



**5401/01/EN/Galutinis
WP 55**

Darbinis dokumentas

Dėl elektroninės komunikacijos sekimo darbo vietoje

Priimta 2002 m. gegužės 29 d.

Komentariai:

* nacionaliniai paragrafai gali būti keičiami suderinus su nacionalinėmis delegacijomis.

Darbo grupė buvo įkurta vadovaujantis Direktyvos 95/46/EB 29 straipsniu. Tai nepriklausomas Europos patariamasis organas duomenų apsaugos ir privatumo klausimais. Jos uždaviniai aprašyti Direktyvos 95/46/EB 30 straipsnyje ir Direktyvos 97/66/EB 14-ame straipsnyje.

Sekretoriatą teikia Europos Komisijos Direktoratas A (funkcionuojantis ir įtakojamas vieningos rinkos – koordinavimo – duomenų apsaugos), Internal Market Directorate-General, B-1049 Brussels, Belgium, Office No C100-6/136.

ASMENŲ APSAUGOS DĖL ASMENS DUOMENŲ TVARKYMO DARBO GRUPĖ

Įkurta vadovaujantis Europos Parlamento ir Tarybos 1995 m. spalio 24 d. Direktyva 95/46/EB¹,

atsižvelgdama į Direktyvos 29 ir 30 straipsnių paragrafus 1 (a) ir 3,

atsižvelgdama į jos Procedūros taisykles, ypač į jos 12 ir 14 straipsnius,

priėmė šį darbinį dokumentą:

¹ Official Journal no. L 281 of 23/11/1995, p. 31, prienamas adresu:

http://europa.eu.int/comm/internal_market/en/dataprot/index.htm

29 straipsnio darbo grupės darbinis dokumentas² dėl elektroninių komunikacijų stebėjimo darbo vietoje

Dokumento santrauka

Šis darbinis dokumentas papildo 2001/8 nuomonę dėl asmens duomenų tvarkymo darbo santykių kontekste³ ir pagerina unifikuotų nacionalinių priemonių taikymą, nustatytą Duomenų apsaugos Direktyvoje 95/46/EB⁴. Jis netrukdo nacionalinės teisės taikymui su duomenų apsauga susijusiose srityse.

29 straipsnio Darbo grupė sudarė subgrupę siekiant išnagrinėti šį klausimą⁵ ir priėmė **išsamų dokumentą**, kuris gali būti surastas internete šiuo adresu⁶:

http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/index.htm

29 straipsnio Darbo grupė šiame darbiniam dokumente išnagrinėjo klausimą dėl elektroninės komunikacijos darbo vietoje stebėjimo ir sekimo, kitaip tariant, darbdavio veiksmus stebint, kaip darbuotojai naudojami elektroniniu paštu ir internetu.

Europos Žmogaus teisių teismo jurisprudencijos dėl Žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos 8 straipsnio bei kitų susijusių tarptautinių tekstų ir Direktyvos 95/46/EB priemonių šviesoje, šis darbinis dokumentas pateikia nuorodas ir konkrečius pavyzdžius apie tai, kas sudaro teisėtus stebėjimo veiksmus bei priimtinas darbuotojo stebėjimo ribas. Atkreipkite dėmesį, kad kai kuriose šalyse narėse teisės aktai gali nustatyti aukštesnius apsaugos standartus nei nurodyta šiame darbiniam dokumente.

Darbuotojai nepraranda savo teisės į privatumą ir duomenų apsaugą kas rytą atverdami darbovietės duris. Jie teisėtai gali tikėtis tam tikro privatumo lygio darbo

² 29 straipsnio Darbo grupė yra patariamoji grupė, sudaryta iš šalių narių duomenų apsaugos institucijų atstovų, kuri veikia nepriklausomai ir, be kita ko, turi užduotį spręsti bet kurį klausimą, susijusį su nacionalinių priemonių, priimtų vadovaujantis Duomenų apsaugos direktyva, taikymu, siekiant pagerinti unifikuotą tokių priemonių taikymą.

³ Nuomonė patvirtinta 2001 m. rugsėjo 13 d. ir prieinama adresu: http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp48en.pdf. Nuomonėje yra išsami analizė dėl Duomenų apsaugos direktyvos priemonių taikymo (ypač dėl 6, 7 ir 8 straipsnių) asmens duomenų tvarkymui su darbo santykiais susijusioje veikloje.

⁴ Europos Parlamento ir Tarybos 1995 m. spalio 24 d. Direktyva 95/46/EB dėl asmens apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo. OJ L 281, 23.11.95, p. 31

⁵ Šios priežiūros institucijos prisidėjo prie subgrupės darbo: AT, BE, DE, EL, EN, FR, IR, IT, NL, UK.

⁶ Prie dokumento yra priedas, kuriame surašyti labiausiai su duomenų apsauga susiję šalių narių teisės aktai drauge su jų įtaka elektroninės komunikacijos darbo vietoje sekimui ir priežiūrai.

vietoje, kadangi svarbią santykių su kitais asmenimis dalį jie įgyvendina darbovietėje. Tačiau ši teisė turi būti subalansuota su kitomis teisėmis ir teisėtais interesais, ypač darbdavio teise efektyviai vykdyti veiklą iki tam tikro laipsnio, ir, be kita ko, apsaugoti save nuo atsakomybės ar žalos, kurią gali sukelti darbuotojo veiksmai. Šios teisės ir interesai sudaro teisėtą pagrindą, kuris gali pateisinti tam tikras priemones, apribojančias darbuotojo teisę į privatumą. Aiškiausias pavyzdys būtų atvejai, kai darbdavys yra darbuotojo kriminalinio nusikaltimo auka.

Tačiau skirtingų teisių ir interesų subalansavimas reikalauja atsižvelgimo į daugybę principų, ypač į proporcingumo principą. Turi būti aišku, kad paprastas faktas, jog stebėjimas ar sekimas laikomas patogu siekiant įgyvendinti darbdavio interesus nepateisins jokios intervencijos į darbuotojo privatumą. Prieš įdiegiant bet kokią stebėjimo priemonę darbo vietoje, ji turi praeiti aibę testų, kurie išsamiai aprašomi šiem darbiniame dokumente.

Šie klausimai gali apibendrinti tokio įvertinimo pobūdį:

- a) Ar stebėjimo veikla skaidri darbuotojams?
- b) Ar ji būtina? Ar darbdavys negali pasiekti to paties rezultato tradiciniais priežiūros metodais?
- c) Ar asmens duomenų tvarkymas sąžiningai pasiūlytas darbuotojams?
- d) Ar jis proporcingas problemoms, kurias siekia išspręsti?

Sutelkiant dėmesį į praktinį šių principų pritaikymą, darbinis dokumentas pateikia nuorodas dėl minimalaus įmonių elektroninio pašto ir interneto naudojimo taisyklių turinio, kurį darbdaviai ir darbuotojai gali naudoti kaip pagrindą tolesniam tobulinimui (atsižvelgdami į konkrečios įmonės ypatumus, jos dydį ir nacionalinius su duomenų apsauga susijusius teisės aktus).

Svarstant interneto vartojimą asmeniniais tikslais, 29 straipsnio Darbo grupė laikosi nuomonės, kad prevencija turi būti svarbesnė nei identifikavimas, kitaip tariant, darbdavio interesai yra tenkinami geriau imantis prevencinių priemonių neteislingam interneto vartojimui, nei nustatant tokį vartojimą. Šiame kontekste ypač naudingi technologiniai sprendimai. Besąlygiškas darbdavių draudimas naudotis internetu asmeniniais tikslais nėra pagrįstas ir nenusako laipsnio, kuriuo internetas gali pasitarnauti darbuotojams jų kasdieniniame gyvenime.

Darbo grupė norėtų pabrėžti, jog labai svarbu, kad darbdaviai informuotų darbuotoją dėl (i) bet kokios identifikavimo įrangos ir/ar aparatūros, aktyvuotos priklausomai nuo darbuotojo darbo statuso, buvimo, naudojimo ir jo tikslo ir (ii) bet kokio neteisingo elektroninės komunikacijos (internetu ar elektroninio pašto) naudojimo identifikavimo, nebent svarbios priežastys pateisina slapto sekimo teisimą⁷, kas nėra įprastas atvejis. Greita informacija gali būti nesunkiai perduodama programine įranga, pvz., išpėjantys langai, kurie iššoka kaip pranešimas darbuotojui, jog sistema nustatė neleistiną tinklo naudojimą ir/ar ėmėsi tolesnių veiksmų jo prevencijai.

⁷ Pagrįsto užslėpto stebėjimo atvejai yra tinkamas pavyzdys.

Praktiškai darbdaviai galėtų apvarstyti, ar neverta darbuotojams suteikti dviejų elektroninio pašto dėžučių.

- a) vieną dėžutę išimtinai profesiniais tikslais, kurioje stebėjimas, apsiribojantis šiame darbiniam dokumente nustatytais atvejais būtų galimas.
- b) kitą dėžutę išimtinai asmeniniais tikslais (ar autorizacijos kodą interneto naudojimui); ji būtų apsaugota tik įprastomis priemonėmis, ir tikrinama dėl neteisingo naudojimo tik išimtiniais atvejais.

29 straipsnio Darbo grupė pastebėjo kai kuriuos neatitikimus tarp nacionalinių su duomenų apsauga susijusių teisės aktų, dažniausiai analizuodama leistinus nukrypimus nuo pagrindinių teisių į korespondencijos slaptumą, bei susijusius su kolektyvinio darbuotojo veiklos ir sprendimų priėmimo pobūdžio apimtimi ir efektu. Nežiūrint to, 29 straipsnio Darbo grupė nepastebėjo nukrypimų tarp nacionalinių teisės aktų duomenų apsaugos srityje, kurie galėtų būti pagrindiniais trukdžiais vieningai praktikai, ir dėl to išleido šį darbinį dokumentą, kuris bus peržiūrėtas 2002-2003 metais, atsižvelgiant į praktinę patirtį ir naujus pasiekimus šioje srityje.

