29 STRAIPSNIO DUOMENŲ APSAUGOS DARBO GRUPĖ

17/LT

WP 249

Nuomonė 2/2017 dėl duomenų tvarkymo darbe

Priimta 2017 m. birželio 8 d.

Ši darbo grupė sudaryta pagal Direktyvos 95/46/EB 29 straipsnį. Ji yra nepriklausomas Europos patariamasis organas duomenų apsaugos ir privatumo klausimais. Jos uždaviniai aprašyti Direktyvos 95/46/EB 30 straipsnyje ir Direktyvos 2002/58/EB 15 straipsnyje.

Sekretoriato paslaugas teikia Europos Komisijos Teisingumo ir vartotojų reikalų generalinio direktorato C direktoratas (Pagrindinės teisės ir teisinė valstybė), B-1049 Brussels, Belgium. Kabinetas MO59 05/35.

Interneto svetainė: http://ec.europa.eu/justice/data-protection/index_en.htm

Turinys

1. Santrauka

Šia nuomone papildomi ankstesni 29 straipsnio darbo grupės (toliau – WP29) leidiniai *Nuomonė 8/2001 dėl asmens duomenų tvarkymo su darbo santykiais susijusiame kontekste* (WP48)[1] ir 2002 m. *Darbinis dokumentas dėl elektroninių ryšių stebėjimo darbo vietoje* (WP55)[2]. Nuo šių dokumentų paskelbimo pradėta naudotis įvairiomis naujomis technologijomis, kuriomis sudaromos sąlygos sistemingiau tvarkyti darbuotojų asmens duomenis darbe, ir dėl to kyla nemažų privatumo ir duomenų apsaugos problemų.

Šia nuomone iš naujo įvertinama darbdavių teisėtų interesų ir darbuotojų pagrįstų privatumo lūkesčių pusiausvyra – bendrai apibūdinami naujų technologijų keliami pavojai ir atliekamas įvairių scenarijų, kuriems įvykus šios technologijos gali būti panaudotos, proporcingumo vertinimas.

Nors šioje nuomonėje daugiausia aptariama Duomenų apsaugos direktyva, joje taip pat paminimi papildomi įpareigojimai, darbdaviams nustatyti Bendruoju duomenų apsaugos reglamentu. Šioje nuomonėje dar kartą pakartojama Nuomonėje 8/2001 ir WP55 darbiniame dokumente išdėstyta pozicija ir išvados, t. y. kad tvarkant darbuotojų asmens duomenis:

- darbdaviai, neatsižvelgdami į naudojamą technologiją, visada turėtų nepamiršti fundamentalių duomenų apsaugos principų;
- iš verslo subjekto patalpų užmezgamų elektroninių ryšių turiniui taikomos tokios pačios pagrindinių teisių apsaugos nuostatos kaip ir analoginiams ryšiams;
- labai mažai tikėtina, kad sutikimas bus teisinis duomenų tvarkymo darbe pagrindas, nebent darbuotojai gali atsisakyti duoti sutikimą nepatirdami neigiamų padarinių;
- kartais galima remtis sutarties vykdymu ir teisėtais interesais, jeigu duomenų tvarkymas būtinai reikalingas teisėtu tikslu ir atitinka proporcingumo ir subsidiarumo principus;
- darbuotojai turėtų gauti aktualią informaciją apie vykdomą stebėseną; ir
- tarptautiniu mastu darbuotojų duomenys turėtų būti perduodami tik tuo atveju, jei užtikrinama pakankamo lygio apsauga.

2. Įvadas

Darbo vietoje sparčiai diegiant naujas informacines technologijas – infrastruktūrą, programas, išmaniuosius įrenginius – sudaromos sąlygos naujais būdais sistemingai ir galbūt intervencinėmis priemonėmis tvarkyti duomenis darbe. Pavyzdžiai:

- technologijas, kuriomis sudaromos sąlygos tvarkyti duomenis darbe, dabar galima įdiegti kelis kartus mažesnėmis sąnaudomis negu prieš keletą metų, o asmens duomenų tvarkymo naudojantis šiomis technologijomis pajėgumai išaugo geometrine progresija;

[1] WP29, *Nuomonė 08/2001 dėl asmens duomenų tvarkymo su darbo santykiais susijusiame kontekste*, WP48, 2001 m. rugsėjo 13 d., url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf.

[2] WP29, *Darbinis dokumentas dėl elektroninių ryšių stebėjimo darbo vietoje*, WP55, 2002 m. gegužės 29 d., url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2002/wp55_en.pdf.

- naujos duomenų tvarkymo formos, pvz., susijusios su asmens duomenimis apie naudojimąsi internetinėmis paslaugomis ir (arba) su išmaniojo įrenginio perduodamais vietos duomenimis, darbuotojams yra daug mažiau pastebimos negu kitos labiau tradicinės formos, pvz., atviros apsauginių vaizdo stebėjimo sistemų (AVSS) kameros. Todėl kyla klausimų, kiek darbuotojams šios technologijos yra žinomos, nes darbdaviai gali neteisėtai įdiegti šias duomenų tvarkymo priemones apie tai iš anksto nepranešdami darbuotojams; ir
- vis labiau nyksta asmeninio ir profesinio gyvenimo ribos. Pavyzdžiui, kai darbuotojai dirba nuotoliniu būdu (pvz., iš namų) arba kai jie keliauja verslo reikalais, gali būti stebima ne fizinėje darbo aplinkoje vykdoma veikla ir tai gali būti asmens stebėjimas privačiomis aplinkybėmis.

Todėl, nors naudojantis tokiomis technologijomis galima lengviau aptikti įmonės intelektinės ir materialinės nuosavybės praradimo atvejus ir jiems užkirsti kelią, pagerinti darbuotojų produktyvumą ir apsaugoti asmens duomenis, už kuriuos yra atsakingas duomenų valdytojas, dėl šių technologijų taip pat kyla nemažų privatumo ir duomenų apsaugos problemų. Todėl reikia iš naujo įvertinti darbdavio teisėto intereso apsaugoti savo verslą ir duomenų subjektų – darbuotojų – pagrįstų privatumo lūkesčių pusiausvyrą.

Nors šioje nuomonėje daugiausia dėmesio skiriama naujoms informacinėms technologijoms – vertinami devyni skirtingi jų panaudojimo scenarijai, tačiau joje taip pat trumpai apsvarstomi labiau tradiciniai duomenų tvarkymo darbe metodai, kai dėl technologinių pokyčių padaugėja pavojų.

Kai šioje nuomonėje vartojamas žodis *darbuotojas*, WP29 neketina jo reikšmės susiaurinti iki asmenų, turinčių pagal taikytinus darbo teisės aktus pripažįstamą darbo sutartį. Pastaraisiais dešimtmečiais tapo labiau įprasti nauji verslo modeliai, kuriems būdingi įvairių rūšių darbo santykiai, ypač laisvai samdomų asmenų atliekamas darbas. Šioje nuomonėje ketinama apžvelgti visus atvejus, kai esama darbo santykių, nesvarbu, ar šie santykiai grindžiami darbo sutartimi, ar ne.

Svarbu nurodyti, kad darbuotojai retai turi galimybę savanoriškai duoti, atsisakyti duoti ar atšaukti sutikimą, nes darbdavio ir darbuotojo santykiai lemia priklausomybę. Išskyrus išimtinius atvejus, darbdaviai turės remtis kitu negu sutikimas teisiniu pagrindu – pvz., būtinumu tvarkyti duomenis siekiant savo teisėto intereso. Vis dėlto vien teisėto intereso nepakanka, kad duomenų tvarkymas taptų svarbesnis už darbuotojų teises ir laisves.

Nepaisant tokio duomenų tvarkymo teisinio pagrindo, prieš imantis tvarkyti duomenis turėtų būti atliktas proporcingumo patikrinimas siekiant apsvarstyti, ar duomenų tvarkymas reikalingas teisėtam tikslui pasiekti, taip pat priemones, kurių reikia imtis, kad būtų kuo mažiau pažeidžiamos teisės į privatų gyvenimą ir ryšių slaptumą. Tai gali būti poveikio duomenų apsaugai vertinimo dalis.

3. Teisinė sistema

Nors toliau pateikiama analizė atlikta pagal dabartinę teisinę sistemą, nustatytą Direktyva 95/46/EB (Duomenų apsaugos direktyva)[3], tačiau šioje nuomonėje taip pat nagrinėjami įpareigojimai pagal Reglamentą 2016/679 (Bendrąjį duomenų apsaugos reglamentą)[4], kuris jau įsigaliojo ir kurį bus pradėta taikyti 2018 m. gegužės 25 d.

Siūlomo E. privatumo reglamento[5] klausimu darbo grupė ragina ES teisės aktų leidėjus sukurti konkrečią išimtį dėl darbuotojams išduodamų įrenginių duomenų perdavimo trikdymo[6]. Siūlomame reglamente nenustatyta tinkama bendro draudimo trikdyti duomenų perdavimą išimtis, o darbdaviai paprastai negali pateikti galiojančio sutikimo tvarkyti savo darbuotojų asmens duomenis.

3.1. Direktyva 95/46/EB – Duomenų apsaugos direktyva

Nuomonėje 08/2001 WP29 anksčiau bendrai išdėstė, kad darbdaviai, tvarkydami asmens duomenis su darbo santykiais susijusiame kontekste, atsižvelgia į Duomenų apsaugos direktyvoje nustatytus pagrindinius duomenų apsaugos principus. Naujų technologijų ir naujų duomenų tvarkymo metodų plėtra minėtomis aplinkybėmis šios padėties nepakeitė – faktiškai galima sakyti, kad esant tokioms tendencijoms darbdaviams tapo *dar svarbiau* tai daryti. Šiomis aplinkybėmis darbdaviai turėtų:

- užtikrinti, kad duomenys būtų tvarkomi nurodytais teisėtais tikslais, kurie būtų proporcingi ir reikalingi;
- atsižvelgti į tikslo apribojimo principą, kartu užtikrinant, kad duomenys būtų tinkami, aktualūs ir proporcingi teisėtam tikslui pasiekti;
- nepaisant taikytino teisinio pagrindo, taikyti proporcingumo ir subsidiarumo principus;
- skaidriai informuoti darbuotojus apie stebėjimo technologijų naudojimą ir tikslus;
- sudaryti duomenų subjektams sąlygas naudotis savo teisėmis, įskaitant teises susipažinti su asmens duomenimis ir prireikus juos ištaisyti, ištrinti arba blokuoti;
- laikyti duomenis tikslius ir nelaikyti jų ilgiau negu reikalinga; ir
- imtis visų reikiamų priemonių, kad duomenys būtų apsaugoti nuo neteisėtos prieigos, ir užtikrinti, kad darbuotojai pakankamai gerai žinotų apie duomenų apsaugos prievoles.

Nekartodama anksčiau pateiktų rekomendacijų, WP29 nori pabrėžti tris principus: teisinius pagrindus, skaidrumą ir automatinius sprendimus.

3.1.1. *TEISINIAI PAGRINDAI (7 STRAIPSNIS)*

[3] 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, *OL L 281, 1995 11 23, p. 31–50*, url: http://eur-lex.europa.eu/legal-content/LT/TXT/?uri=celex:31995L0046.

