020332.

Mačernytė-Panomariovienė, I. *et al*. (2023). *Besikeičiantys darbo santykiai ir jų reguliavimas Lietuvoje*. Vilnius: Mykolo Romerio universitetas.

Mole, M. (2022). The Internet of Things and Artificial Intelligence as Workplace Supervisors: Explaining and Understanding the New Surveillance to Employees Beyond Art. 8 ECHR. Italian *Labour Law e-Journal,* Issue 2, Vol. 15, https://doi.org/10.6092/issn.1561-8048/15598.

Newlands, G. (2021). Algorithmic Surveillance in the Gig Economy: The Organization of Work through Lefebvrian Conceived Space. *Organization Studies,* 42(5), p. 719–737, https://doi.org/10.1177/0170840620937900.

Štareikė, E. (2021). Assurance of the right to privacy and the protection of personal data in Labour relations. *Public security and public order*, 26, p. 221–235.

Tamašauskaitė-Janickė, G. (2016). *Informacinių ir komunikacinių technologijų panaudojimas darbo vietoje darbo teisės požiūriu.* Daktaro disertacija, socialiniai mokslai, teisė (01S), Vilniaus universitetas. Vilnius: Vilniaus universiteto leidykla.

Todoli-Signes, A. (2021). Making Algorithms Safe for Workers: Occupational Risks Associated With Work Managed by Artificial Intelligence. *Transfer: European Review of Labour and Research*, p. 1–20, https://doi.org/10.1177/10242589211035040.

Zaleskis, J. (2019). *Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė.* Vilnius: VĮ Registrų centras.

Teismų praktika

Europos Žmogaus Teisių Teismo sprendimai

Köpke prieš Vokietiją [EŽTT], Nr. 420/07, [2010-10-05]. ECLI:CE:ECHR:2010:1005DEC000042007

Barbulescu prieš Rumuniją [EŽTT], Nr. 61496/08, [2017-09-05]. ECLI:CE:ECHR:2017:0905JUD006149608

Antović ir Mirković prieš Juodkalniją [EŽTT], Nr. 70838/13, [2017-11-28]. ECLI:CE:ECHR:2017:1128 JUD007083813

López Ribalda ir kt. prieš Ispaniją [EŽTT], Nr. 1874/13 ir 8567/13, [2019-10-17]. ECLI:CE:ECHR:2019:1017J UD000187413

Florindo de Almeida Vasconcelos Gramaxo prieš Portugaliją [EŽTT], Nr. 26968/16, [2022-12-13]. ECLI:CE:E CHR:2022:1213JUD002696816

Lietuvos Aukščiausiojo Teismo praktika

Lietuvos Aukščiausiojo Teismo 2024 m. spalio 8 d. nutartis civilinėje byloje Nr. e3K-3-176-684/2024

Kiti šaltiniai

Bernhardt, A. *et al*. (2021). Data and algorithms at work: The case for worker technology rights. [interaktyvus]. Prieiga per internetą: https://escholarship.org/uc/item/9831k83p [žiūrėta 2023 m. balandžio 9 d.].

European Commission – International Labour Organization joint project "Building Partnerships on the Future of Work". The Algorithmic Management of work and its implications in different contexts. 2022 (9) [interaktyvus]. Prieiga per internetą: https: https://www.ilo.org/wcmsp5/groups/public/---ed_emp/documents/publication/wcms_849220.pdf [žiūrėta 2023 m. spalio 27 d.].

European Commission – International Labour Organization joint project "Building Partnerships on the Future of Work". Technical workshop on "Practices towards algorithmic management and their impact on workers". 2021 [interaktyvus]. Prieiga per internetą: https://www.ilo.org/wcmsp5/groups/public/--ed_emp/documents/meetingdocument/wcms_810116.pdf [žiūrėta 2023 m. spalio 27 d.].

Europos Komisija. Baltoji knyga. Dirbtinis intelektas. Europos požiūris į kompetenciją ir pasitikėjimą. COM (2020) 65.

ES 29 str. duomenų apsaugos darbo grupė. *Nuomonė Nr. 3/2012 dėl biometrinių technologijų pokyčių, Nr. WP 193.* Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_lt.pdf [žiūrėta 2023 m. kovo 22 d.].

ES 29 str. duomenų apsaugos darbo grupė. *Nuomonė Nr. 3/2013 dėl tikslo ribojimo, Nr. WP 203.* Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf [žiūrėta 2023 m. kovo 24 d.].

ES 29 str. duomenų apsaugos darbo grupė. *Nuomonė Nr. 2/2017 dėl duomenų tvarkymo darbe, Nr. WP 249.* Prieiga per internetą: https:// ec.europa.eu/newsroom/article29/items/610169 [žiūrėta 2023 m. kovo 28 d.].

European Trade Union Confederation (2022). ETUC Resolution calling for an EU Directive on Algorithmic Systems at Work [interaktyvus]. Prieiga per internetą: https://www.etuc.org/en/document/etuc-resolution-calling-eu-directive-algorithmic-systems-work [žiūrėta 2024 m. spalio 27 d.].

IndustriAll European Trade Union (2023). AI at the workplace: Collective bargaining needed to ensure worker involvement [interaktyvus]. Prieiga per internetą: https://news.industriall-europe.eu/Article/924 [žiūrėta 2024 m. spalio 27 d.].

Lexology. *Employee Evaluation System may Violate GDPR.* [interaktyvus] (modifikuota 2020-07-14). Prieiga per internetą: https://www.lexology.com/library/detail.aspx?g=d5ed6780-77d5-452f-a4f0-fbec9cb01173 [žiūrėta 2023 m. spalio 2 d.].

Mateescu, A.; Nguyen, A. (2019). Explainer: Algorithmic Management in the Workplace. *Data&Society* [interaktyvus]. Prieiga per internetą: https://datasociety.net/wp-content/uploads/2019/02/DS_Algorithmic_Management_Explainer.pdf [žiūrėta 2023 m. spalio 27 d.].

Ssudhan, V. (2023). Can AI predict if you're going to quit your Job? Trymintly blog, [blog] 19 March. Prieiga per internetą: https://www.trymintly.com/blog/can-ai-algorithms-predict-if-youre-going-to-quit-your-job/ [žiūrėta 2023 m. kovo 28 d.].

Ineta Breskienė yra Vilniaus universiteto Teisės fakulteto Privatinės teisės katedros doktorantė. Rengiamos disertacijos tema: „Dirbtinio intelekto panaudojimo teisiniai aspektai". Pagrindinės mokslinių interesų sritys – technologijų teisė, darbo teisė.

Ineta Breskienė is a doctoral student at the Department of Private Law, Faculty of Law, Vilnius University. The title of her dissertation is: *Legal Aspects of the Use of Artificial Intelligence*. The main areas of the author's scientific interest are technology law and labour law.