1. SEKIMAS DARBO VIETOJE. IŠŠŪKIS VISUOMENEI.

Darbuotojų sekimas neseniai sulaukė daug spaudos dėmesio, ir šiuo metu dėl to vyksta vieši debatai Bendrijoje. Iš tiesų, palaipsnis temos dėl elektroninio pašto darbo vietoje naudojimo įvedimas į Bendriją pritraukė tiek darbdavių, tiek darbuotojų, nerimaujančių dėl invazijos į jų privatumą darbo vietoje rizikos, dėmesį.

Svarstant sekimo klausimą, nuolat reikia turėti omeny, kad tuo tarpu, kai darbuotojai turi teisę į tam tikrą privatumo laipsnį darbo vietoje, ši teisė turi būti subalansuota su darbdavio teise kontroliuoti savo verslo funkcionavimą ir apginti save nuo darbuotojų veiksmų, kurie galėtų pažeisti teisėtus darbdavio interesus, pvz., jei darbdavys prisiima atsakomybę už darbuotojo veiksmus.

Kol naujos technologijos sudaro teigiamą išteklių, prieinamų darbdaviams, vystymąsi, elektroninio sekimo priemonės sudaro galimybę naudoti jas taip, kad būtų pažeistos pagrindinės darbuotojų teisės ir laisvės. Neturi būti pamiršta, kad sulig informacinių technologijų atėjimu be galo svarbu, kad darbuotojai turėtų tas pačias teises nepriklausomai nuo to, ar jie dirba internetinėje aplinkoje, ar ne.

Papildomai turi būti pabrėžta, kad darbo sąlygos vystėsi tokia linkme, jog šiandien tampa vis sudėtingiau aiškiai atskirti darbo valandas nuo privataus gyvenimo. Ypač kai vystosi "namų biuras", daugybė darbuotojų tęsia darbą namuose, naudodami kompiuterinę įrangą suteiktą darbdavio tam ar kitam tikslui.

Darbuotojo asmens orumas nusveria visus kitus argumentus. Svarstant šį klausimą svarbu turėti šį faktą omenyje, kaip ir neigiamas pasekmes, kurias kai kurie veiksmai gali turėti darbuotojų santykių su darbdaviu kokybei ir pačiam jų darbui.

Išvardintų faktorių šviesoje nenuostabu, kad šis klausimas yra pirmose viešų debatų linijose, ir svarbu kuo skubiau sukurti vieningą Direktyvos 95/46/EB nuostatų interpretaciją ir jas perimančią nacionalinę teisę, atsižvelgiant į naujausią Europos Žmogaus teisių teismo jurisprudenciją.

Dėl to darbo grupė manė, jog būtų naudinga suteikti toliau sekančią informaciją ir pristatyti darbinis dokumentus visuomenei ir privačiam sektoriui. Turi būti pažymėta, jog šio darbinio dokumento prerogatyva – bet kokia veikla, susijusi su elektroninės informacijos darbo vietoje sekimu, taikoma tiek sekimui esamuoju laiku, tiek priėjimui prie išsaugotų duomenų.

2. TARPTAUTINIAI TEISINIAI INSTRUMENTAI

2.1 EUROPOS KONVENCIJOS DĖL ŽMOGAUS TEISIŲ IR PAGRINDINIŲ LAISVIŲ APSAUGOS 8-AS IR 10-AS STRAIPSNIAI

8-as straipsnis.

1. Kiekvienas turi teisę į savo privataus ir šeimos gyvenimo, savo namų ir korespondencijos gerbimą.
2. Neturi būti jokio viešosios institucijos įsikišimo į šios teisės įgyvendinimą, iškirus atvejus, kai tai atitinka įstatymus ir yra būtina demokratinėje visuomenėje nacionalinio saugumo, visuomenės saugumo ir ekonominės šalies gerovės, nusikaltimo ar tvarkos pažeidimo prevencijos, sveikatos ir moralės apsaugos ar kitų teisių ir laisvių apsaugos tikslais.

10-as straipsnis.

1. Kiekvienas turi teisę į žodžio laisvę. Į šią teisę įeina teisė laikytis nuomonės ir gauti ar skleisti informaciją ar idėjas be visuomeninių institucijų įsikišimo, nepriklausomai nuo valstybių ribų. Šis straipsnis nedraudžia šalims narėms reikalauti transliacijų, televizijos ir kino įmonių licencijavimo.
2. Pasinaudojimas šiomis teisėmis, kadangi jis yra susijęs su pareigomis ir atsakomybe, gali būti reglamentuojamas formalumais, sąlygomis, apribojimais ar baudomis, kaip nustatyta teisės aktais ir būtina demokratinėi visuomenei nacionalinio saugumo, teritorinio vientisumo ar visuomenės saugumo, tvarkos pažeidimo ar nusikaltimo prevencijos, sveikatos ir moralės apsaugos, kitų reputacijos ir teisių apsaugos, informacijos, gautos slaptai apsaugos ar teisėsaugos institucijų autoriteto ir nešališkumo palaikymo tikslais.

Visos šalys narės ir Europos Sąjunga yra išipareigojusios pagal Europos Žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos nuostatas. Šiomis teisėmis tradiciškai būdavo naudojamosi vertikaliai (t.y., individai priešais valstybę) ir debatai apie lygį, kuriuo šiomis teisėmis jei galėtų naudotis horizontaliai (t.y. tarp individų) tebevyksta. Tačiau akivaizdu, kad šios teisės, bendrai paėmus, egzistuoja.

Dėl to Darbo grupė laikosi nuomonės, kad svarstant nacionalinių priemonių, priimtų vadovaujantis Direktyva 95/46/EB, taikymą ir siekiant sukurti vieningą tokių priemonių taikymą, būtina atsiminti svarbiausius precedentinės teisės principus, kadangi ji šiuo metu vyrauja Europos Žmogaus teisių teisme svarstant klausimus, susijusius su šia nuostata, ir ypač klausimus, liečiančius korespondencijos slaptumą.

Šiai dienai pateiktuose vertinimuose Teismas aiškiai nustatė, kad “privataus gyvenimo” apsauga, puoselėjama 8-ame straipsnyje, nedaro išimčių privataus darbuotojo gyvenimui ir neapsiriboja vien tik apsauga jo namuose.

Niemitz prieš Vokietiją bylos pagrindas buvo apieška, kurią atliko vyriausybė institucija pareiškėjo biure. Vyriausybė bandė argumentuoti, kad 8-as straipsnis nenumato apsaugos nuo kratos kieno nors biure, kadangi Konvencija nubrėžia aiškius skirtumus tarp privataus gyvenimo ir namų iš vienos pusės, ir profesinio ar verslo gyvenimo ir patalpų iš kitos pusės.

Teismas atmetė šį požiūrį, konstatuodamas:

*Pagarba privačiam gyvenimui taip pat turi apimti tam tikro laipsnio teisę sukurti ir puoselėti santykius su kitais žmonėmis. Tokiu būdu, nėra jokios principinės priežasties, kodėl supratimas "privatus gyvenimas" neturėtų apimti profesionalios ar verslo veiklos, kadangi, galų gale, daugybė žmonių savo darbinės veiklos eigoje išnaudoja svarbią, jei ne pačią didžiausią, galimybę sukurti santykius su išoriniu pasauliu. Šis požiūris paremtas faktu, kad, kaip teisingai pažymėjo komisija, ne visada įmanoma aiškiai atskirti, kuri individo veikla sudaro jo profesinio ir verslo gyvenimo dalį, o kuri į jį neįeina."*⁸

Dar tikslesnes išvadas Teismas pateikė **Halford prieš Jungrinę Karalystę** byloje; nustatydamas, kad darbuotojo telefono skambučio perėmimas pažeidė Konvencijos 8-ą straipsnį. Įdomu tai, kad poniai Halford buvo suteikti du telefonai, iš kurių vienas buvo skirtas privačiam naudojimui. Jai nebuvo pateikta jokių apribojimų ar nuorodų dėl telefono naudojimo.

Ponia Halford pareiškė, kad jos telefono skambučio perėmimas sąlygojo Konvencijos 8-o straipsnio pažeidimą. Vyriausybė teigė, kad ponios Halford padarytiems skambučiams iš jos darbo vietos netaikoma 8 straipsnio apsauga, kadangi ji negalėjo pagrįstai tikėtis privatumo skambindama. Prieš bylos svarstymą Teisme Vyriausybės atstovas pareiškė nuomonę, kad darbdavys iš principo, be išankstinio darbuotojo įspėjimo, turi teisę stebėti pastarojo daromus skambučius telefonu, kurį jam suteikė darbdavys.

Tačiau Teismo nuomone *"pagal precedentą akivaizdu, kad skambučiai, atliekami tiek iš verslo patalpų, tiek iš namų, patenka po "privataus gyvenimo" ir "korespondencijos" sąvokomis ta prasme, kuria jos įvardinamos 8-o straipsnio 1-oje pastraipoje (...).*

*Nėra jokių įrodymų, kad ponia Halford, kaip vidinės telekomunikacijų sistemos naudotoja, buvo kaip nors įspėta, kad skambučiai, padaryti šioje sistemoje, gali būti perimti. Tokiu atveju ji, kaip nusprendė Teismas, galėjo pagrįstai tikėtis savo skambučių privatumo..."*⁹

"Korespondencijos" sąvokos supratimas apima ne tik laiškus popierine forma, bet ir kitas elektroninės komunikacijos formas, gaunamas ar sukuriamas darbo vietoje, pvz. telefono skambučius, inicijuojamus ar gaunamus verslo patalpose, ar elektroninius laiškus, gautus ar išsiųstus iš biuro kompiuterių.