[4] 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas), *OL L 119, 2016 5 4, p. 1–88*, url: http://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A32016R0679.

[5] Pasiūlymas dėl Europos Parlamento ir Tarybos reglamento dėl teisės į privatų gyvenimą ir asmens duomenų apsaugos elektroninių ryšių sektoriuje, kuriuo panaikinama Direktyva 2002/58/EB, 2017/0003 (COD), url: http://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:52017PC0010&from=LT.

[6] Žr. WP29 *Nuomonę 01/2017 dėl pasiūlymo dėl E. privatumo reglamento*, WP247, 2017 m. balandžio 4 d., p. 29; url: http://ec.europa.eu/newsroom/document.cfm?doc_id=44103.

Tvarkant asmens duomenis darbo santykių kontekste turi būti įvykdytas bent vienas iš 7 straipsnyje išdėstytų kriterijų. Jeigu tvarkomi ypatingų kategorijų asmens duomenys (kaip išsamiau išdėstyta 8 straipsnyje), juos tvarkyti draudžiama, nebent taikoma išimtis[7,8]. Net jeigu darbdavys gali remtis viena iš tų išimčių, tam, kad duomenų tvarkymas būtų teisėtas, vis tiek turi būti taikomas 7 straipsnyje nurodytas teisinis pagrindas.

Dėl to apibendrinant pasakytina, kad darbdaviai turi atsižvelgti į šiuos dalykus:

- dėl darbdavio ir darbuotojo santykių pobūdžio daugumos tokio duomenų tvarkymo darbe atvejų **teisinis pagrindas negali būti ir neturėtų būti darbuotojų sutikimas** (7 straipsnio a punktas);
- duomenų tvarkymas gali būti reikalingas **sutarčiai vykdyti** (7 straipsnio b punktas) tais atvejais, kai darbdavys turi tvarkyti darbuotojo asmens duomenis, kad įvykdytų tokias prievoles;
- dažnai **darbo teisės aktuose gali būti nustatytos teisinės prievolės** (7 straipsnio c punktas)**, kurioms įvykdyti reikia tvarkyti asmens duomenis**; tokiais atvejais darbuotojas turi būti aiškiai ir visapusiškai informuojamas apie tokį duomenų tvarkymą (išskyrus atvejus, kai taikoma išimtis);
- jeigu darbdavys nuspręstų remtis **teisėtais interesais** (7 straipsnio f punktas), duomenų tvarkymo tikslas turi būti teisėtas; pasirinktas metodas ar konkreti technologija turi būti reikalingi, proporcingi ir įgyvendinami kuo mažiau trikdant duomenų perdavimą, o darbdaviui turi būti sudarytos sąlygos įrodyti, kad **imtasi tinkamų priemonių** pusiausvyrai su darbuotojų pagrindinėmis teisėmis ir laisvėmis užtikrinti[9];
- duomenų tvarkymo operacijos taip pat turi atitikti **skaidrumo reikalavimus** (10 ir 11 straipsniai), o darbuotojai turėtų būti aiškiai ir visapusiškai informuojami apie jų asmens duomenų tvarkymą[10], įskaitant tai, ar taikoma kokia nors stebėsena, ar ne; ir
- siekiant užtikrinti tvarkymo saugumą (17 straipsnis), turėtų būti įgyvendintos **tinkamos techninės ir organizacinės priemonės**.

Aktualiausi 7 straipsnio kriterijai išsamiau išdėstomi toliau.

- **Sutikimas (7 straipsnio a punktas)**

Duomenų apsaugos direktyvoje sutikimas apibrėžiamas kaip savanoriškai ir žinomai duotas konkretus duomenų subjekto pageidavimų pareiškimas, kuriuo duomenų subjektas nurodo savo sutikimą, kad būtų tvarkomi su juo susiję asmens duomenys. Kad sutikimas galiotų, jį turi būti galima atšaukti.

---

[7] Kaip nurodyta Nuomonės 08/2001 8 dalyje, pavyzdžiui, 8 straipsnio 2 dalies b punkte numatyta išimtis, kai duomenis tvarkyti būtina, norint įgyvendinti duomenų valdytojo prievoles ir specifines teises darbo įstatymų srityje, kiek tai leidžiama pagal nacionalinės teisės aktus, kuriuose nustatytos atitinkamos apsaugos priemonės.

[8] Pažymėtina, kad kai kuriose šalyse taikomos specialios priemonės, kurių darbdaviai turi laikytis darbuotojų privačiam gyvenimui apsaugoti. Viena iš šalių, kuriose taikomos tokios specialios priemonės, yra Portugalija, panašios priemonės gali būti taikomos ir kai kuriose kitose valstybėse narėse. Taigi, dėl šių priežasčių Portugalijos atžvilgiu negalioja šios nuomonės 5.6 skirsnyje padarytos išvados ir 5.1 bei 5.7.1 skirsniuose pateikti pavyzdžiai.

[9] WP29, *Nuomonė 06/2014 dėl duomenų valdytojo teisėtų interesų sampratos pagal Direktyvos 95/46/EB 7 straipsnį*, WP217, priimta 2014 m. balandžio 9 d., url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_lt.pdf.

[10] Pagal Duomenų apsaugos direktyvos 11 straipsnio 2 dalį duomenų valdytojui netaikoma prievolė pateikti informaciją duomenų subjektui, jeigu reikalavimas įrašyti arba rinkti duomenis yra konkrečiai nustatytas teisės aktais.

Anksčiau WP29 Nuomonėje 8/2001 bendrai išdėstyta, kad, jeigu darbdavys turi tvarkyti savo darbuotojų asmens duomenis, klaidinga pradėti tai daryti remiantis prielaida, kad duomenų tvarkymą galima įteisinti gavus darbuotojų sutikimą. Tais atvejais, kai darbdavys teigia, kad jam reikia sutikimo, ir yra realus arba galintis realiu tapti išankstinis nusistatymas, kylantis dėl to, kad darbuotojas nesutinka (darbo santykių kontekste tai gali būti labai tikėtina, ypač jeigu tai susiję su darbdavio atliekamu nuolatiniu darbuotojo elgsenos sekimu), tada sutikimas negalioja, nes jis nėra ir negali būti savanoriškai duotas. Taigi, daugeliu darbuotojų duomenų tvarkymo atvejų teisinis pagrindas negali būti ir neturėtų būti darbuotojų sutikimas, todėl reikalingas kitoks teisinis pagrindas.

Be to, net ir tais atvejais, kai sutikimą būtų galima laikyti teisėtu tokio duomenų tvarkymo teisiniu pagrindu (t. y. jeigu neabejotinai galima daryti išvadą, kad sutikimas yra savanoriškai duotas), tai turi būti konkretus, informacija pagrįstas darbuotojo pageidavimų pareiškimas. Gamykliniai parametrai įrenginiuose ir (arba) programinės įrangos, padedančios elektroniniu būdu tvarkyti asmens duomenis, įdiegimas negali būti laikomi darbuotojų duotu sutikimu, nes sutikimas turi būti aktyvus valios išreiškimas. Veiksmų nebuvimas (t. y. gamyklinių parametrų nepakeitimas) paprastai negali būti laikomas konkrečiu sutikimu leisti taip tvarkyti duomenis[11].

- **Sutarties vykdymas (7 straipsnio b punktas)**

Darbo santykiai dažnai grindžiami darbdavio ir darbuotojo darbo sutartimi. Siekdamas įvykdyti tokios sutarties prievoles, pvz., sumokėti darbuotojui, darbdavys privalo tvarkyti kai kuriuos asmens duomenis.

- **Teisinės prievolės (7 straipsnio c punktas)**

Darbo teisės aktuose gana dažnai darbdaviui nustatomos teisinės prievolės, kurioms įvykdyti reikia tvarkyti asmens duomenis (pvz., mokesčių apskaičiavimo ir darbo užmokesčio administravimo tikslu). Aišku, kad tokiais atvejais minėtasis teisės aktas laikytinas duomenų tvarkymo teisiniu pagrindu.

- **Teisėti interesai (7 straipsnio f punktas)**

Jeigu darbdavys pageidauja remtis Duomenų apsaugos direktyvos 7 straipsnio f punkte nurodytu teisiniu pagrindu, duomenų tvarkymo tikslas turi būti teisėtas, o pasirinktas būsimo duomenų tvarkymo metodas ar konkreti technologija turi būti reikalingi darbdavio teisėtiems interesams pasiekti. Duomenų tvarkymas taip pat turi būti proporcingas verslo poreikiams, t. y. tikslui, kurio juo siekiama. Duomenų tvarkymas darbe turėtų būti kuo mažiau intervencinis ir turėtų būti nukreiptas į konkrečią pavojaus sritį. Be to, jeigu remiamasi 7 straipsnio f punktu, darbuotojas išlaiko teisę prieštarauti dėl duomenų tvarkymo 14 straipsnyje nurodytais privalomais teisėtais pagrindais.

Siekiant remtis 7 straipsnio f punktu kaip duomenų tvarkymo teisiniu pagrindu, būtina įgyvendinti specialias pavojaus mažinimo priemones, kuriomis būtų užtikrinta tinkama darbdavio teisėtų interesų ir darbuotojų pagrindinių teisių ir laisvių pusiausvyra[12]. Tarp tokių

[11] Taip pat žr. WP29 *Nuomonę 15/2011 dėl sąvokos „sutikimas“ apibrėžties,* WP187, 2011 m. liepos 13 d., url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_lt.pdf, p. 24.

[12] Pavyzdį, kokios pusiausvyros reikia laikytis, žr. Sprendime *Köpke / Vokietija*, [2010] ECHR 1725, (URL: http://www.bailii.org/eu/cases/ECHR/2010/1725.html), šioje byloje darbuotojas buvo atleistas, darbdaviui ir

priemonių, priklausomai nuo stebėsenos formos, turėtų būti stebėsenos apribojimai siekiant užtikrinti, kad nebūtų pažeidžiamas darbuotojo privatumas. Tokie apribojimai galėtų būti:

- geografiniai (pvz., stebėsena tik konkrečiose vietose; stebėti jautrias teritorijas, pvz., religinių apeigų vietas, sanitarines zonas ir poilsio kambarius, turėtų būti draudžiama),
- orientuoti į duomenis (pvz., asmeninės elektroninės rinkmenos ir ryšiai neturėtų būti stebimi), ir
- susiję su laiku (pvz., turėtų būti taikomas atrankinis, o ne nuolatinis stebėjimas).

3.1.2. *SKAIDRUMAS (10 IR 11 STRAIPSNIAI)*

10 ir 11 straipsniuose išdėstyti skaidrumo reikalavimai taikomi duomenų tvarkymui darbe; darbuotojai turi būti informuojami apie bet kokios stebėsenos buvimą, tikslus, kuriais planuojama tvarkyti asmens duomenis, ir jiems turi būti pateikta bet kokia kita informacija, reikalinga, sąžiningam duomenų tvarkymui užtikrinti.

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.

3.1.3. *AUTOMATINIAI SPRENDIMAI (15 STRAIPSNIS)*

Duomenų apsaugos direktyvos 15 straipsnyje duomenų subjektams taip pat suteikiama teisė, kad jų atžvilgiu nebus daromas sprendimas, kuris sukuria jiems teisinį poveikį arba kuris panašiai ženkliai paveikia juos ir kuris yra paremtas tiktai automatiniu duomenų tvarkymu, skirtu įvertinti tam tikrus asmeniškus su jais susijusius aspektus, pvz., jų darbo efektyvumą, išskyrus atvejus, kai tas sprendimas reikalingas siekiant sudaryti arba įvykdyti sutartį, tą sprendimą leidžiama priimti pagal Sąjungos arba valstybės narės teisę arba jis grindžiamas konkrečiu duomenų subjekto sutikimu.

3.2. Reglamentas 2016/679 – Bendrasis duomenų apsaugos reglamentas

Į Bendrąjį duomenų apsaugos reglamentą yra įtraukti ir juo sustiprinami Duomenų apsaugos direktyvos reikalavimai. Reglamente taip pat nustatomi nauji įpareigojimai visiems duomenų valdytojams, įskaitant darbdavius.

3.2.1. *PRITAIKYTOJI DUOMENŲ APSAUGA*

Bendrojo duomenų apsaugos reglamento 25 straipsnyje reikalaujama, kad duomenų valdytojai įgyvendintų pritaikytosios duomenų apsaugos ir standartizuotosios duomenų apsaugos priemones. Pavyzdžiui, kai darbdavys darbuotojams išduoda įrenginius, kuriuose naudojamos sekimo technologijos, turėtų būti pasirenkami privatumą labiausiai apsaugantys sprendimai. Turi būti atsižvelgiama į duomenų kiekio mažinimo principą.

3.2.2. *POVEIKIO DUOMENŲ APSAUGAI VERTINIMAI*

---

privačių detektyvų agentūrai įvykdžius slaptą vaizdo stebėjimo operaciją. Nors šiuo atveju EŽTT padarė išvadą, kad nacionalinės institucijos užtikrino teisingą darbdavio teisėtų interesų (apsaugoti savo nuosavybės teises), darbuotojo teisės apsaugoti privatų gyvenimą ir viešojo intereso apginti teisingumą pusiausvyrą, EŽTT taip pat pažymėjo, kad dėl technologijų plėtros įvairiems atitinkamiems interesams ateityje gali būti priskirta kitokia svarba.

Bendrojo duomenų apsaugos reglamento 35 straipsnyje bendrai išdėstomi reikalavimai duomenų valdytojui atlikti poveikio duomenų apsaugai vertinimą, kai dėl duomenų tvarkymo rūšies, visų pirma, kai naudojamos naujos technologijos, ir atsižvelgiant į duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, fizinių asmenų teisėms bei laisvėms gali kilti didelis pavojus. Pavyzdys – sistemingas ir išsamus su fiziniais asmenimis susijusių asmeninių aspektų vertinimas, kuris yra grindžiamas automatizuotu tvarkymu, įskaitant profiliavimą, ir kuriuo remiantis priimami sprendimai, kuriais padaromas su fiziniu asmeniu susijęs teisinis poveikis arba kurie daro panašų didelį poveikį fiziniam asmeniui.

Kai atlikus poveikio duomenų apsaugai vertinimą paaiškėja, kad duomenų valdytojas negali pakankamai sumažinti nustatyto pavojaus, t. y. pavojus išlieka didelis, tada duomenų valdytojas, prieš pradėdamas tvarkyti duomenis, turi pasikonsultuoti su priežiūros institucija (36 straipsnio 1 dalis, paaiškinta WP29 gairėse dėl poveikio duomenų apsaugai vertinimų[13].

3.2.2. *DUOMENŲ TVARKYMAS SU DARBO SANTYKIAIS SUSIJUSIAME KONTEKSTE*

Bendrojo duomenų apsaugos reglamento 88 straipsnyje teigiama, kad valstybės narės gali teisės aktuose ar kolektyvinėse sutartyse numatyti konkretesnes taisykles, kuriomis siekiama užtikrinti teisių ir laisvių apsaugą tvarkant darbuotojų asmens duomenis su darbo santykiais susijusiame kontekste. Minėtos taisyklės visų pirma gali būti nustatomos šiais tikslais:

- įdarbinimo;
- darbo sutarties vykdymo (įskaitant teisės aktais arba kolektyvinėmis sutartimis nustatytų prievolių vykdymą);
- darbo administravimo, planavimo ir organizavimo;
- lygybės ir įvairovės darbo vietoje;
- darbuotojų saugos ir sveikatos;
- darbdavio ar kliento turto apsaugos;
- siekiant pasinaudoti su darbo santykiais susijusiomis individualiomis teisėmis ir išmokomis; ir
- siekiant nutraukti darbo santykius.

Pagal 88 straipsnio 2 dalį visos tos taisyklės turėtų apimti tinkamas ir konkrečias priemones, kuriomis siekiama apsaugoti duomenų subjekto žmogiškąjį orumą, teisėtus interesus ir pagrindines teises, ypatingą dėmesį skiriant:

- duomenų tvarkymo skaidrumui;
- asmens duomenų perdavimui įmonių grupėje arba bendrą ekonominę veiklą vykdančių įmonių grupėje; ir
- stebėsenos sistemoms darbo vietoje.

Šioje nuomonėje darbo grupė pateikė gaires, kaip teisėtai naudotis naujomis technologijomis įvairiais konkrečiais atvejais, ir išsamiai išdėsto tinkamas konkrečias priemones darbuotojų žmogaus orumui, teisėtiems interesams ir pagrindinėms teisėms apsaugoti.

4. Pavojai

[13] WP29, *Gairės dėl poveikio duomenų apsaugai vertinimo ir nustatymo, ar duomenų tvarkymas gali kelti didelį pavojų pagal Reglamentą 2016/679*, WP248, 2017 m. balandžio 4 d., url: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137, p. 18.

Šiuolaikinėmis technologijomis sudaromos sąlygos, naudojantis įvairiais įrenginiais, pvz., išmaniaisiais telefonais, staliniais kompiuteriais, planšetiniais kompiuteriais, transporto priemonėmis ir ant kūno nešiojamais įrenginiais, tam tikrą laiką sekti darbuotojus įvairiose darbo vietose ir namuose. Jeigu nenustatomos duomenų tvarkymo ribos ir jeigu šis duomenų tvarkymas yra neskaidrus, kyla didelis pavojus, kad teisėti darbdavių interesai – gerinti efektyvumą ir apsaugoti įmonės turtą – taps nepateisinamu, intervenciniu stebėjimu.

Ryšių stebėjimo technologijos taip pat gali atgrasyti darbuotojus nuo naudojimosi pagrindinėmis savo teisėmis burtis į grupes, rengti darbuotojų susirinkimus ir konfidencialiai palaikyti ryšius (įskaitant teisę ieškoti informacijos). Ryšių ir elgsenos stebėsena darbuotojams bus daromas spaudimas laikytis reikalavimų, kad nebūtų aptikta dalykų, kurie gali būti suvokiami kaip anomalijos, panašiai kaip intensyvus AVSS naudojimas daro įtaką piliečių elgsenai viešose erdvėse. Be to, dėl šių technologijų galimybių darbuotojai gali nežinoti, kokie asmens duomenys tvarkomi ir kokiais tikslais tai daroma, taip pat jie netgi gali nežinoti apie pačios stebėsenos technologijos buvimą.

Naudojimosi IT priemonėmis stebėsena taip pat skiriasi nuo kitų, labiau pastebimų stebėsenos priemonių, pvz., AVSS, nes tokia stebėsena gali būti vykdomas slapta. Jei nėra lengvai suprantamos ir lengvai prieinamos darbo vietos stebėsenos politikos, darbuotojai gali nežinoti apie vykdomo stebėsenos buvimą ir padarinius ir todėl gali neturėti sąlygų naudotis savo teisėmis. Papildomą pavojų kelia pernelyg didelio duomenų kiekio rinkimas tokiose sistemose, pvz., *WiFi* buvimo vietos duomenų rinkimas.

Daugėjant darbo vietos aplinkoje generuojamų duomenų ir taikant naujus duomenų analizės ir sutikrinimo metodus, taip pat gali kilti pavojų, kad duomenys bus toliau tvarkomi nesilaikant reikalavimų. Tolesnio neteisėto duomenų tvarkymo pavyzdžiai – kai sistemos, teisėtai įrengtos turtui apsaugoti, vėliau naudojamos darbuotojų buvimui darbo vietoje, darbo efektyvumui ir draugiškumui klientų atžvilgiu stebėti. Kiti pavyzdžiai – per AVSS surinkti duomenys naudojami darbuotojų elgsenai ir darbo efektyvumui reguliariai stebėti arba geografinės buvimo vietos nustatymo sistemos (pvz., *WiFI* arba *Bluetooth* sekimo) duomenys naudojami darbuotojų judėjimui ir elgsenai nuolat tikrinti.

Todėl tokiu sekimu gali būti pažeidžiamos darbuotojų teisės į privatumą, neatsižvelgiant į tai, ar stebėsena vykdoma sistemingai, ar kartais. Pavojus kyla ne tik dėl ryšių turinio analizės. Taigi, asmens metaduomenų analizė gali sudaryti sąlygas ne mažiau privatumą pažeidžiančiu būdu išsamiai stebėti asmens gyvenimą ir elgsenos tendencijas.

Plačiai naudojant stebėsenos technologijas taip pat gali būti apribotas darbuotojų noras (ir kanalai, kuriais jie tai galėtų padaryti) informuoti darbdavius apie vadovų ir (arba) kitų darbuotojų daromus pažeidimus ar neteisėtus veiksmus, kuriais gali būti padaryta žala verslui (ypač klientų duomenims) arba darbo vietai. Kad atitinkamas darbuotojas imtųsi veiksmų ir praneštų apie tokius atvejus, dažnai reikalingas anonimiškumas. Stebėsena, kuria pažeidžiamos darbuotojų teisės į privatumą, gali trukdyti pateikti reikiamus pranešimus atitinkamiems pareigūnams. Tokiu atveju nustatytos vidaus pažeidimų atskleidimo priemonės gali tapti neveiksmingos[14].

[14] Žr., pavyzdžiui, WP29 *Nuomonę 1/2006 dėl ES duomenų apsaugos taisyklių taikymo vidaus pažeidimų atskleidimo sistemoms apskaitos, vidaus apskaitos kontrolės, audito, kovos su kyšininkavimu, bankininkystės ir*

5. Scenarijai

Šiame skirsnyje aptariami tam tikri duomenų tvarkymo darbe scenarijai, kuriems įvykus naujos technologijos ir (arba) esamų technologijų plėtra tampa arba gali tapti dideliu pavojumi darbuotojų privatumui. Visais tokiais atvejais darbdaviai turėtų apsvarstyti, ar:

- duomenų tvarkymo veikla yra reikalinga, ir jeigu taip, kokie taikomi teisiniai pagrindai;
- siūlomas asmens duomenų tvarkymas yra sąžiningas darbuotojų atžvilgiu;
- duomenų tvarkymo veikla yra proporcinga iškeltoms problemoms;
- duomenų tvarkymo veikla yra skaidri.