Kai kurie vertintojai nurodo, jog susidaro įspūdis (nors teismo išvadoje taip nenurodoma), kad jei darbdavys iš anksto perspėja darbuotoją apie jo korespondencijos perėmimo galimybę, darbuotojas negali tikėtis privatumo, ir perėmimas nebus laikomas Konvencijos 8 straipsnio pažeidimu. Darbo grupė nemano, jog išankstinis darbuotojo įspėjimas yra pakankamas bet kokio duomenų apsaugos teisių pažeidimo pateisinimui.

Iš precedentinių bylų Europos Žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos 8 straipsnio klausimais gali būti apibendrinti trys principai:

- a) Darbuotojai gali teisėtai tikėtis privatumo darbo vietoje, ir jis nėra persveriamas fakto kad darbuotojai naudoja darbdavio komunikacinę įrangą ar kitas verslo priemones.

⁸ 1992 m. lapkričio 23 d. Serija A n° 251/B, par. 29; Pabraukta sudarytojų.

⁹ 1997 m. gegužės 1997.

Tačiau darbdaviui suteikus tinkamą informaciją darbuotojui, jo teisėti lūkesčiai dėl privatumo gali būti sumažinti.

- b) Bendrasis korespondencijos slaptumo principas apima komunikacijas darbo vietoje. Tikėtina, kad apima ir elektroninį paštą ir pridėtus su juo susijusius failus.
- c) Privataus gyvenimo gerbimas iki tam tikro laipsnio apima ir teisę sukurti bei puoselėti santykius su kitais žmonėmis. Faktas, kad tokie santykiai didele dalimi įgyvendinami darbo vietoje, apriboja teisėtą darbdavio poreikį į sekimo priemones.

10 straipsnis taip pat svarbus, tačiau ne tiek, kadangi jis apima išraiškos ir informacijos laisvę, ir pabrėžia individo teisę gauti ir skleisti informaciją ir idėjas be valstybinės institucijos įsikišimo. 10 straipsnio svarbą, panašu, atspindi Teismo svarstymai aukščiau paminėtoje Niemitz prieš Vokietiją byloje. Kaip pasakė Teismas, darbo vietoje žmonės sukuria svarbią savo santykių dalį su išoriniu pasauliu, ir dėl to jų teisė į išraiškos laisvę vaidina svarbų vaidmenį šiame kontekste.

2.2 KONVENCIJA DĖL ASMENŲ APAUGOS RYŠIUM SU ASMENS DUOMENŲ AUTOMATIZUOTU TVARKYMU (ETS NR. 108)

Konvencija buvo pasirašyta 1981 m. sausio 28 d. ir tapo pirmuoju teisiniu tarptautiniu instrumentu duomenų apsaugos srityje. Pagal šią Konvenciją, šalys privalo pereiti būtinus žingsnius nacionalinėje teisėje, kad būtų pritaikyti Konvencijoje nustatyti principai siekiant užtikrinti pagarbą visų individų pagrindinėms žmogaus teisėms, susijusioms su asmens duomenų tvarkymu, jų teritorijose.¹⁰

Kiti dokumentai, susiję su Konvencija Nr. 108 ir svarbūs nagrinėjamam klausimui, yra:

- Europos Tarybos Darbinis dokumentas (89) 2 Dėl asmens duomenų, naudojamų įdarbinimo tikslais, apsaugos¹¹,
- Europos Tarybos Darbinis dokumentas (97) 5 Dėl medicininių duomenų apsaugos¹²,
- Europos Tarybos Darbinis dokumentas (86) 1 Dėl duomenų, naudojamų socialinio saugumo tikslais, apsaugos¹³.
- Europos Tarybos Rekomendacija (95) 4 Dėl asmens duomenų apsaugos telekomunikacijų paslaugose, ypač dėl telefoninių paslaugų.

2.3. EUROPOS SĄJUNGOS PAGRINDINIŲ TEISIŲ CHARTIJA

¹⁰ Taip pat žiūrėkite Europos Tarybos rekomendaciją (89) 2 Dėl asmens duomenų, naudojamų įdarbinimo tikslais, apsaugos: <http://cm.coe.int/ta/rec/1989/89r2.htm>

¹¹ <http://cm.coe.int/ta/rec/1989/89r2.htm>

¹² <http://cm.coe.int/ta/rec/1997/97r5.html>

¹³ [http://www.legal.coe.int/dataprotection/Default.asp?fd=rec&fn=R\(86\)1E.htm](http://www.legal.coe.int/dataprotection/Default.asp?fd=rec&fn=R(86)1E.htm)

7-as straipsnis. Pagarba privačiam ir šeimyniniam gyvenimui.

Kiekvienas turi teisę į savo privataus ir šeimyninio gyvenimo, namų ir korespondencijos gerbimą.

8-as straipsnis. Asmens duomenų apsauga.

- 1. Kiekvienas turi teisę į su juo susijusių asmens duomenų apsaugą.*
- 2. Tokie duomenys turi būti tvarkos sąžiningai, iš anksto nustatytais tikslais, atsižvelgiant į konkretaus asmens aplinkybes ar kitus pagrindus, nustatytus teisės aktuose. Kiekvienas turi teisę priėti prie surinktų su juo susijusių duomenų, bei teisę į duomenų ištaisymą.*
- 3. Atitikimą šioms taisyklėms kontroliuoja nepriklausoma institucija.*

Europos Sąjungos Pagrindinių teisių chartija, iš visko sprendžiant, laikosi pagrindinių ECHR krypties, o korespondencijos slaptumo koncepcija buvo praplėsta, ir tapo naujosios kartos koncepcija “komunikacijos slaptumas”, kuri siekia elektroninei komunikacijai suteikti tą patį apsaugos laipsnį, kokį tradiciškai turėjo paštas.

Papildomai, 8-as straipsnis, suteikdamas duomenų apsaugai visiškai kitokį pobūdį, papildo duomenų apsaugą, suteiktą 7-uoju straipsniu. Šis rezultatas yra ypatingai svarbus kalbant apie elektroninio pašto stebėjimą.

2.4. TARPTAUTINĖ DARBO ORGANIZACIJA (TDO)

Tarptautinės darbo organizacijos praktikos kodeksas numato darbuotojų asmens duomenų apsaugą (1997).

"5. Bendrieji principai

- 5.1. Asmens duomenys turi būti tvarkomi teisėtai ir sąžiningai, ir tik tiesiogiai su darbuotojo įdarbinimu susijusiais tikslais.*
- 5.2. Iš principo, asmens duomenys turi būti naudojami tik tais tikslais, kuriais jie nuo pat pradžių buvo surinkti.*
- 5.3. Jei asmens duomenis ketinama tvarkyti kitais tikslais, nei jie buvo surinkti, darbdavys turi užtikrinti, kad jie nėra naudojami su pradiniu tikslu nesuderinamu būdu, bei turi imtis būtinų priemonių, kad būtų išvengta neteisingo duomenų interpretavimo pasikeitus jų tvarkymo kontekstui.*
- 5.4. Asmens duomenys, surinkti techninėmis ar organizacinėmis priemonėmis siekiant užtikrinti automatinių informacinių sistemų saugumą ir tinkamą veikimą, neturi būti naudojami darbuotojų elgesio kontrolės tikslais.*
- 5.5. Sprendimai, susiję su darbuotoju, neturi būti paremti vien automatiniu darbuotojo duomenų apdorojimu.*
- 5.6. Asmens duomenys, surinkti elektroninio stebėjimo būdu, neturi būti vieninteliai darbuotojo veiklos įvertinimo faktoriai (...)*

6.14.

(1) *Jei darbuotojai yra stebimi, jie turi būti iš anksto informuoti apie stebėjimo priežastis, grafiką, duomenų rinkimo duomenų rinkimo metodą ir technologijas, duomenis, kuriuos ketinama surinkti; darbdavys turi užtikrinti, kad įsikišimas į darbuotojų privatumą būtų minimalus.*

(2) *Slaptas stebėjimas leidžiamas tik tuomet, kai:*

a) jis atitinka nacionalinius teisės aktus, arba

b) yra rimtas pagrindas įtarti kriminalinę veiklą ar kitas rimtas nesąžiningas veikas.

(3) *Nuolatinis stebėjimas leidžiamas tik tuomet, kai jis būtinas sveikatai ir saugumui ar nuosavybės apsaugai (...)*

12.2. *Darbuotojų atstovai, ten, kur jie yra, atitinkamai nacionaliniams teisės aktams ir praktikai turi būti informuojami ir konsultuojami:*

a) automatinių sistemų, tvarkančių darbuotojų asmens duomenis, įvedimo ar modifikavimo klausimais,

b) prieš įvedant bet kokį elektroninį darbuotojo elgsenos stebėjimą darbo vietoje,

c) apie apklausų ar testų, susijusių su darbuotojų asmens duomenimis, administravimo ir interpretavimo tikslus, turinį ir pobūdį".

3. ELEKTRONINĖS KOMUNIKACIJOS DARBO VIETOJE SEKIMAS IR STEBĖJIMAS PAGAL DIREKTYVĄ 95/46/EB

Šis darbinis dokumentas paremtas principų, išdėstytų Direktyvoje 95/46/EB pritaikymu nagrinėjamam klausimui, atsižvelgiant į Europos Žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos 8-ą straipsnį, reikalaujantį pagarbos korespondencijai ir privačiam gyvenimui.

Yra daugybė sekimo formų, prieinamų darbdaviams darbo vietoje, ir kiekviena jų sukuria individualias problemas. Dvi formos, kurioms taikomi panašūs principai, bus nagrinėjamos šiame dokumente: tai elektroninio pašto stebėjimas ir prisijungimo prie interneto sekimas.