5.1. Duomenų tvarkymo operacijos vykstant įdarbinimo procesui

Asmenys gana plačiai naudojasi socialine žiniasklaida ir, priklausomai nuo paskyros turėtojo pasirinktų parametrų, gana dažnai vartotojų profiliai būna viešai matomi. Taigi, darbdaviai gali manyti, kad vykstant įdarbinimo procesams, gali būti pateisinama peržiūrėti galimų kandidatų socialinius profilius. Tai pasakytina ir apie kitą viešai prieinamą informaciją apie galimą darbuotoją.

Vis dėlto darbdaviai neturėtų daryti prielaidos, jog vien todėl, kad asmens socialinės žiniasklaidos profilis yra viešai prieinamas, jie gali tvarkyti tuos duomenis savo tikslais. Šiam duomenų tvarkymui reikalingas teisinis pagrindas, pvz., teisėti interesai. Šiomis aplinkybėmis darbdavys, prieš peržiūrėdamas socialinės žiniasklaidos profilį, turėtų atsižvelgti į tai, ar kandidato socialinės žiniasklaidos profilis susijęs su verslo, ar su asmeniniais tikslais, nes tai gali būti svarbus duomenų patikrinimo teisinio leistinumo požymis. Be to, darbdaviams rinkti ir tvarkyti su kandidatais į darbo vietas susijusius asmens duomenis leidžiama tik tiek, kiek tų duomenų rinkimas reikalingas ir aktualus pareigoms, į kurias pretenduojama, vykdyti.

Įdarbinimo proceso metu surinkti duomenys paprastai turėtų būti ištrinami iš karto, kai tampa aišku, kad nebus pateiktas darbo pasiūlymas arba atitinkamas asmuo jo nepriima[15]. Apie tokį duomenų tvarkymą taip pat turi būti tinkamai informuojamas pats asmuo prieš jam pradedant dalyvauti įdarbinimo procese.

Darbdavys neturi teisinio pagrindo reikalauti, kad galimi darbuotojai *susidraugautų* su galimu darbdaviu ar kitais būdais suteiktų prieigą prie savo profilių turinio.

Pavyzdys

Įdarbindamas naujus darbuotojus, darbdavys tikrina kandidatų profilius įvairiuose socialiniuose tinkluose ir į atrankos procesą įtraukia informaciją iš šių tinklų (ir visą kitą internete prieinamą informaciją).

---

finansiniais nusikaltimais srityse, WP117, 2006 m. vasario 1 d., url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2006/wp117_lt.pdf.

[15] Taip pat žr. Europos Tarybos Ministrų Komiteto *rekomendacijos CM/Rec(2015)5 valstybėms narėms dėl asmens duomenų tvarkymo darbo santykių kontekste* 13.2 punktą (2015 m. balandžio 1 d., url: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3f7a). Tais atvejais, kai darbdavys pageidauja išsaugoti duomenis, norėdamas turėti galimybę pasiūlyti kandidatui laisvą darbo vietą vėliau, duomenų subjektas turėtų būti atitinkamai informuojamas ir jam turėtų būti suteikta galimybė nesutikti dėl tokio tolesnio duomenų tvarkymo – tokiu atveju duomenys turėtų būti ištrinti (id.).

Teisinį pagrindą pagal 7 straipsnio f punktą peržiūrėti viešai prieinamą informaciją apie kandidatus darbdavys gali turėti tik tokiu atveju, jei peržiūrėti informaciją apie kandidatą socialinėje žiniasklaidoje reikalinga, pavyzdžiui, siekiant įgyti galimybę įvertinti konkrečius pavojus, susijusius su kandidatais į konkrečias pareigas, ir kandidatai apie tai tinkamai informuojami (pavyzdžiui, darbo skelbimo tekste).

5.2. Duomenų tvarkymo operacijos, atliekamos tikrinant darbuotojus darbo santykių kontekste

Dėl esamų profilių socialinėje žiniasklaidoje ir plėtojantis naujoms analitinėms technologijoms, darbdaviai turi (arba gali gauti) techninę galimybę nuolat tikrinti darbuotojus rinkdami informaciją apie jų draugus, nuomones, įsitikinimus, interesus, įpročius, buvimo vietą, požiūrį ir elgseną, taip fiksuodami duomenis, įskaitant neskelbtinus duomenis, apie darbuotojo privatų ir šeimos gyvenimą.

Darbuotojų socialinės žiniasklaidos profiliai darbo santykių kontekste bendraisiais pagrindais neturėtų būti tikrinami.

Be to, darbdaviai neturėtų reikalauti darbuotojo arba kandidato į darbo vietą suteikti prieigą prie informacijos, kuria jis dalijasi su kitais asmenimis socialiniuose tinkluose.

Pavyzdys
Nekonkuravimo išlygų galiojimo laikotarpiu darbdavys stebi buvusių darbuotojų, susaistytų nekonkuravimo išlygomis, *LinkedIn* profilius. Šios stebėsenos tikslas – stebėti, kaip laikomasi šių išlygų. Stebimi tik šie buvę darbuotojai.

Tol, kol darbdavys gali įrodyti, kad tokia stebėsena yra reikalinga jo teisėtiems interesams apginti ir nėra kitų ne tokių intervencinių priemonių, o buvę darbuotojai yra tinkamai informuoti apie reguliaraus jų viešų ryšių stebėjimo mastą, darbdavys veikiausiai gali remtis Duomenų apsaugos direktyvos 7 straipsnio f punkte nurodytu teisiniu pagrindu.

Be to, iš darbuotojų neturėtų būti reikalaujama naudotis darbdavio suteiktu socialinės žiniasklaidos profiliu. Net kai tai yra konkrečiai numatyta atsižvelgiant į darbuotojų (pvz., organizacijos atstovo spaudai) pareigas, jiems turi būti palikta galimybė naudoti *nedarbinį* neviešą profilį, kurį jie galėtų naudoti vietoje oficialaus su darbdaviu susijusio profilio, ir tai turėtų būti nurodyta kaip viena iš darbo sutarties sąlygų.

5.3. Duomenų tvarkymo operacijos, atliekamos stebint, kaip IRT naudojamos darbo vietoje

Tradiciškai elektroninių ryšių (pvz., telefono, interneto naršymo, e. pašto, tikralaikių pokalbių, IP telefonijos ir kt.) sekimas darbo vietoje laikomas pagrindine grėsme darbuotojų privatumui. Savo 2001 m. *Darbiniame dokumente dėl elektroninių ryšių sekimo darbo vietoje* WP29 pateikė tam tikras išvadas dėl e. pašto ir interneto naudojimo stebėjimo. Nors tos išvados tebėra aktualios, reikia atsižvelgti į technologinę plėtrą, dėl kurios tapo įmanomi naujesni, ir galbūt labiau intervenciniai ir skvarbesni stebėjimo būdai. Tokia plėtra, be kita ko, apima:

- duomenų praradimo prevencijos priemones, kuriomis stebimi siunčiami ryšio signalai siekiant aptikti galimus duomenų saugumo pažeidimus;
- naujos kartos ugniasienes ir integruotas grėsmės valdymo sistemas, galinčias suteikti įvairių stebėsenos technologijų, įskaitant išsamią duomenų paketo analizę, transporto lygmens protokolo, skirto saugumui užtikrinti, perėmimą, svetainių filtravimą, prietaise kaupiamas ataskaitas, informaciją apie vartotojo tapatybę ir (kaip jau aprašyta) duomenų praradimo prevenciją. Tokios technologijos taip pat gali būti panaudojamos individualiai, priklausomai nuo darbdavio;

- saugumo programas ir priemones, apimančias darbuotojo prisijungimų prie darbdavio sistemų registravimą;
- technologiją *eDiscovery*, susijusią su bet kuriuo procesu, kuriuo ieškoma elektroninių duomenų siekiant juos panaudoti kaip įrodymus;
- programos ir įrenginio naudojimo sekimą nematoma programine įranga, esančia staliniame kompiuteryje arba debesijoje;
- biuro programų, teikiamų kaip debesijos paslauga, kuriomis teoriškai sudaromos sąlygos labai išsamiai registruoti darbuotojų veiklą, naudojimą darbo vietoje;
- asmeninių įrenginių (pvz., nešiojamųjų kompiuterių, mobiliųjų telefonų, planšetinių kompiuterių), kuriuos darbuotojai pasitelkia savo darbui pagal konkrečią naudojimo politiką, pvz., asmeninių įrenginių naudojimo politiką arba mobiliųjų įrenginių valdymo technologiją, kuria sudaromos sąlygos paskleisti programas, duomenis, konfigūravimo parametrus ir mobiliųjų įrenginių programų keitimo kodus, stebėseną; ir
- ant kūno nešiojamų įrenginių (pvz., sveikatos ir fizinės formos stebėjimo įrenginių) naudojimą.

Gali būti, kad darbdavys įgyvendins stebėsenos sprendimą *viskas viename*, pvz., saugumo paketų rinkinį, kuriuo jam sudaromos sąlygos stebėti, kaip darbo vietoje naudojamos visos IRT, o ne tik e. paštas ir (arba) interneto svetainės, kaip būdavo anksčiau. WP55 priimtos išvados būtų taikomos bet kuriai sistemai, kuria sudaromos sąlygos vykdyti tokią stebėseną[16].

Pavyzdys

Darbdavys ketina panaudoti transporto lygmens protokolo, skirto saugumui užtikrinti, tikrinimo įrenginį, kuriuo būtų iššifruotas ir patikrintas apsaugotas duomenų srautas, kad būtų aptikta piktavališka veikla. Įrenginys taip pat gali registruoti ir analizuoti visą darbuotojo internetinę veiklą organizacijos tinkle.

Siekiant nuo perėmimo apsaugoti internetinius duomenų srautus, kuriuose esama asmens duomenų, vis dažniau naudojami šifruoti ryšių protokolai. Vis dėlto tai gali kelti ir problemų, nes dėl šifravimo tampa neįmanoma stebėti priimamų ir siunčiamų duomenų. Transporto lygmens protokolo, skirto saugumui užtikrinti, tikrinimo įranga iššifruojamas duomenų srautas, analizuojamas turinys saugumo tikslais ir tada srautas vėl užšifruojamas.

Šiame pavyzdyje darbdavys remiasi teisėtais interesais – būtinumu apsaugoti tinklą ir tinkle laikomus darbuotojų bei klientų asmens duomenis nuo neteisėto prisijungimo ar duomenų nutekėjimo. Vis dėlto visos darbuotojų internetinės veiklos stebėsena yra neproporcingas atsakas ir teisės į ryšių slaptumą pažeidimas. Darbdavys pirmiausia turėtų išnagrinėti kitas, ne tokias intervencines priemones klientų duomenų konfidencialumui ir tinklo saugumui užtikrinti.