Pradėti reikėtų nuo punktų, nurodytų Nuomonėje 8/2001, patvirtinimo, kad Direktyva 95/46/EB taikoma asmens duomenų tvarkymui įdarbinimo kontekste taip pat, kaip ir bet kuriame kitame kontekste¹⁴. Papildomai bendrajai Direktyvai 95/46/EC, Direktyva 97/66/EB Dėl asmens duomenų tvarkymo ir privatumo apsaugos telekomunikacijų sektoriuje taip pat gali būti svarbi. Ši Direktyva detalizuoja ir papildo Direktyvą 95/46/EB dėl asmens duomenų tvarkymo telekomunikacijų sektoriuje. Elektroninės komunikacijos stebėjimas, įskaitant elektroninį pašta ir prisijungimą prie interneto, patenka tiek į Direktyvos 95/46/EB prerogatyvą, tiek gali patekti į Direktyvos 97/66/EB, kuri šiuo metu peržiūrima dėl Bendrijos teisės aktų telekomunikacijų sektoriuje pakeitimų, prerogatyvą. Tais atvejais, kai taikoma ši Direktyva, jos 5-as straipsnis (dėl komunikacijų konfidencialumo) ir 6-as straipsnis (dėl duomenų judėjimo ir sąskaitų išrašymo) gali būti ypatingai svarbūs.

3.1 BENDRIEJI PRINCIPAI, TAIKOMI ELEKTRONINIO PAŠTO IR INTERNETO STEBĖJIMUI

Toliau aprašomi duomenų apsaugos principai yra išvesti iš Direktyvos 95/46/EB, ir jų turi būti laikomasi svarstant asmens duomenų tvarkymą, kuris įeina į tokį stebėjimą. Visų toliau aprašomų principų laikymasis yra būtinas bet kokiai stebėjimo veiklai, kad ji būtų teisėta ir pagrįsta.

3.1.1. BŪTINUMAS

Šis principas reiškia, kad darbdavys turi įsitikinti, kad bet kokia stebėjimo forma yra neišvengiamai būtina nustatytam tikslui prieš pradėdamas tokią veiklą. Tradiciniai priežiūros metodai, mažiau pažeidžiantys į individų privatumą, turi būti detalčiai apsvarstomi, ir kur įmanoma, pritaikyti prieš pradėdamas elektroninės komunikacijos stebėjimą.

Tik išimtinėmis aplinkybėmis darbuotojų pašto ar interneto naudojimo stebėjimas gali būti laikomas būtinu. Pavyzdžiui, darbuotojo elektroninio pašto stebėjimas gali tapti būtinas siekiant gauti patvirtinimą ar įrodymą tam tikriems darbuotojo veiksams. Tokiais veiksmais laikoma kriminalinė veikla iš darbuotojo pusės, kai darbdaviui reikia ginti savo interesus, pavyzdžiui, jei jis atsakingas už darbuotojo veiksmų padarinius.

¹⁴ http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp48en.pdf

Taip pat galima veikla, siekiant nustatyti virusus, ir apskritai bet kokia darbdavio veikla, siekiant garantuoti sistemos saugumą.

Turi būti pažymėta, kad darbuotojo elektroninio pašto atidarymas gali būti būtinas kitais nei stebėjimas ar sekimas tikslais, pvz. siekiant palaikyti korespondenciją, kai darbuotojas yra išvykęs iš biuro (pvz. serga ar atostogauja), ir korespondencija negali būti garantuota kitais būdais (pvz. auto atsakovu ar automatiniu persiuntimu).

Būtinumo principas taip pat reiškia, kad darbdavys turi saugoti duomenis tik ne ilgiau, nei jie yra būtini nustatytam stebėjimo veiklos tikslui pasiekti.

3.1.2. BAIGTINUMAS

Šis principas reiškia, kad duomenys turi būti renkami nustatytam, aiškiam ir teisėtam tikslui, ir neturi būti toliau tvarkomi būdu, neatitinkančiu šių tikslų. Šiame kontekste "atitikimo" principas reiškia, pvz., kad jei duomenų tvarkymas yra pagrįstas sistemos saugumo pagrindu, šie duomenys negali būti tvarkomi kitu tikslu, tarkim darbuotojo elgsenos stebėjimu.

3.1.3. SKAIDRUMAS

Šis principas reiškia, kad darbdavys turi būti atviras ir vykdyti aiškia veiklą. Tai reiškia, kad neleidžiamas joks paslėptas elektroninio pašto stebėjimas, išskyrus atvejus, esant kuriems stebėjimas leidžiamas pagal nacionalinę teisę, atitinkančia Direktyvos 13-ą straipsnį¹⁵. Labiausiai tikėtina, kad tai bus atvejai, kai identifikuota tam tikra kriminalinė veikla (būtina gauti įrodymus pagal teisinės ir procedūrinės šalių narių taisykles) arba atvejai, kai nacionalinė teisė numato būtinus saugiklius, leidžiančius darbdaviui imti tam tikrų veiksmų siekiant nustatyti pažeidimus darbo vietoje.

Toliau šis principas gali būti išskiriamas į du aspektus:

3.1.3.1. PRIEVOLE SUTEIKTI INFORMACIJĄ DUOMENŲ SUBJEKTUI

Tai ko gero labiausiai tinkamas pavyzdys, iliustruojantis skaidrumo principą praktikoje, nagrinėjant šį klausimą. Tai reiškia, kad darbdavys turi pateikti darbuotojams laisvai prieinamą, aiškų ir tikslų pareiškimą apie savo politiką elektroninio pašto ir interneto stebėjimo atžvilgiu.

Darbuotojams turi būti suteikta pilna informacija, kokios specifinės aplinkybės pateisins tokias išskirtines priemones, kokie bus tokios tebejimo mastai. Informacija turi turėti šiuos elementus:

1. Elektroninio pašto/interneto politika kompanijoje, detaliam aprašant mastą, kuriuo kompanijos valdomi komunikacijos įrenginiai gali būti naudojami asmeninei/privačiai darbuotojų komunikacijai (pvz., laiko ir naudojimosi trukmės apribojimai).

¹⁵ Direktyvos 13-as straipsnis leidžia Šalims narėms priimti teisinės priemones, apribojančias prievolių ir teisių mastą, numatytą konkrečiuose Direktyvos straipsniuose, kai tokie apribojimai sąlygoja būtinas priemones apsaugoti svarbius visuomenės interesus, tokius kaip nacionalinis saugumas arba kriminalių nusikaltimų prevencija, tyrimas, nustatymas ir apkalta, arba duomenų subjekto ar kitų teisių ir laisvių apsauga.

2. Priežastis ir tikslus, kuriais stebėjimas yra atliekamas, jei atliekamas. Tais atvejais, kai darbdavys leido naudotis įmonės komunikacijos įrenginiais privačiais tikslais, tokia privati komunikacija gali būti stebima tik esant labai ribotoms aplinkybėms, pvz. užtikrinti informacinės sistemos saugumą (patikrinimas nuo virusų).
3. Taikomų sekimo priemonių detales, t.y. Kas? Ką? Kaip? Kada?
4. Bet kokių priverstinių procedūrų detales, nurodant kaip ir kada darbuotojai bus perspėti apie vidinių taisyklių nesilaikymą, ir jiems bus suteikta galimybė atsakyti į bet kokius kaltinimus prieš juos.

Darbo grupė norėtų pabrėžti, kad žiūrint iš tam tikro taško, darbuotojui patartina iš karto informuoti darbuotoją apie bet koki aptiktą neteisingą elektroninės komunikacijos panaudojimą, nebent svarbios priežastys gali pateisinti sekimo tęsimą¹⁶, kas nėra įprasta. Skubi informacija gali būti lengvai perduodama programine įranga, pvz., perspėjantys langai, iššokantys ir išpėjantys darbuotoją, kad sistema nustatė neleistiną tinklo vartojimą. Gana didelė dalis nesusipratimų gali būti išspręsta šiuo būdu.

Kitas skaidrumo principo pavyzdys yra darbdavių praktika informuoti ir/ar konsultuoti darbuotojų atstovus prieš įvedant su darbuotoju susijusias taisykles. Turi būti pažymėta, kad sprendimai apie darbuotojų stebėjimą, įskaitant ir darbuotojų elektroninės komunikacijos sekimą, yra reglamentuojami neseniai priimtoje 2002/14/EB Direktyvoje, jei įmonė ar įstaiga patenka į jos taikymo sritį. Ši Direktyva numato darbuotojų informavimą ir konsultavimą dėl sprendimų, kurie, kaip tikėtina, gali sąlygoti esminius darbo organizacijos ar sutartinių sąlygų pasikeitimus. Nacionalinė teisė ar kolektyvinės sutartys gali numatyti sąlygas, kurios yra dar palankesnės darbuotojams.

Kolektyvinės sutartys gali net tik įpareigoti darbdavį informuoti ir konsultotis su darbuotojų atstovais prieš įvedant sekimo sistemas, bet ir padaryti tokį įdiegimą galimą tik turint išankstinį darbuotojų atstovų sutikimą.

Kolektyvinės sutartys taip pat gali numatyti leidžiamo darbuotojų elektroninio pašto ir interneto naudojimo laipsnį ir mastus, taip pat tokio naudojimo stebėjimo detales.

3.1.3.2. PAREIGA INFORMUOTI PRIEŽIŪROS INSTITUCIJAS PRIEŠ PRADEDANT VISIŠKAI AR IŠ DALIES AUTOMAZUOTĄ TVARKYMO OPERACIJĄ AR TOKIŲ OPERACIJŲ RINKINĮ

Tai yra kitas būdas suteikti skaidrumą, kadangi darbuotojas visada gali pasitikrinti Duomenų apsaugos registruose, pvz., kokias savo darbuotojų duomenų kategorijas, kokiais tikslais gali tvarkyti darbdavys ir kokiems duomenų gavėjams juos perduoti.

3.1.3.3. TEISĖ SUSIPAŽINTI

¹⁶ Pagrįsto paslėpto stebėjimo atvejai gali būti geras pavyzdys.

Darbuotojas, kaip bet kuris kitas asmuo pagal Direktyvą¹⁷, turi teisę susipažinti su juo susijusiais asmens duomenimis, tvarkomais jo darbdavio, ir kur reikia, reikalauti jų ištaisymo arba ištrynimo ar blokavimo tais atvejais, kai jie neatitinka Direktyvos nuostatų, paprastai dėl to, kad jie neišsamūs ar netikslūs.

Darbuotojo priėjimas prie darbdavio failų be apribojimų pagrįstais intervalais ir be per didelio delsimo ar išlaidų yra naudingas įrankis, kurį darbuotojai individualiai gali naudoti norėdami įsitikinti, kad stebėjimo veikla darbo vietoje išlieka teisėta ir sąžininga darbuotojų atžvilgiu. Tačiau priėjimas prie darbdavio failų gali būti problematiškas išimtinėmis aplinkybėmis, pavyzdžiui, priėjimas prie taip vadinamų vertinimo duomenų.

Darbo grupė jau laikosi pirmojo požiūrio šiuo klausimu¹⁸ ir ateityje gali teikti tolesnes nuorodas atsižvelgdama į patirtį.

3.1.4. TEISĖTUMAS

Šis principas reiškia, kad bet kokia duomenų tvarkymo operacija gali būti atliekama tik tada, kai ji turi teisėtą tikslą, kaip numatoma Direktyvos 7 straipsnyje ir nacionalinėje jį perkeliančioje teisėje. Direktyvos 7 (f) straipsnis yra ypatingai svarbus šiam principui ta prasme, kad tam, jog darbuotojų duomenų tvarkymas būtų leistinas pagal Direktyvą 95/46/EB, darbdavys turi nustatyti teisėtais interesais paremtus tikslus, ir jie neturi pažeisti pagrindinių darbuotojo teisių.

Darbdavio poreikis ginti savo verslą nuo esminių grėsmių, pvz., užtikrinti konfidencialios informacijos perdavimo konkurentui prevenciją, gali būti laikomas teisėtu interesu.

Ypatingų duomenų tvarkymas šiame kontekste yra labai problematiškas, kadangi Direktyvos 8-as straipsnis nenumato interesų pusiausvyros Direktyvos 7-as straipsnio reikšmės ribose. Tačiau 8-o straipsnio antrasis paragrafas, punktas b) pateikia nuorodas į "tvarkymą, būtiną išipareigojimų ir specifinių valdytojo teisių įgyvendinimo tikslais

¹⁷ 12 straipsnis. Valstybės narės garantuoja kiekvienam duomenų subjektui teisę reikalauti, kad duomenų valdytojas:

a) be apribojimų, priimtinais laiko tarpais, per daug nedelsdamas ir be pernelyg didelių išlaidų, pateiktų:

- patvirtinimą, ar su juo susiję duomenys yra tvarkomi, ir informaciją bent jau apie tvarkymo tikslus, duomenų kategorijas, gavėjus, kuriems atskleidžiami duomenys, arba jų kategorijas,

- pranešimą suprantamu pavidalu apie tvarkomus duomenis ir bet kurią prieinamą informaciją apie jų šaltinius;

- žinias apie loginius metodus, naudojamus automatiškai tvarkant duomenis apie duomenų subjektą, bent 15-o straipsnio 1-oje dalyje nurodytų automatinėlių sprendimų atveju;

b) tinkamai ištaisytų, ištrintų arba blokuotų duomenis, kurie tvarkomi nesilaikant šios direktyvos nuostatų, o ypač, kai tie duomenys yra neišsamūs ar netikslūs;

c) praneštų trečiosioms šalims, kurioms duomenys buvo atskleisti, kad pagal (b) punktą duomenys buvo ištaisyti, ištrinti ar blokuoti, nebent tai padaryti būtų neįmanoma arba pernelyg sunku.

¹⁸ Žr. rekomendaciją 1/2001 dėl darbuotojų įvertinimo duomenų.

darbo santykių teisės srityje tiek, kiek jis yra leidžiamas pagal nacionalinę teisę, suteikiančią adekvačius saugiklius".

Ypatingų duomenų tvarkymas, susijęs su stebėjimo ir sekimo veikla yra sudėtingas klausimas, ne visai susijęs su įdarbinimo kontekstu. Iš tiesų tai bendras klausimas, kuriuo Darbo grupė gali pateikti nuorodas ateityje.

Tiesą sakant, nebent nacionalinė teisė detaliai leidžia tai daryti numatant adekvačius saugiklius, stebėjimo veikla tiesiogiai siekiant darbuotojų ypatingų duomenų tvarkymo neras teisinio pagrindo pagal Direktyvos 95/46/EB nuostatas ir nebus priimtina. Tačiau imantis bet kokios stebėjimo veiklos prevencijos ar priemonių, padarančių ją labai sudėtinga (kas daugumoje atvejų yra ne tik teisėta, bet net ir pageidautina, pvz. priemonės tiesiogiai nukreiptos į sistemos saugumo garantavimą) gali būti, kad tam tikrų ypatingų duomenų tvarkymas yra neišvengiamai įtrauktas, taip pat atrodo nepriimtinas.

3.1.5. PROPORCINGUMAS

Šis principas reikalauja, kad asmens duomenys, įskaitant tuos, kurie gaunami stebint, turi būti adekvatūs, susiję ir ne pertekliniai lyginant su nustatytu siekiamu tikslu. Įmonės taisyklės šioje srityje turi būti nustatytos pagal rizikos, su kuriuo susiduria konkreči kompanija, tipą ir laipsnį.

Dėl to proporcingumo principas išstumia neatrankinį kiekvieno dirbančio individo elektroninio pašto ir interneto naudojimo stebėjimą bet kokiais tikslais išskyrus sistemos saugumo užtikrinimą. Kur nustatytas tikslas gali būti pasiektas mažiau privatumą pažeidžiančiomis priemonėmis, darbdavys turi apsvarstyti šią galimybę (pvz., jis/ji turi vengti sistemos, kuri stebi automatiškai ir nuolat).

Elektroninio pašto stebėjimas, jei įmanoma, turėtų apsiriboti dalyvių duomenų srauto ir komunikacijos laiko, o ne turinio fiksavimu, jei to pakanka darbdavio poreikių patenkinimui. Jei priėjimas prie elektroninio pašto turinio yra tikrai būtinas, turi būti atsižvelgta ne tik į organizacijos narių, bet ir į gaunančių laiškus už organizacijos ribų privatumą. Darbdavys, pavyzdžiui, negali gauti laiškų, kuriuos darbuotojui atsiunčia ne organizacijos narys, turinio. Darbdavys turi dėti pagrįstas pastangas tam, kad informuotų išorinius organizacijos asmenis apie stebėjimo veiklos egzistavimą, jei ji gali paveikti išorinius asmenis. Praktinis pavyzdys gali būti perspėjančių žinučių apie stebėjimo sistemos egzistavimą įterpimas, pridėtas prie visų iš organizacijos išėinančių žinučių.

Technologija darbdaviui suteikia daug galimybių įvertinti darbuotojų elektroninio pašto naudojimą, pvz. tikrinant išsiųstų ir gautų laiškų skaičių arba prisegtų failų formatą, ir dėl to realus elektroninio pašto atidarymas yra neproporcingas. Dar daugiau, technologija gali būti naudojama siekiant užtikrinti, kad priemonės, kurių darbdavys imasi norėdamas apsisaugoti nuo neleistino darbuotojų naudojimosi jo suteikiamais interneto kanalais, būtų proporcingos, naudojant blokavimo, o ne stebėjimo mechanizmus¹⁹.

¹⁹ Praktikoje jau galima rasti daug šios technologijos naudojimo pavyzdžių.

- Internetas: kai kurios kompanijos naudoja programinę įrangą, kuri gali būti sukonfigūruojama taip, kad blokuotų bet koki prisijungimą prie iš anksto nustatytų interneto svetainių kategorijų. Darbdavys po konsultacijų su agreguotomis svetainėmis, kurias lankė jo darbuotojai, gali nuspręsti papildyti

Elektroninės komunikacijos tvarkymo sistemos turi būti suprogramuotos taip, kad tvarkomų asmens duomenų kiekis būtų apribotas iki kraštutinio minimumo.²⁰

Svarstant proporcingumo klausimą, turi būti pabrėžta, kad kolektyvinių derybų mechanizmas gali būti labai naudingas sprendžiant, kokie veiksmai yra proporcingi darbdaviui gresiančiai rizikai. Taip gali būti pasiektas kompromisas dėl darbdavio ir darbuotojo interesų pusiausvyros.

3.1.6. TIKSLUMAS IR DUOMENŲ IŠSAUGOJIMAS

Šis principas reikalauja, kad bet kokie duomenys, sudaryti iš ar susiję su darbuotojo elektroninio pašto sąskaita ar interneto naudojimu, teisėtai saugomi darbdavio (po to, kai buvo atsižvelgta į visus kitus šiame dokumente nurodytus principus) turi būti tikslūs ir nuolat atnaujinami, bet nesaugomi ilgiau nei būtina. Darbdaviai turi nustatyti elektroninio pašto saugojimo terminą savo centriniuose serveriuose remdamiesi savo verslo poreikiais. Sunku įsivaizduoti, kad ilgesnis nei trijų mėnesių saugojimo terminas paprastai galėtų būti pagrįstas.

3.1.7. SAUGUMAS

Šis principas įpareigoja darbdavį įdiegti atitinkamas technines ir organizacines priemones siekiant užtikrinti, kad bet kokie jo saugomi asmens duomenys būtų saugūs ir apsaugoti nuo išorinio kišimosi. Jis taip pat apima darbdavio teisę saugoti savo sistemą nuo virusų ir leidžia naudoti automatinius elektroninio pašto ir tinklo duomenų srauto skanavimą.