Jeigu tam tikrą transporto lygmens protokolo, skirto saugumui užtikrinti, duomenų srauto perėmimą galima laikyti būtinai reikalingu, įrenginys turėtų būti sukonfigūruotas taip, kad

[16] Taip pat žr. Sprendimą *Copland / Jungtinė Karalystė,* (2007 m.) 45 EHRR 37, 25 BHRC 216, 2 ALR Int'l 785, [2007] ECHR 253 (url: http://www.bailii.org/eu/cases/ECHR/2007/253.html), kuriame EŽTT nurodė, kad iš verslo patalpų siunčiami e. pašto laiškai ir stebint interneto naudojimą gauta informacija gali sudaryti darbuotojo privataus gyvenimo ir korespondencijos dalį ir kad tos informacijos rinkimas ir saugojimas be darbuotojo žinios prilygtų darbuotojo teisių pažeidimui, nors EŽTT ir nenurodė, kad tokia stebėsena demokratinėje visuomenėje niekada nebūtų reikalinga.

nebūtų visą laiką registruojama darbuotojo veikla, o, pavyzdžiui, būtų blokuojamas įtartinas priimamas ar siunčiamas srautas ir vartotojas būtų nukreipiamas į informacinį portalą, kuriame jis galėtų prašyti peržiūrėti tokį automatinį sprendimą. Jeigu tam tikras bendras registravimas vis dėlto būtų laikomas būtinai reikalingu, įrenginys taip pat gali būti sukonfigūruotas nekaupti žurnalo duomenų, jeigu įrenginys neparodė, kad įvyko incidentas, ir rinkti kuo mažesnį informacijos kiekį.

Taikydamas gerąją patirtį, darbdavys galėtų pasiūlyti darbuotojams alternatyvią nestebimą prieigą. Tai būtų galima padaryti pasiūlant nemokamą belaidį vietinį tinklą (*WiFi*) arba atskirus įrenginius arba terminalus (taikant tinkamas apsaugos priemones ryšių konfidencialumui užtikrinti), kuriais naudodamiesi darbuotojai galėtų įgyvendinti savo teisėtą teisę kartais pasinaudoti darbo įranga asmeniniais tikslais[17]. Be to, darbdaviai turėtų atsižvelgti į tam tikrų rūšių duomenų srautą, kurio perėmimas kelia pavojų tinkamai darbdavio teisėtų interesų ir darbuotojo privatumo – pvz., asmeninio internetinio e. pašto naudojimo, apsilankymų internetinės bankininkystės ir sveikatos svetainėse – pusiausvyrai, siekdami tinkamai sukonfigūruoti įrenginį, kad proporcingumo principo neatitinkančiomis aplinkybėmis ryšiai nebūtų perimami. Darbuotojams turėtų būti nurodoma, kokių rūšių ryšiai stebimi įrenginiu.

Turėtų būti parengta politika, kada ir kas gali prisijungti prie įtartinų žurnalo duomenų, ir visiems darbuotojams turi būti suteikta galimybė nuolat lengvai su ja susipažinti, kad jie, be kita ko, galėtų suprasti, koks yra priimtinas ir nepriimtinas tinklo ir infrastruktūros naudojimas. Taip darbuotojams sudaromos sąlygos pritaikyti savo elgseną, kad jie nebūtų stebimi, kai teisėtai naudojasi darbo IT įranga asmeniniais tikslais. Geroji patirtis būtų įvertinti tokią politiką bent kartą per metus, siekiant išnagrinėti, ar pasirinktas stebėsenos sprendimas duoda planuotų rezultatų ir ar esama kitų, ne tokių intervencinių priemonių ar būdų tiems patiems tikslams pasiekti.

Neatsižvelgiant į atitinkamą technologiją ar jos teikiamas galimybes, 7 straipsnio f punkte nurodytą teisinį pagrindą galima taikyti tik tuo atveju, jei duomenų tvarkymas atitinka tam tikras sąlygas. Pirmiausia, šiuos produktus ir programas naudojantys darbdaviai turi įvertinti savo įgyvendinamų priemonių proporcingumą ir tai, ar galima imtis papildomų veiksmų duomenų tvarkymo mastui ir poveikiui sušvelninti ar sumažinti. Prieš pradedant taikyti bet kurią stebėsenos technologiją, šis argumentas turėtų būti taikomas kaip geroji patirtis atliekant poveikio duomenų apsaugai vertinimą. Antra, darbdaviai turi įgyvendinti ir paskelbti priimtino naudojimo politikos priemones kartu su privatumo politikos priemonėmis, bendrai išdėstydami, kaip leidžiama naudoti organizacijos tinklą ir įrangą, ir tiksliai išvardydami, kaip tvarkomi duomenys.

Kai kuriose šalyse tokiai politikai sukurti būtų teisiškai reikalingas darbuotojų tarybos arba panašios darbuotojams atstovaujančios struktūros pritarimas. Praktiškai tokias politikos priemones dažnai rengia IT priežiūros darbuotojai. Kadangi daugiausia dėmesio tie darbuotojai skiria saugumui, o ne teisėtiems darbuotojų privatumo lūkesčiams, WP29

[17] Žr. Sprendimą *Halford / Jungtinė Karalystė*, [1997] ECHR 32, (url: http://www.bailii.org/eu/cases/ECHR/1997/32.html), kuriame EŽTT nurodė, kad *telefono skambučiai iš verslo patalpų ir iš namų gali patekti į privataus gyvenimo ir korespondencijos sąvokų sritį, kaip nurodyta [konvencijos] 8 straipsnio 1 dalyje*; ir Sprendimą *Barbulescu / Rumunija*, [2016] ECHR 61, (url: http://www.bailii.org/eu/cases/ECHR/2016/61.html), dėl darbinės tikralaikių pokalbių paskyros naudojimo asmeninei korespondencijai, kuriame EŽTT nurodė, kad darbdavio vykdomas paskyros stebėjimas buvo ribotas ir proporcingas; teisėjo Pinto de Alberquerque atskiroje nuomonėje raginama sukurti apdairią pusiausvyrą.

rekomenduoja, kad vertinant stebėsenos reikalingumą ir politikos logiką bei prieinamumą visais atvejais dalyvautų reprezentatyvi darbuotojų imtis.

Pavyzdys

Darbdavys, naudodamasis duomenų praradimo prevencijos priemone, automatiškai stebi siunčiamus e. pašto laiškus, kad būtų užkirstas kelias neleistinam nuosavybinių duomenų (pvz., kliento asmens duomenų) perdavimui, nepriklausomai nuo to, ar toks perdavimas vykdomas netyčia, ar tyčia. Kai e. pašto laiškas pripažįstamas galimu duomenų saugumo pažeidimo šaltiniu, atliekamas tolesnis tyrimas.

Darbdavys vėl remiasi savo teisėtais interesais – būtinumu apsaugoti klientų asmens duomenis ir jo turtą nuo neleistinos prieigos ar duomenų nutekėjimo. Tačiau taikant tokią duomenų praradimo prevencijos priemonę, duomenys gali būti tvarkomi be reikalo, pavyzdžiui, kai sistemoje pateikiamas klaidingas įspėjimas, gali būti neleistinai prisijungta prie darbuotojų išsiųstų teisėtų e. pašto laiškų (kurie, pavyzdžiui, gali būti asmeniniai e. pašto laiškai).

Todėl duomenų praradimo prevencijos priemonės reikalingumas ir jos panaudojimas turėtų būti iki galo pagrįstas, kad būtų pasiekta tinkama teisėtų darbdavio interesų ir darbuotojų pagrindinės teisės į savo asmens duomenų apsaugą pusiausvyra. Kad būtų galima remtis teisėtais darbdavio interesais, turėtų būti imamasi tam tikrų pavojaus mažinimo priemonių. Pavyzdžiui, taisyklės, pagal kurias sistemoje e. pašto laiškas įvardijamas kaip galimas duomenų saugumo pažeidimas, vartotojams turėtų būti visiškai skaidrios, o tokiais atvejais, kai sistemoje pripažįstama, kad e. pašto laiškas, kurį planuojama siųsti, yra galimas duomenų pažeidimas, to e. pašto laiško siuntėjui prieš persiunčiant laišką turėtų būti parodomas įspėjamasis pranešimas, kad siuntėjas turėtų galimybę šį persiuntimą atšaukti.

Kai kuriais atvejais darbuotojus įmanoma stebėti ne todėl, kad naudojamos konkrečios technologijos, o tiesiog todėl, kad darbuotojai raginami naudotis darbdavio suteiktomis internetinėmis programomis, kuriomis tvarkomi asmens duomenys. Šio atvejo pavyzdys – debesijos pagrindu veikiančios biuro programos (pvz., dokumentų redagavimo programos, kalendoriai, socialiniai tinklai). Turėtų būti užtikrinta, kad darbuotojai galėtų nusistatyti tam tikras privačias erdves, į kurias darbdavys galėtų patekti tik išimtinėmis aplinkybėmis. Tai, pavyzdžiui, pasakytina apie kalendorius, kurie dažnai naudojami ir privatiems susitikimams. Jeigu darbuotojas susitikimą pažymi kaip *privatų* arba tai pažymi pačiame įraše apie susitikimą, darbdaviams (ir kitiems darbuotojams) neturėtų būti leidžiama peržiūrėti įrašo apie susitikimą turinio.

Reikalavimas laikytis subsidiarumo principo šiomis aplinkybėmis kartais reiškia, kad stebėsenos apskritai negalima vykdyti. Pavyzdžiui, taip yra tada, kai draudžiamo ryšių paslaugų naudojimo galima išvengti blokuojant tam tikras svetaines. Siekiant įvykdyti šį reikalavimą laikytis subsidiarumo principo, jeigu įmanoma blokuoti svetaines, vietoj nuolatinės visų ryšių stebėsenos turėtų būti pasirenkamas blokavimas.

Apskritai prevencijai turėtų būti skiriama daugiau dėmesio negu aptikimui – darbdavio interesai geriau įgyvendinami techninėmis priemonėmis užkertant kelią netinkamam interneto naudojimui, o ne plečiant išteklius netinkamo naudojimo atvejams aptikti.

5.4. Duomenų tvarkymo operacijos, atliekamos stebint, kaip naudojamos IRT ne darbo vietoje

Naudotis IRT ne darbo vietoje imta dažniau populiarėjant tokiai politikai, kuria skatinama dirbti namuose, dirbti nuotoliniu būdu ir darbe naudoti asmeninius įrenginius. Tokių

technologijų teikiamos galimybės gali kelti pavojų darbuotojų privačiam gyvenimui, nes daugeliu atvejų darbo vietoje esančias sistemas imama veiksmingai taikyti ir darbuotojų namų aplinkoje, kurioje jie tą įrangą naudoja.

5.4.1. *DARBO NAMUOSE IR NUOTOLINIO DARBO STEBĖSENA*

Darbdaviai dažniau siūlo darbuotojams galimybę dirbti nuotoliniu būdu, pvz., namuose ir (arba) kelionės metu. Iš tikrųjų tai yra vienas iš svarbiausių veiksnių, dėl kurių mažėja darbo vietos ir namų skirtumai. Apskritai tai pasakytina apie tokius atvejus, kai darbdavys darbuotojams suteikia IRT įrangą arba programinę įrangą, kuri įrengiama jų namuose ir (arba) jų pačių įrenginiuose ir suteikia jiems tokio paties lygio prieigą prie darbdavio tinklo, sistemų ir išteklių, kurią jie turėtų būdami darbo vietoje, atsižvelgiant į tai, kaip tai įgyvendinama.

Nors nuotolinis darbas gali būti teigiama tendencija, dėl to darbdaviams gali kilti papildomų pavojų. Pavyzdžiui, darbuotojai, turintys nuotolinę prieigą prie darbdavio infrastruktūros, neprivalo laikytis fizinių saugumo priemonių, kurios gali būti taikomos darbdavio patalpose. Paprastai tariant, neįgyvendinus tinkamų techninių priemonių neleistino prisijungimo pavojus didėja ir dėl to gali būti prarasta arba sunaikinta darbdavio turima informacija, įskaitant darbuotojų arba klientų asmens duomenis.