Darbo grupė mano, kad atsižvelgiant į sistemos saugumo palaikymo svarbą, toks automatinis elektroninio pašto atidarymas nebūtų laikomas darbuotojo teisės į privatumą pažeidimu tuo atveju, jei yra įdiegti tinkami saugikliai. Pvz., darbdaviai gali pasinaudoti automatinėmis technologijomis savo saugumo interesams tenkinti nepažeisdami darbuotojo teisės į privatumą.

29 straipsnio Darbo grupė atkreipia dėmesį į sistemos administratoriaus, t.y. darbuotojo, kuris turi svarbias pareigas, susijusias su duomenų apsauga, vaidmens svarbą. Labai svarbu, kad sistemos administratorius ar bet kas kitas, kad gali prieiti prie asmens duomenų apie stebimus darbuotojus, gautų griežtus pareiginius nurodymus dėl profesinės paslapties, susijusios su slapta informacija, prie kurios jis gali prieiti.

blokuotų svetainių sąrašą naujomis (greičiausiai svetainė po pastebėjimo, kad darbuotojai prisijungė, bus blokuota, išskyrus atvejus kai darbuotojas įrodys poreikį susisiekti su svetaine).

- Elektroninis paštas: kitos kompanijos naudoja automatinio nukreipimo į izoliuotą serverį įrangą bet kokiam elektroniniam paštui, kurio dydis viršija nustatytą. Asmuo, kuriam buvo adresuotas laiškas, yra automatiškai informuojamas apie tai, kad įtartinas elektroninis laiškas buvo nukreiptas į tam tikrą serverį, ir tuo klausimu reikia kreiptis į jį.

²⁰Direktyvos 97/66 projektas, 30-a konstatuojamoji dalis.

4. ELEKTRONINIO PAŠTO STEBĖJIMAS

4.1. KORESPONDENCIJOS SLAPTUMAS

Kaip buvo paaiškinta anksčiau šiame dokumente, Darbo grupė laikosi nuomonės, kad interneto komunikacijos ir ne interneto komunikacijos situacijos neturi būti traktuojamos skirtingai be priežasties, ir tokiu būdu elektroninis paštas naudojami ta pačia pagrindinių teisių apsauga, kaip ir tradicinis “popierinis” paštas²¹. Europos Žmogaus teisių teismo jurisprudencija yra pateikusi keletą nuorodų dėl teisės į korespondencijos slaptumą demokratinėje visuomenėje taikymo. Nežiūrint to, šalių narių teisinės sistemos šį principą interpretuoja kiek skirtingai, ypač klausimus, susijusius su jo taikymu profesinei komunikacijai, tiek jos turiniui, tiek duomenų srautui. Iš duomenų apsaugos pusės tai turi reikšmingos įtakos svarstant toleruotino įsibrovimo į dabuotojo elektroninį pašta laipsnį.

29 straipsnio Darbo grupė laikosi nuomonės, kad elektroninė komunikacija, atliekama iš verslo patalpu, gali būti priskiriama “privataus gyvenimo” ir “korespondencijos” sąvokoms Europos Konvencijos 8-o straipsnio 1-o paragrafo supratimo ribose. Šiuo klausimu yra nedaug vietos interpretacijai, kadangi jis buvo aiškiai išdėstytas Teismo **Halford prieš Jungtinę Karalystę byloje, minimoje aukščiau.**

Ką reikėtų pastebėti, ir kas iš tiesų palieka tam tikras ribas interpretacijai, tai kokiu laipsniu nuo šio principo galima nukrypti ar jį apriboti, ypač kai jis prieštarauja kitų teisėms ir laisvėms, panašiai saugomoms Konvencijos (pvz., teisėti darbdavio interesai). **Bet kuriuo atveju, naudojamų elektroninių vieta ir nuosavybės teisė nepanaikina komunikacijos ir korespondencijos slaptumo, kaip nurodyta pagrindiniuose teisiniuose principuose ir konstitucijose.**

Nežiūrint to, 29 straipsnio Darbo grupė norėtų priminti, kad tai nėra išskirtinė asmens duomenų tvarkymo problema darbo santykių atveju, bet bendra problema, kuri kyla iš fakto, kad duomenų apsaugos teisė ir teisiniai aktai netaikomi abstrakčiai. Duomenų apsaugos teisės turėtų būti taikomos skirtingose teisinėse sistemose su kitais galiojančiais teisės aktais, nustatančiais kitas individų teises ir pareigas (pvz., darbo teise). Vis dėlto 29 straipsnio Darbo grupė yra įsitikinusi, kad sprendimai, siūlomi šiame darbiname dokumente, gali būti naudingi siekiant sudėtingo interesų balanso.

²¹ Viena iš pirmųjų rekomendacijų, išleistų Darbo grupės, Rekomendacija 3/97 “Anonimiškumas internete”, jau teigė, kad interneto ir ne interneto situacijos turi būti traktuojamos vienodai:

Žr. http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp6en.pdf

Interneto Laikinosios darbo grupės dokumentas, svarbiausias Privatumo internete Darbo grupės priimtas dokumentas, primygtinai reiškė šią idėją trečiame skyriuje, psl. 21:

Žr. http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp37en.pdf

4.2. ĮTEISINIMAS PAGAL DIREKTYVĄ 95/46/EB

Elektroniniame pašte yra asmeninių duomenų, saugomų Direktyvos 95/46/EB nuostatomis, ir dėl to darbdaviai turi turėti teisėtus pagrindus šių duomenų tvarkymui. Kaip buvo išsamiai paaiškinta Nuomonėje 8/2001, darbuotojo sutikimas turi būti duotas laisvai, jam turint visą informaciją, ir darbdaviai neturi pasikliauti sutikimu kaip bendriausia tokio proceso įteisinimo priemone.

Labiausiai tikėtina, kad elektroninio pašto įteisinimo pagrindas gali būti rastas Direktyvos 7 (f) straipsnyje, t.y., kuomet tvarkymas yra būtinas teisėtiems valdytojo arba trečiosios šalies ar šalių, kuriems duomenys perduodami, interesams įgyvendinti. Prieš svarstant šios nuostatos pritaikymą nagrinėjamiems klausimams, turi būti pabrėžta, kad toks įteisinimas negali nusverti pagrindinių darbuotojo teisių ir laisvių, tame tarpe, kur tinkama, ir pagrindinės teisės į korespondencijos slaptumą.

Darbo grupė jau atkreipė dėmesį į²²:

"Tuo atveju, kai darbdavys turi tvarkyti asmens duomenis kaip būtiną ir neišvengiamą darbo santykių pasekmę, yra klaidinga, jei jis siekia įteisinti šį procesą per sutikimą. Pasitikėjimas sutikimu turi būti apribojamas atvejais, kai darbuotojas nuoširdžiai ir laisvai apsisprendžia sutikti, ir atitinkamai gali be nuostolių atšaukti sutikimą."

Turint omenyje, kad elektroninį paštą sudaro tiek siuntėjo, tiek gavėjo asmens duomenys, darbdaviai paprastai gali gauti tik vienos iš šių šalių sutikimą be didelių sunkumų (nebent elektroninis paštas yra vidinė personalo korespondencija), galimybė įteisinti elektroninio pašto stebėjimą tokio sutikimo pagrindu yra labai ribota. Panašūs svarstymai taikomi Direktyvos 7 (b) straipsniui, kadangi viena laiško šalis niekada neturės sutarties su duomenų valdytoju šios nuostatos taikymo, t.y. elektroninio pašto stebėjimo, ribose.

Esant tokiam susikirtimui, turi būti pažymėta, kad kur darbuotojui yra suteikta elektroninio pašto dėžutė ar leidimas naudotis internetiniu paštu grynai asmeniniais tikslais, tokio elektroninio pašto atidarymas iš darbdavio pusės (išskyrus skanavimą nuo virusų) gali būti pateisintas tik labai ribotomis aplinkybėmis²³, ir normaliomis sąlygomis negali būti pateisinamas 7 (f) straipsniu, kadangi priėjimas prie tokių duomenų nėra teisėtas darbdavio interesas. Vietoje to, pagrindinė teisė į korespondencijos slaptumą dominuoja.

Dėl to klausimas, koku laipsniu 7 (f) straipsnis leidžia elektroninio pašto stebėjimą priklausyti nuo pagrindinių principų, paaiškintų 3.2. skyriuje, taikymo konkrečiam atvejui. Kaip jau nurodyta 3.1.4 skyriuje (teisėtumas), atliekant balanso testą tinkamai, turi būti atsižvelgta į išorinių organizacijos subjektų privatumą, bei kaip jį paveiks stebėjimas.

²² Žr. paragrafą Nuomonės 8/2001 rėmuose, p. 23.

²³ Tokius veiksmus sudaro kriminalinė darbuotojo veikla, kuomet darbdaviui būtina ginti savo interesus, pvz., kuomet jis yra atsakingas už darbuotojo veiksmus arba yra kriminalinio nusikaltimo auka.

4.3 REKOMENDUOJAMA MINIMALI INFORMACIJA, KURIA KOMPANIJA TURI SUTEIKTI SAVO DARBUOTOJAMS

Sudarydami savo taisykles, darbdaviai turi užtikrinti, kad jos atitiktų 3.1.3 skyriuje išdėstytus principus, įeinančius į bendrąjį Skaidrumo principą²⁴, atsižvelgiant į būtinumą ir organizacijos dydį.

Detaliau, kalbant apie elektrinį paštą, turi būti išnagrinėti šie momentai:

- a) Ar darbuotojui suteikta elektroninio pašto dėžutė grynai asmeniniam naudojimui, ar darbe leidžiama naudotis priėjimu prie interneto ir ar darbdavys rekomenduoja asmeninio priėjimo ar asmeninės pašto dėžutės naudojimą asmeniniais tikslais (žr. 4.4 skyrių).
- b) Tvarką, suderintą su darbuotojais, kaip prieinama prie elektroninio pašto turinio, pvz., kai darbuotojo nėra darbo vietoje dėl nežinomos priežasties, nustatant tokio priėjimo tikslus.
- c) Jei daromos žinučių atsarginės (angl. “*backup*”) kopijos, jų saugojimo laikas.
- d) Informacija, kada elektroninis paštas yra negrįžtamai ištrinamas iš serverio.
- e) Saugumo klausimai.
- f) Darbuotojų atstovo įtraukimas į taisyklių kūrimą.

Turi būti pažymėta, kad nėra nuolatinio darbdavio įpareigojimo užtikrinti, kad jo taisyklės turi būti nuolat atnaujinamos lygiagrečiai technologiniam vystymuisi ir darbuotojų nuomonei.

4.4 INTERNETINIS PAŠTAS²⁵

Darbo grupė laikosi nuomonės, kad taisyklės, leidžiančios darbuotojams naudotis privačia pašto dėžute ar internetiniu paštu galėtų būti pragmatiškas problemos sprendimas. Toks darbdavio darbo dokumentas išaiškintų skirtumą tarp elektroninio

²⁴

1. Elektroninio pašto/interneto naudojimo taisyklės įmonėje, detalai nustatančios laipsnį, kuriuo kompanijos valdoma komunikacijos įranga gali būti naudojama asmeninei/privačiai darbuotojų komunikacijai (pvz., laiko ir naudojimo trukmės apribojimai).
2. Tikslai ir priežastys, dėl kurių stebima, jei stebima. Jei darbdavys leido naudotis įmonės komunikacine įranga privačiais tikslais, tokia privati komunikacija gali būti stebima tik labai ribotomis aplinkybėmis, pvz. siekiant užtikrinti informacinės sistemos saugumą (patikrinimas nuo virusų).
3. Naudojamų sekimo priemonių detalės, tai yra Kas? Ką? Kada?
4. Bet kokių spaudimo procedūrų detalės, nurodančios, kada ir kaip darbuotojai bus išpėjami apie vidinių taisyklių pažeidimus, ir jiems bus suteikta galimybė atsakyti į pareiškimus prieš juos.

²⁵ Internetinis paštas yra interneto elektroninio pašto sistema, kuri suteikia internetu paremtą elektroninį paštą iš bet kokio POP ar IMAP serverio; paprastai jam taikoma naudotojo vardo ir slaptažodžio apsauga.

pašto profesiniam ir privačiam naudojimui, ir sumažintų darbdavių galimybę kištis į darbuotojų privatumą. Dar daugiau, jis nereikalautų jokių, arba minimalių papildomų kaštų darbdaviui.

Jei darbdavys priima tokias taisykles, tada specifinėse situacijose, kai darbuotojo elgsena kelia rimtą įtarimą, būtų galima stebėti, koku laipsniu darbuotojas naudoja savo personalinį kompiuterį asmeniniais tikslais, fiksuojant laiką, praleistą internetiniame pašte. Tokiu būdu darbuotojo interesai bus patenkinti be galimybės atskleisti darbuotojo duomenis, ypač ypatingus duomenis.

Dar daugiau, tokios taisyklės gali pasitarnauti darbuotojams, kadangi jos suteiktų jiems tikrumą dėl privatumo lygio, kurio jie gali tikėtis, kadangi elgsenos kodeksuose jo gali trūkti arba jis per daug komplikuoatas. Po to, kai pasakėme šitai, yra būtina pabrėžti, kad:

a) tai, kad internetinio pašto ar asmeninės pašto dėžutės naudojimas yra leidžiamas, neapriboja pilno anksčiau šiame skyriuje išdėstytų nuostatų taikymo kitoms pašto dėžutėms darbo vietoje.

b) leisdamos naudotis internetiniu paštu, įmonės turi suprasti, kad jų naudojimas gali mesti iššūkį įmonės tinklų saugumui, ypač kalbant apie virusų plitimą.

c) darbuotojai turi suprasti, kad kai kada internetinio pašto serveriai yra trečiųjų šalių teritorijoje, kur gali nebūti adekvačios individų asmens duomenų apsaugos.

Turi būti turima omenyje, kad šie svarstymai taikomi standartiniams darbdavio-darbuotojo santykiams. Ypatingos taisyklės gali būti taikomos komunikacijai tų darbuotojų, kurie susieti profesinės paslapties išipareigojimais.

5. PRIĖJIMO PRIE INTERNETO STEBĖJIMAS

5.1 INTERNETO NAUDOJIMAS PRIVAČIAIS TIKSLAIS DARBE

Visų pirma turi būti pabrėžta, kad nuo kompanijos priklauso, ar darbuotojams leidžiama naudoti internetą asmeniniais tikslais, ir koku laipsniu.

Net ir turint tai omenyje, Darbo grupė laikosi nuomonės, kad vienareikšmiškas draudimas naudotis internetu darbuotojų asmeniniais tikslais gali būti nepraktiškas ir kiek nerealistiškas, kadangi juo neįmanoma atspindėti laipsnio, kuriuo internetas yra reikalingas darbuotojams kasdieniniame gyvenime.

5.2. SU INTERNETO STEBĖJIMU SUSIJĘ PRINCIPAI

Egzistuoja tam tikri principai, kurie gali būti taikomi svarstant darbuotojų priėjimo prie interneto klausimą.

Kur įmanoma, **prevencija turi būti svarbesnė nei detekcija**. Kitaip tariant, darbdavio interesai yra geriau patenkinami imantis prevencinių priemonių prieš netinkamą interneto naudojimą techninėmis priemonėmis, nei papildomos išlaidos netinkamo naudojimo užfiksavimui. Tam tikru laipsniu pagrįstai įmanoma interneto politika turėtų remtis techninėmis priemonėmis, apribojančiomis prisijungimą nei stebėjimo veikla, tai yra blokuojant kai kurias svetaines ar instaliuojant automatinį prisijungimo perspėjimą.

Greitos informacijos perdavimas darbuotojui apie įtartino interneto naudojimo identifikavimą yra svarbus siekiant minimizuoti problemas. Net jei priemonė būtina, bet koks stebėjimas turi būti **proporcingas** darbdavio patiriamai rizikai. Daugumoje atvejų netinkamas interneto naudojimas gali būti nustatytas be būtinumo analizuoti aplankytų svetainių turinį. Pavyzdžiui, praleisto laiko ar dažniausiai departamento lankomų svetainių tikrinimas gali būti pakankamas, kad darbdavys įsitikintų, ar jo įranga naudojama teisingai. Jei tokie bendrieji patikrinimai atskleidžia galimą neteisingą interneto naudojimą, tada darbdavys gali svarstyti papildomo stebėjimo rizikos sferoje galimybę.

Įvertindami darbuotojų naudojimąsi internetu, darbdaviai **turi stengtis atsargiai daryti išvadas**, atsižvelgiant į lengvą svetainių aplankymo nesąmoningai galimybę, per iš anksto nenumatytus atsakymus į paieškos sistemų priemones, neiškias perdėto teksto nuorodas, klaidinančias banerių reklamas ir raktus. Bet koku atveju, darbuotojams turi būti pateikti faktai ir suteikta pilna galimybė ginčyti darbdavio tvirtinamą neteisingą interneto naudojimą.

5.3 REKOMENDUOJAMAS MINIMALUS ĮMONĖS INTERNETO POLITIKOS TURINYS

1. Informacija, nurodyta 3.1.3 skyriuje (Skaidrumo principas)²⁶.

Dar detaliau, kalbant konkrečiai apie interneto naudojimą, turi būti atsižvelgiama į:

2. Darbdaviai turi aiškiai nustatyti darbuotojams sąlygas, kuriomis privatus interneto naudojimas yra leidžiamas, nurodant medžiagą, kuri negali būti peržiūrima ar kopijuojama. Šios sąlygos ir apribojimai turi būti paaiškinti darbuotojams.
3. Darbuotojai turi būti informuoti apie įdiegtą sistemą, užkertančią kelią priėjimui prie tam tikrų svetainių ir nustatančią neteisingą naudojimą. Tokio stebėjimo laipsnis turi būti detalizuotas, pvz., ar toks stebėjimas gali įtakoti individus, ar konkrečius įmonės sektorius, ar darbdaviai tam tikromis aplinkybėmis peržiūri ir įrašo lankomų svetainių turinį. Dar daugiau, taisyklės turi nustatyti, koks naudojimas, ir ar iš viso, bus atliekamas su duomenis apie tai, kas aplankė kurias svetaines.
4. Informuoti darbuotojus apie jų atstovų įtraukimą tiek į taisyklių įdiegimą, tiek į įtariamų pažeidimų tyrimą.

-
1. Elektroninio pašto/interneto naudojimo taisyklės įmonėje, detaliai nustatančios laipsnį, kuriuo kompanijos valdoma komunikacijos įranga gali būti naudojama asmeninei/privačiai darbuotojų komunikacijai (pvz., laiko ir naudojimo trukmės apribojimai).
 2. Tikslai ir priežastys, dėl kurių stebima, jei stebima. Jei darbdavys leido naudotis įmonės komunikacine įranga privačiais tikslais, tokia privati komunikacija gali būti stebima tik labai ribotomis aplinkybėmis, pvz. siekiant užtikrinti informacinės sistemos saugumą (patikrinimas nuo virusų).
 3. Naudojamų sekimo priemonių detalės, tai yra Kas? Ką? Kada?
 4. Bet kokių spaudimo procedūrų detalės, nurodančios, kada ir kaip darbuotojai bus išpėjami apie vidinių taisyklių pažeidimus, ir jiems bus suteikta galimybė atsakyti į pareiškimus prieš juos.

IŠVADOS

Darbo grupė sudarė šį darbinį dokumentą siekdama prisidėti prie vieningo bendrųjų priemonių, priimtų pagal Direktyvą 95/46/EB elektroninės komunikacijos darbo vietoje sekimo ir stebėjimo srityje, taikymo. (Žr. nacionalinių teisės aktų santraukas šio dokumento prieduose).