Siekdami sumažinti šią pavojaus sritį, darbdaviai gali manyti, jog yra pagrįsta naudoti programinės įrangos paketus (arba patalpoje, arba debesijoje), teikiančius galimybių, pavyzdžiui, registruoti klaviatūros paspaudimus ir pelės judesius, fiksuoti ekrano vaizdą (atsitiktiniu metu arba nustatytais intervalais), registruoti naudojamas programas (ir jų naudojimo trukmę), o suderinamuose įrenginiuose – ir įjungti internetines kameras bei fiksuoti jų siunčiamą vaizdą. Tokios technologijos yra plačiai prieinamos, be kita ko, jas teikia trečiosios šalys, pvz., debesijos paslaugų teikėjai.

Vis dėlto tokiomis technologijomis vykdomas duomenų tvarkymas yra neproporcingas ir labai mažai tikėtina, kad darbdavys turės teisinį pagrindą – teisėtus interesus, pvz., įrašinėti darbuotojo klaviatūros paspaudimus ir pelės judesius.

Svarbiausia yra proporcingai ir tik būtinu mastu sumažinti darbo namuose ir nuolatinio darbo keliamą pavojų, kad ir kokiu būdu ta galimybė būtų suteikiama ir kad ir kokia technologija būtų siūloma, ypač jeigu jų naudojimo verslo ir asmeniniais tikslais ribos yra neaiškios.

5.4.2. *ASMENINIŲ ĮRENGINIŲ NAUDOJIMAS*

Didėjant vartotojams skirtų elektroninių įrenginių populiarumui, gausėjant jų funkcijoms ir pajėgumams, darbdaviai gali susidurti su darbuotojų reikalavimais leisti darbo vietoje naudoti asmeninius įrenginius darbui atlikti. Tai žinoma kaip asmeninių įrenginių naudojimo politika.

Asmeninių įrenginių naudojimo politika darbuotojams gali teikti įvairią naudą, be kita ko, didinti jų pasitenkinimą darbu, gerinti mikroklimatą darbe, didinti darbo efektyvumą ir lankstumą. Vis dėlto suprantama, kad tam tikrą laiko dalį darbuotojas savo įrenginį naudos asmeniniais tikslais, ir labiau tikėtina, kad jis tai darys tam tikru dienos metu (pvz., vakarais ir savaitgaliais). Todėl esama aiškios galimybės, kad darbuotojams naudojantis asmeniniais įrenginiais darbdaviai tvarkys ne įmonės informaciją apie tuos darbuotojus ir galbūt jų šeimų narius, kurie taip pat naudojasi atitinkamais įrenginiais.

Darbo santykių kontekste asmeninių įrenginių naudojimo keliami pavojai privatumui paprastai siejami su stebėsenos technologijomis, kuriomis renkami identifikaciniai duomenys, pvz., MAC adresai, arba su atvejais, kai darbdavys prisijungia prie darbuotojo įrenginio kaip pagrindą nurodydamas saugumo patikrą, pvz., siekiant aptikti kenkimo programinę įrangą. Reaguojant į pastarąjį pavojų esama įvairių komercinių sprendimų, kuriais sudaromos sąlygos tikrinti asmeninius įrenginius, tačiau naudojantis tais sprendimais gali būti įgyjama prieiga prie visų tame įrenginyje esančių duomenų, todėl jie turi būti atidžiai valdomi. Pavyzdžiui, prie įrenginio skilčių, kurios, kaip manoma, naudojamos tik asmeniniais tikslais (pvz., prie katalogo su įrenginiu padarytoms nuotraukoms laikyti) prisijungti apskritai negalima.

Tokių įrenginių vietos ir duomenų srauto stebėsena gali būti laikoma atitinkančia teisėtus interesus apsaugoti asmens duomenis, už kuriuos darbdavys yra atsakingas kaip duomenų valdytojas; tačiau darbuotojo asmeninio įrenginio atžvilgiu tai gali būti neteisėta, jeigu tokios stebėsenos metu renkami duomenys, susiję su darbuotojo privačiu ir šeimos gyvenimu. Siekiant užkirsti kelią asmeninės informacijos stebėsenai, turi būti taikomos tinkamos priemonės, kuriomis asmeninio įrenginio naudojimas būtų atskiriamas nuo jo naudojimo verslo tikslais.

Be to, darbdaviai turėtų įgyvendinti metodus, kuriuos taikant įrenginyje esantys jų duomenys būtų saugiai siunčiami tarp įrenginio ir jų tinklo. Todėl įrenginys gali būti sukonfigūruotas taip, kad visas duomenų srautas per virtualųjį privatųjį tinklą (VPN) būtų nukreipiamas atgal į įmonės tinklą, taip sukuriant tam tikrą saugumo lygį; vis dėlto, jeigu naudojama tokia priemonė, darbdavys taip pat turėtų įvertinti, kad stebėsenos tikslais įdiegta programinė įranga kelia pavojų privatumui tais laikotarpiais, kai darbuotojas įrenginiu naudojasi asmeniniais tikslais. Taip pat būtų galima naudoti įrenginius, teikiančius papildomų apsaugos priemonių, pvz., galimybę duomenis *uždaryti į smėlio dėžę* (angl. *sandboxing*, sulaikyti duomenis konkrečioje programoje).

Ir atvirkščiai, darbdavys taip pat turi įvertinti galimybę taikyti draudimą tam tikrus darbo įrenginius naudoti asmeniniais tikslais, jeigu neįmanoma užkirsti kelio tam, kad būtų stebimas asmeninis naudojimas, pavyzdžiui, jeigu įrenginys suteikia galimybę nuotoliniu būdu prisijungti prie asmens duomenų, kurių atžvilgiu darbdavys yra duomenų valdytojas.

5.4.3. *MOBILIŲJŲ ĮRENGINIŲ VALDYMAS*

Mobiliųjų įrenginių valdymu darbdaviams sudaromos sąlygos nuotoliniu būdu nustatyti įrenginių vietą, naudoti konkrečius parametrus ir (arba) programas ir prireikus ištrinti duomenis. Darbdavys šiomis funkcijomis gali naudotis pats arba per trečiąją šalį. Mobiliųjų įrenginių valdymo paslaugomis darbdaviams taip pat sudaromos sąlygos įrašinėti įrenginio duomenis arba jį sekti tikruoju laiku, netgi jeigu nėra pranešta apie jo vagystę.

Jeigu bet kuri tokia technologija yra nauja arba ji yra nauja duomenų valdytojui, prieš pradėdamas ją naudoti jis turėtų atlikti poveikio duomenų apsaugai vertinimą. Jeigu atliekant poveikio duomenų apsaugai vertinimą nustatoma, kad konkrečiomis aplinkybėmis reikalinga mobiliųjų įrenginių valdymo technologija, vis tiek turėtų būti įvertinama, ar ja naudojantis vykdomas duomenų tvarkymas atitinka proporcingumo ir subsidiarumo principus. Darbdaviai turi užtikrinti, kad duomenys, renkami naudojantis šiais nuotolinio vietos nustatymo pajėgumais, būtų tvarkomi konkrečiu tikslu ir nebūtų bei negalėtų būti platesnės programos, kuriomis sudaromos sąlygos nuolat stebėti darbuotojus, dalis. Net ir nurodytais tikslais sekimo funkcijos turėtų būti apribotos. Sekimo sistemos gali būti sudarytos taip, kad buvimo

vietos duomenys būtų registruojami nepateikiant jų darbdaviui – tokiais atvejais buvimo vietos duomenys turėtų tapti prieinami tik tais atvejais, kai būtų pranešta apie su įrenginiu susijusį incidentą arba įrenginio praradimą.

Darbuotojai, kurių įrenginiai įtraukiami į mobiliųjų įrenginių valdymo paslaugas, taip pat turi būti visapusiškai informuojami, koks sekimas vykdomas ir kokius padarinius tas sekimas jiems turi.

5.4.4. *ANT KŪNO NEŠIOJAMI ĮRENGINIAI*

Darbdaviai vis dažniau būna linkę savo darbuotojams išduoti ant kūno nešiojamus įrenginius, kad galėtų sekti ir stebėti darbuotojų sveikatą ir veiklą darbo vietoje, o kartais ir už jos ribų. Tačiau šis duomenų tvarkymas apima sveikatos duomenų tvarkymą, todėl pagal Duomenų apsaugos direktyvos 8 straipsnį jis yra draudžiamas.

Kadangi darbdavių ir darbuotojų santykiai yra nelygūs, t. y. darbuotojas yra finansiškai priklausomas nuo darbdavio, o sveikatos duomenys yra neskelbtino pobūdžio, labai mažai tikėtina, kad tokiems duomenims sekti ar stebėti gali būti duotas teisiškai galiojantis konkretus sutikimas, nes darbuotojai iš esmės negali tokio sutikimo duoti *savanoriškai*. Net jeigu darbdavys sveikatos duomenis renka per trečiąją šalį, kuri darbdaviui teikia tik apibendrintą informaciją apie bendras sveikatos tendencijas, duomenų tvarkymas vis tiek yra neteisėtas.

Be to, kaip aprašyta *Nuomonėje 5/2014 dėl nuasmeninimo metodų*[18], techniškai labai sudėtinga užtikrinti visišką duomenų nuasmeninimą. Net ir tokioje aplinkoje, kurioje dirba daugiau nei tūkstantis darbuotojų, turėdamas kitus duomenis apie darbuotojus, darbdavys vis tiek gali išskirti konkrečius darbuotojus, turinčius konkrečių sveikatos būklės sutrikimų, pvz., aukštą kraujospūdį arba nutukimą.

Pavyzdys:

Organizacija kaip bendrą dovaną savo darbuotojams siūlo fizinės formos stebėsenos įrenginius. Įrenginiai nuolat skaičiuoja darbuotojų žingsnius, registruoja jų pulsą ir miego struktūrą.

Gaunami sveikatos duomenys turėtų būti prieinami tik darbuotojui, o ne darbdaviui. Bet kurie duomenys, persiunčiami tarp darbuotojo (kaip duomenų subjekto) ir įrenginio arba paslaugos teikėjo (kaip duomenų valdytojo), yra tų šalių reikalas.

Kadangi sveikatos duomenis taip pat galėtų tvarkyti komercinė šalis, pagaminusi įrenginius arba teikianti paslaugą darbdaviams, pasirinkdamas įrenginį arba paslaugą darbdavys turėtų įvertinti gamintojo ir (arba) paslaugų teikėjo privatumo politiką, siekdamas užtikrinti, kad ja nebūtų sudaromos sąlygos neteisėtai tvarkyti darbuotojų sveikatos duomenų.

5.5. Duomenų tvarkymo operacijos, susijusios su laiku ir dalyvavimu

Sistemos, kuriomis sudaromos sąlygos darbdaviams kontroliuoti, kas gali patekti į jų patalpas ir (arba) tam tikras jų patalpų erdves, taip pat gali suteikti galimybę sekti darbuotojų veiklą.

[18] WP29 *Nuomonė 5/2014 dėl nuasmeninimo metodų*, WP216, 2014 m. balandžio 10 d., url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_lt.pdf.

Nors tokios sistemos naudojamos jau nemažai metų, naujos technologijos, skirtos darbuotojų laikui ir dalyvavimui sekti, naudojamos plačiau ir apima technologijas, kuriomis tvarkomi biometriniai duomenys ir kiti duomenys, pvz., sekami mobilieji įrenginiai.

Nors tokios sistemos gali sudaryti svarbią darbdavio audito sekos dalį, jos taip pat kelia pavojų, nes suteikia pernelyg daug žinių ir galimybių kontroliuoti darbuotojo veiklą darbo vietoje.

Pavyzdys:

Darbdavys turi serverinę, kurioje skaitmenine forma laikomi neskelbtini verslo duomenys, su darbuotojais susiję asmens duomenys ir su klientais susiję asmens duomenys. Siekdamas įvykdyti teisines prievoles apsaugoti duomenis nuo neleistinos prieigos, darbdavys įrengė prieigos kontrolės sistemą, kuria registruojami įeinantys ir išeinantys darbuotojai, turintys reikiamą leidimą patekti į šią patalpą. Jeigu dingtų koks nors įrangos elementas arba būtų be leidimo prisijungta prie duomenų, jie būtų prarasti arba pavogti, darbdavys pagal turimus įrašus galėtų nustatyti, kas tuo metu turėjo galimybę patekti į patalpą.

Kadangi šis duomenų tvarkymas yra reikalingas ir juo nėra varžoma darbuotojų teisė į privatų gyvenimą, toks duomenų tvarkymas gali atitikti teisėtus interesus pagal 7 straipsnio f punktą, jeigu darbuotojai buvo tinkamai informuoti apie duomenų tvarkymo operaciją. Vis dėlto nuolatinė darbuotojų įėjimo ir išėjimo dažnumo ir tikslaus laiko stebėsena negali būti pateisinama, jeigu šie duomenys taip pat bus naudojami kitu tikslu, pvz., darbuotojo darbo efektyvumui įvertinti.

5.6. Duomenų tvarkymo operacijos naudojant vaizdo stebėjimo sistemas

Dėl vaizdo stebėjimo ir toliau kyla panašių su darbuotojų privatumu susijusių problemų kaip ir anksčiau – suteikiama galimybė nuolat fiksuoti darbuotojo elgseną[19]. Aktualiausi pokyčiai, susiję su šios technologijos taikymu darbo santykių kontekste, yra galimybė nuolatiniu būdu lengvai prisijungti prie surinktų duomenų (pvz., per išmanųjį telefoną); sumažėjęs kamerų dydis (kartu didėjant jų pajėgumams, pvz., atsiradus didelei raiškai); ir duomenų tvarkymas, kurį galima atlikti naujomis vaizdo analizės programomis.

Turėdamas vaizdo analizės programų teikiamas galimybes, darbdavys gali automatizuotomis priemonėmis stebėti darbuotojo veido išraišką, aptikti nuokrypius nuo iš anksto nustatytos judėjimo struktūros (pvz., gamyklos sąlygomis) ir kt. Tokia praktika būtų neproporcinga darbuotojų teisių ir laisvių atžvilgiu ir todėl paprastai ji būna neteisėta. Taip pat tikėtina, kad duomenų tvarkymas apims profiliavimą ir galbūt automatizuotą sprendimų priėmimą. Todėl darbdaviai turėtų nenaudoti veido atpažinimo technologijų. Kraštutiniais atvejais galimos tam tikros šios taisyklės išimtys, tačiau remiantis tokiais scenarijais negalima bendrai grįsti minėtos technologijos naudojimo teisėtumo[20].

5.7. Duomenų tvarkymo operacijos, susijusios su darbuotojų naudojamomis transporto priemonėmis

[19] Žr. pirmiau minėtą sprendimą *Köpke / Vokietija*; be to, pažymėtina, jog kai kuriose jurisdikcijose buvo nuspręsta, kad įrengti tokias sistemas kaip AVSS neteisėtai elgsenai įrodyti yra leistina; žr. Ispanijos Konstitucinio Teismo sprendimą *Bershka*.

[20] Be to, pagal Bendrąjį duomenų apsaugos reglamentą biometrinių duomenų tvarkymas identifikaciniais tikslais turi būti grindžiamas 9 straipsnio 2 dalyje numatyta išimtimi.

Plačiai paplito technologijos, kuriomis darbdaviams sudarančios darbdaviams sąlygas stebėti savo transporto priemones, ypač organizacijose, kurių veikla susijusi su transportu arba kurios turi nemažus transporto priemonių parkus.

Bet kuris darbdavys, naudojantis transporto priemonių telematiką, renka duomenis apie transporto priemonę ir konkretų darbuotoją, kuris ta transporto priemone naudojasi. Šie duomenys gali būti ne tik transporto priemonės (ir atitinkamai – darbuotojo) buvimo vieta, nustatoma elementariomis GPS sekimo sistemomis, tačiau, priklausomai nuo technologijos, – ir daug kitos informacijos, įskaitant vairuotojo veiksmus. Tam tikros technologijos (pvz., įvykių duomenų registratoriai) taip pat gali sudaryti sąlygas nuolat stebėti transporto priemonę ir vairuotoją.

Darbdavys gali būti įpareigotas transporto priemonėse įrengti sekimo technologiją, kad galėtų įrodyti, jog laikosi kitų teisinių įpareigojimų, pvz., skirtų tas transporto priemones vairuojančių darbuotojų saugai užtikrinti. Be to, darbdavio teisėti interesai gali būti 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, pvz., lankantis pas gydytoją. Taip darbuotojas gali savo iniciatyva tam tikrus buvimo vietos duomenis apsaugoti kaip privačius. Darbdavys turi užtikrinti, kad renkami duomenys nebūtų naudojami siekiant toliau neteisėtai juos tvarkyti, pvz., 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 (ir kad, priklausomai nuo atitinkamos technologijos, gali būti įrašinėjami ir vairuotojo veiksmai). Pageidautina, kad tokia informacija būtų aiškiai nurodyta kiekviename automobilyje, vairuotojo regėjimo lauke.

Darbuotojams gali būti leidžiama naudotis įmonės transporto priemonėmis ne darbo metu, pvz., asmeniniais tikslais, priklausomai nuo konkrečios tų transporto priemonių naudojimo reglamentavimo politikos. Atsižvelgiant į buvimo vietos duomenų neskelbtinumą, nėra tikėtina, kad būtų teisinis pagrindas stebėti darbuotojų transporto priemonių buvimo vietą ne sutartu darbo metu. Vis dėlto, jeigu tai būtų reikalinga, turėtų būti apsvarstyta, ar reikia įgyvendinti stebėsenos priemones, kurios būtų proporcingos kylantiems pavojams. Pavyzdžiui, tai galėtų reikšti, kad siekiant užkirsti kelią automobilio vagystei automobilio vieta nebūtų registruojama ne darbo metu, jeigu transporto priemonė neišvyksta iš plačiai apibrėžtos teritorijos (regiono arba netgi šalies). Be to, buvimo vieta būtų rodoma tik *avariniu* atveju – darbdavys, prisijungdamas prie sistemoje jau saugomų duomenų, buvimo vietos rodymą aktyvuotų tik tokiu atveju, jeigu transporto priemonė išvyktų iš regiono, kuris buvo nustatytas iš anksto.

Kaip nurodyta WP29 *Nuomonėje 13/2011 dėl išmaniuosiuose mobiliuosiuose įrenginiuose įdiegtų geografinės buvimo vietos nustatymo paslaugų*[21]:

Transporto priemonių sekimo įtaisai nėra darbuotojų sekimo įtaisai. Jų funkcija – sekti arba stebėti transporto priemonių, kuriose šie įtaisai įmontuoti, buvimo vietą. Darbdaviai neturėtų jų laikyti vairuotojų ar kitų darbuotojų elgsenos ar buvimo vietos sekimo ar stebėjimo priemonėmis, pvz., siųsdami įspėjimus dėl transporto priemonės greičio.

Be to, kaip teigiama WP29 *Nuomonėje 5/2005 dėl vietos nustatymo duomenų naudojimo siekiant teikti pridėtinės vertės paslaugas*[22]:

"Vietos nustatymo duomenų tvarkymą galima pateisinti, jeigu tai yra transporto, asmenų ar prekių stebėsenos arba išteklių paskirstymo atskirų vietovių tarnyboms (pvz., planuojant veiklą realiu laiku) dalis arba kai siekiama apsaugoti patį darbuotoją arba jam patikėtas prekes ar automobilius. Priešingai, Darbo grupė mano, kad duomenų tvarkymas visiškai nereikalingas, jeigu darbuotojai patys kaip nori organizuoja savo keliones arba jeigu taip siekiama tik stebėti darbuotojo darbą, kai tai galima daryti kitais būdais."

5.7.1. ĮVYKIO DUOMENŲ REGISTRATORIAI

Įvykio duomenų registratoriai teikia darbdaviui techninę galimybę tvarkyti didelį kiekį įmonės transporto priemones vairuojančių darbuotojų asmens duomenų. Tokie įrenginiai vis dažniau sumontuojami transporto priemonėse siekiant įrašinėti vaizdą, galbūt ir garsą, avarijos atveju. Šios sistemos gali įrašinėti tam tikru metu, pvz., reaguodamos į staigų stabdymą, staigų krypties pasikeitimą arba avarijas, kai įrašomi momentai prieš pat avariją, tačiau jos gali būti nustatytos ir taip, kad vykdytų nuolatinę stebėseną. Vėliau šią informaciją galima naudoti asmens vairavimo veiksmams stebėti ir peržiūrėti siekiant juos patobulinti. Be to, daugelis šių sistemų apima per GPS atliekamą transporto priemonės buvimo vietos stebėjimą tikruoju laiku, o tolesniam tvarkymui taip pat gali būti kaupiami ir kiti vairavimo duomenys (pvz., transporto priemonės greitis).

Šie įrenginiai itin paplito tarp organizacijų, kurių veikla apima transportą ar kurios turi nemažus transporto priemonių parkus. Tačiau įvykio duomenų registratorius galima teisėtai panaudoti tik tuo atveju, jeigu atitinkamus darbuotojo asmens duomenis reikia tvarkyti teisėtu tikslu, o duomenų tvarkymas atitinka proporcingumo ir subsidiarumo principus.

Pavyzdys

Transporto įmonė visų savo transporto priemonių salonuose sumontuoja vaizdo kamerą, įrašančią garsą ir vaizdą. Šių duomenų tvarkymo tikslas – gerinti darbuotojų vairavimo gebėjimus. Kameros sukonfigūruojamos taip, kad saugotų įrašus, kai įvyksta tokie incidentai kaip staigus stabdymas arba staigus krypties pasikeitimas. Įmonė daro prielaidą, kad ji turi teisinį pagrindą tvarkyti duomenis, pagal direktyvos 7 straipsnio f punktą siekdama savo teisėtų interesų užtikrinti savo darbuotojų ir kitų vairuotojų saugą.

[21] WP29 *Nuomonė 13/2011 dėl išmaniuosiuose mobiliuosiuose įrenginiuose įdiegtų geografinės buvimo vietos nustatymo paslaugų,* WP185, 2011 m. gegužės 16 d., url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_lt.pdf.

[22] WP29, *Nuomonė 5/2005 dėl vietos nustatymo duomenų naudojimo siekiant teikti pridėtinės vertės paslaugas,* WP115, 2005 m. lapkričio 25 d., url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp115_lt.pdf

Tačiau įmonės teisėti interesai stebėti vairuotojus nėra viršesni už tų vairuotojų teises apsaugoti savo asmens duomenis. Nuolatinė darbuotojų stebėsena tokiomis kameromis yra didelis jų teisės į privatumą pažeidimas. Esama kitų metodų (pvz., sumontuoti įrangą, neleidžiančią naudotis mobiliaisiais telefonais) ir kitų saugos sistemų, pvz., aukštesnio lygio avarinio stabdymo sistema (AEBS) arba įspėjimo apie nukrypimą nuo eismo juostos sistema, kurią galima naudoti transporto priemonių avarijoms išvengti – jos gali būti tinkamesnės. Be to, yra didelė tikimybė, kad dėl tokio vaizdo įrašo bus tvarkomi trečiųjų šalių (pvz., pėsčiųjų) asmens duomenys, o tokiam duomenų tvarkymui pagrįsti teisėtų įmonės interesų nepakanka.

5.8. Duomenų tvarkymo operacijos, kurias vykdant darbuotojų duomenys atskleidžiami trečiosioms šalims

Įmonės ima vis dažniau perduoti savo klientams savo darbuotojų duomenis, kad užtikrintų patikimą paslaugų teikimą. Priklausomai nuo teikiamų paslaugų masto, šie duomenys gali būti visiškai nereikalingi (pvz., gali būti pateikiama darbuotojo nuotrauka). Tačiau, atsižvelgiant į galios disbalansą, darbuotojai neturi galimybės savanoriškai sutikti dėl darbdavio vykdomo jų asmens duomenų tvarkymo, o jeigu duomenų tvarkymas nėra proporcingas, darbdavys neturi teisinio pagrindo tai daryti.

Pavyzdys:

Pristatymo įmonė siunčia savo klientams e. laišką, kuriame yra nurodytas pristatymą vykdančio asmens (darbuotojo) vardas, pavardė ir buvimo vieta. Įmonė taip pat ketino pateikti pristatymą vykdančio asmens paso nuotrauką. Įmonė darė prielaidą, kad ji turi teisinį pagrindą tvarkyti duomenis siekdama savo teisėtų interesų (direktyvos 7 straipsnio f punktas), sudarydama sąlygas klientui patikrinti, ar pristatymą vykdantis asmuo iš tikrųjų yra tas asmuo.

Tačiau nurodyti klientams pristatymą vykdančio asmens vardą, pavardę ir nuotrauką nėra reikalinga. Kadangi šis duomenų tvarkymas neturi jokio kito teisėto pagrindo, pristatymo įmonei neleidžiama teikti klientams šių asmens duomenų.

5.9. Duomenų tvarkymo operacijos, kurias vykdant tarptautiniu mastu perduodami duomenys apie žmogiškuosius išteklius ir kiti darbuotojų duomenys

Darbdaviai vis dažniau naudojasi debesijos programomis ir paslaugomis, pvz., skirtomis žmogiškųjų išteklių duomenims tvarkyti, taip pat internetinėmis biuro programomis. Naudojantis dauguma šių programų darbuotojų siunčiami duomenys ir duomenys apie juos bus perduodami tarptautiniu mastu. Kaip pirmiau bendrai išdėstyta Nuomonėje 08/2001, direktyvos 25 straipsnyje teigiama, kad asmens duomenys į trečiąją šalį už ES ribų gali būti perduodami tik tuo atveju, jeigu ta trečioji šalis užtikrina adekvatų apsaugos lygį. Kad ir koks būtų pagrindas, duomenų perdavimas turėtų atitikti direktyvos nuostatas.

Taigi, turėtų būti užtikrinta, kad būtų laikomasi šių nuostatų dėl tarptautinio duomenų perdavimo. WP29 pakartoja ankstesnę savo poziciją, kad geriau remtis tinkama apsauga, o ne Duomenų apsaugos direktyvos 26 straipsnyje išvardytais nukrypimais; jeigu remiamasi sutikimu, jis turi būti konkretus, vienareikšmiškas ir duotas savanoriškai. Vis dėlto taip pat turėtų būti užtikrinta, kad duomenų, kuriais keičiamasi už ES ir (arba) EEE ribų, kiekis ir tolesnė tos pačios grupės kitų subjektų prieiga prie tų duomenų neviršytų to, kas reikalinga nustatytiems tikslams pasiekti.

6. Išvados ir rekomendacijos

6.1. Pagrindinės teisės

Minėtų ryšių turiniui ir su jais susijusiems srauto duomenims taikoma tokia pati pagrindinių teisių apsauga kaip ir *analoginiams* ryšiams.

Iš verslo patalpų vykdomiems elektroniniams ryšiams gali būti taikomos *privataus gyvenimo* ir *korespondencijos* sąvokos pagal Europos konvencijos 8 straipsnio 1 dalį. Remdamiesi dabartine Duomenų apsaugos direktyva, darbdaviai duomenis gali rinkti tik teisėtais tikslais, kai duomenys tvarkomi tinkamomis sąlygomis (pvz., duomenų tvarkymas yra proporcingas ir reikalingas, juo siekiama tikrų dabartinių interesų, jis vykdomas teisėtais, aiškiai suformuluotais ir skaidriais metodais), turėdami teisinį pagrindą tvarkyti asmens duomenis, surinktus iš elektroninių ryšių arba per juos.

Tai, kad elektroninių priemonių nuosavybės teisė priklauso darbdaviui, nepanaikina darbuotojų teisės į savo ryšių, atitinkamų buvimo vietos duomenų ir korespondencijos slaptumą. Darbuotojų buvimo vietos sekimas per jiems patiems nuosavybės teise priklausančius ar įmonės išduotus įrenginius turėtų būti vykdomas tik tais atvejais, kai tai būtinai reikalinga teisėtam tikslui pasiekti. Žinoma, jeigu taikoma asmeninių įrenginių naudojimo politika, svarbu, kad darbuotojams būtų suteikta galimybė savo asmeninius ryšius apsaugoti nuo bet kokios su darbu susijusios stebėsenos.

6.2. Sutikimas; teisėti interesai

Darbuotojai beveik niekada neturi galimybės savanoriškai duoti, atsisakyti duoti ar atšaukti sutikimą, nes darbdavio ir darbuotojo santykiai lemia priklausomybę. Dėl galios disbalanso darbuotojai savanorišką sutikimą gali duoti tik išimtinėmis aplinkybėmis, kai nėra visiškai jokių su pasiūlymo priėmimu ar atmetimu susijusių padarinių.

Kartais kaip teisiniu pagrindu galima pasinaudoti darbdavių teisėtais interesais, tačiau tik tuo atveju, kai duomenų tvarkymas yra griežtai būtinas teisėtu tikslu ir atitinka proporcingumo ir subsidiarumo principus. Prieš pradedant naudoti bet kurią stebėsenos priemonę, turėtų būti atliktas proporcingumo patikrinimas siekiant apsvarstyti, ar visi duomenys yra reikalingi, ar šis duomenų tvarkymas yra svarbesnis už bendrąsias darbuotojų teises į privatumą darbo vietoje ir kokių priemonių turi būti imamasi siekiant užtikrinti, kad būtų kuo mažiau pažeidžiama teisė į privatų gyvenimą ir teisė į ryšių slaptumą.

6.3. Skaidrumas

Darbuotojai turėtų būti veiksmingai informuojami apie bet kokią vykdomą stebėseną, šios stebėsenos tikslus ir aplinkybes, taip pat apie darbuotojų galimybes užtikrinti, kad stebėsenos technologijomis nebūtų įrašyti jų duomenys. Teisėtos stebėsenos politikos priemonės ir taisyklės turi būti aiškios ir lengvai prieinamos susipažinti. Darbo grupė rekomenduoja į tokių taisyklių ir politikos priemonių kūrimą ir vertinimą įtraukti reprezentatyvią darbuotojų imtį, nes dauguma stebėsenos priemonių gali būti pažeidžiama darbuotojų teisė į privatų gyvenimą.

6.4. Proporcingumas ir duomenų kiekio mažinimas

Duomenų tvarkymas darbe turi būti proporcingas atsakas į darbdavio patiriamus pavojus. Pavyzdžiui, netinkamo interneto naudojimo atvejus galima aptikti nebūtinai analizuojant svetainių turinį. Jeigu netinkamam naudojimui galima užkirsti kelią (pvz., naudojant interneto filtrus), darbdavys neturi bendros teisės vykdyti stebėseną.

Be to, visa apimantis draudimas naudotis ryšių priemonėmis asmeniniais tikslais yra nepraktiškas ir jo laikymuisi užtikrinti gali prireikti neproporcingos stebėsenos. Prevencijai turėtų būti skiriama daugiau dėmesio negu aptikimui – darbdavio interesai geriau įgyvendinami techninėmis priemonėmis užkertant kelią netinkamam interneto naudojimui, o ne plečiant išteklius netinkamo naudojimo atvejams aptikti.

Turėtų būti kuo labiau sumažintas nuolatinės stebėsenos metu registruojamos informacijos kiekis ir darbdaviui rodomos informacijos kiekis. Darbuotojai turėtų turėti galimybę laikinai išjungti buvimo vietos sekimą, jeigu tai yra pagrįsta atsižvelgiant į aplinkybes. Pavyzdžiui, transporto priemonių sekimo sprendimai gali būti sukurti taip, kad padėties duomenys būtų registruojami jų nepateikiant darbdaviui.

Spręsdami dėl naujų technologijų panaudojimo darbdaviai turi atsižvelgti į duomenų kiekio mažinimo principą. Informacija turėtų būti saugoma trumpiausią būtiną laiką ir turėtų būti nurodytas jos saugojimo laikotarpis. Kai informacijos nebereikia, ji turėtų būti iš karto ištrinama.

6.5. Debesijos paslaugos, internetinės programos ir tarptautinis duomenų perdavimas

Tais atvejais, kai tikimasi, kad darbuotojai naudosis asmens duomenis tvarkančiomis internetinėmis programomis (pvz., internetinėmis biuro programomis), darbdaviai turėtų apsvarstyti galimybę sudaryti darbuotojams sąlygas nusistatyti tam tikras privačias erdves, prie kurių darbdavys negalėtų prisijungti jokiomis aplinkybėmis, pvz., privatų pašto arba dokumentų katalogą.

Naudojantis dauguma debesijos programų darbuotojų duomenys bus perduodami tarptautiniu mastu. Turėtų būti užtikrinta, kad į ES nepriklausančią trečiąją šalį asmens duomenys būtų perduodami tik tokiu atveju, jeigu užtikrinama pakankamo lygio apsauga, ir kad duomenys, kuriais keičiamasi už ES ir (arba) EEE ribų, ir tolesnė tos pačios grupės kitų subjektų prieiga prie tų duomenų neviršytų to, kas reikalinga nustatytiems tikslams pasiekti.

* * *

Priimta Briuselyje 2017 m. birželio 8 d.

Darbo grupės vardu
Pirmininkė
Isabelle FALQUE-PIERROTIN