Darbo grupė pastebėjo kai kuriuos neatitikimus tarp nacionalinių teisių, daugiausiai su duomenų apsauga susijusiose srityse dėl leidžiamų nukrypimų nuo pagrindinių teisių korespondencijos slaptumui, taip pat susijusių su kolektyvinio atstovavimo ir kolektyvinio sprendimo priėmimo mastu ir įtaka. Nežiūrint to, 29 straipsnio Darbo grupė norėtų pabrėžti, kad bet kokie neatitikimai tarp šalių narių teisių įdiegiant Direktyvą 95/46/EB nėra pačios didžiausios kliūtis bendram taikymui, kuris telpa į principuose ir geroje praktikoje, pažymėtoje darbiniam dokumente.

Darbo santykių Pogrupis nuolat atnaujins šį darbinį dokumentą atsižvelgiant į patirtį ir tolesnį vystymąsi šioje srityje 2002-2003 metais.

Sudaryta Briuselyje 2002 m. gegužės 29 d.

Darbo grupės vardu

Pirmininkas

Stefano RODOTA

Darbinio dokumento priedas

NACIONALINĖS ELEKTRONINĖS KOMUNIKACIJOS DARBO VIETOJE SEKIMO IR STEBĖJIMO TEISĖS

6.1.1 Belgija

22-as Belgijos Konstitucijos straipsnis garantuoja teisę į privatumą.

2,s.1 kolektyvinės sutarties Nr.13 straipsnis (1983 m. gruodžio 13 d.) skelbia: “kai darbdavys nusprendžia investuoti į naują technologiją (...), turinčią svarbias kolektyvines pasekmes (...) darbo sąlygoms, jis, prieš pradėdamas naujos technologijos įvedimą, turi pateikti informaciją apie naujos technologijos pobūdį, įvedimą pagrindžiančius faktorius ir jo pasekmes, ir konsultuotis su darbuotojų atstovais įdiegiant naują technologiją”.

Dar daugiau, korespondencijos privatumo principą gina 1991 m. kovo 21 d. įstatymo “Dėl tam tikrų ekonominių valstybinių kompanijų reformos” 109 d straipsnis, skelbiantis, kad “saugant su susitikimu (...) nepriklausomai nuo to, ar tai atlieka patys, ar trečioji šalis, bet kam draudžiama sužinoti apie bet kokių duomenų, perduodamų telekomunikacijos priemonėmis, kuriuos sukuria ar kurie yra skirti kitiems asmenims, egzistavimą”.

Belgijos Duomenų apsaugos institucija taip pat nagrinėjo elektroninio pašto ir interneto stebėjimo klausimą savo Nuomonėje 2000 m. (Nuomonė Nr.10-2000, 2000 m. balandžio 3 d.). Kalbant apie elektroninio pašto stebėjimą, Belgijos Komisija laikosi nuomonės, kad darbdavys neturi gauti priėjimo prie elektroninio pašto turinio, kadangi tokie veiksmai nėra proporcingi bet kokiems darbdavio interesams, kuriuos jis siekia apginti. Komisija rekomendavo vietoje to darbdaviui stebėti remiantis elektroninio pašto judėjimo duomenimis ir naudotis programine įranga, galinčia identifikuoti neįprastai dideles arba grandines žinutes.

Dėl interneto naudojimo stebėjimo Komisija laikosi nuomonės, kad nuolatinis individų stebėjimas yra netinkamas. Komisija rekomenduoja darbdaviui daryti bendrąsias darbuotojo lankytų svetainių apžvalgas (nenustatant, kuris individas lankėsi konkrečioje svetainėje) ir, remiantis tokiu tyrimu, nustatyti galimas rizikos sferas bei imtis atitinkamų individualių veiksmų.

6.1.2 Danija

Stebėjimas ir sekimas darbo vietoje daugiausiai reglamentuojamas kolektyvinėmis sutartimis, ypač taip vadinama “bendraja sutartimi”. Pagrindinė šios bendrosios sutarties dalis yra pripažinimas, kad darbdaviui leidžiama stebėti darbą, atliekamą darbo vietoje. Tačiau precedentinėje teisėje buvo pripažinta, kad ši teisė yra darbdavio išipareigojimas elgtis tinkamai ir nepiktnaudžiauti savo galimybėmis.

Pagal Bendrosios sutarties tarp Danijos Darbdavių konfederacijos ir Danijos Profesinių sąjungų konfederacijos priedą, darbdavys privalo informuoti darbuotojus apie bet kokią stebėjimo veiklą, kurią jis ketina įgyvendinti likus ne mažiau kaip dviem savaitėms iki stebėjimo pradžios.

Ši sutartis yra tipinė galiojančioms Danijoje.

Telekomunikacijų stebėjime yra priešingai pagal Danijos Kriminalinio Kodekso s.263 (1)(3) nepriklausomai nuo to, ar komunikacija yra privati, ar profesinė. Tačiau ar elektroninis paštas įeina į šį draudimą, yra neaišku, o privatus interneto naudojimas neįeina.

Danijos Duomenų apsaugos agentūra kai kuriose bylose yra nustačiusi, kad darbdavys gali įrašinėti/įsijungti į darbuotojo interneto naudojimą. Tam turi būti išpildytos šios sąlygos:

Įrašymas ir įsijungimo failo tikrinimas turi būti būtinas teisėtiems darbdavio interesams, ir darbuotojo interesai neturi būti viršesni. Teisėti interesai gali būti techniniai ar saugumo, taip pat darbdavio interesas stebėti, kaip darbuotojas naudojasi internetu.

Paprastai darbdavys aiškiai ir nedviprasmiškai turi iš anksto informuoti darbuotoją apie įrašymą, ir apie tai, kad įrašymas gali būti tikrinamas esant įtarimui apie neleistiną interneto naudojimą.

Kalbant apie elektroninį paštą, Danijos Duomenų apsaugos agentūra nustatė, kad įmonė gali pasidaryti atsarginę darbuotojo elektroninio pašto kopiją, ir išnagrinėti šią kopiją esant įtarimui dėl neteisingo elektroninio pašto sistemos naudojimo. Tam turi būti išpildytos šios sąlygos:

Darbuotojo elektroninio pašto atsarginė kopija ir galimas jos nagrinėjimas gali įvykti tik tada, jei jis būtinas teisėtiems darbdavio interesams, ir darbuotojo interesai jų nepersveria.

Teisėti interesai gali būti verslo veikla, saugumas, elektroninio pašto atstatymas, dokumentavimas ir stebėjimas.

Tiek interneto, tiek elektroninio pašto stebėjimo atveju darbdavys privalo tvarkyti duomenis atitinkamai gerai duomenų tvarkymo praktikai.

6.1.3 Vokietija

Konstitucijos 10-as straipsnis garantuoja pašto ir telekomunikacijos privatumą. Papildomai Telekomunikacijų akto 85-a dalis įpareigoja kiekvieną telekomunikacijų paslaugų teikėją laikytis telekomunikacijų slaptumo.

Apsaugos laipsnis yra skirtingas tarp privataus ir oficialaus elektroninės komunikacijos naudojimo. Oficialaus pašto kontrolė yra leidžiama. Bet be sutikimo neleidžiama naudoti (oficialaus) elektroninio pašto sekimo, kaip darbuotojo efektyvumo kontrolės priemonės. Darbdavio ir darbuotojų tarybos sutartis yra tam būtina. Bet kuriuo atveju yra draudžiama kontroliuoti ir ypač skaityti privatų elektroninį paštą. Geriausias praktinis šios problemos sprendimas yra atskiros pašto dėžutės privačiam ir oficialiam paštui.

Jei interneto naudojimas yra galimas darbo vietoje, kyla tos pačios problemos. Teisės aktai dėl duomenų apsaugos telepaslaugų srityje (Telepaslaugų duomenų apsaugos aktas, neseniai atnaujintas variantas) netaikomas oficialiam interneto naudojimui darbo vietoje. Bet jie taikomi privačiam interneto naudojimui, kiek jis yra leidžiamas.

Sekimas ir stebėjimas yra leidžiami be sutikimo, jei jie būtini siekiant užtikrinti efektyvų sistemos funkcionavimą (pvz., tikrinimas nuo virusų).

6.1.4 Graikija

Graikijos 1975 m. Konstitucija, atnaujinta 2001 m. balandį, įtraukia pagrindinių teisių saugančių privatumą, rinkinį, ir platesnę teisę į asmenybę.

Dar daugiau, Graikija turi nuolatinės nuostatas dėl pagarbos žmogiškai vertei ir jos apsaugos, kurios individas negali atsisakyti. Pagal graikų teisę, sutartis, kuri perdėtai apriboja individo laisvę, yra negaliojanti.

Civilinio kodekso 178 ir 179 straipsniai skelbia, kad bet koks teisinis aktas, prieštaraujantis gerai moralei, yra negaliojantis, taip pat graikų teisė skelbia, kad negalioja ir teisinis aktas, kai jis perdėtai apriboja kito laisvę. Terminas "laisvė" naudojamas išreiškiant konstitucines žmogaus teisių nuostatas, tame tarpe ir teisę į privatumą.

Šios nuostatos turi būti naudojamos panaikinant elektroninio pašto stebėjimą, kadangi tokie veiksmai apriboja darbuotojų teisę į privatumą.

Įstatymas 1767/1988, pataisytas įstatymu 2224/1994, suteikia darbuotojų taryboms teisę bendrai su darbdaviu spręsti tam tikrus klausimus, tame tarpe ir sekimą.

Dar daugiau, Graikijos Duomenų apsaugos institucija priėmė sprendimą dėl stebėjimo darbo vietoje.

6.1.5 Ispanija

Ispanijos Konstitucija 18-ame straipsnyje skelbia komunikacijos privatumą, taip pat ir privačios, tiek pašto, tiek telegrafo ar telefono. Ji taip pat nustato duomenų tvarkymo, įsteigto ir atliekamo teisėtai, naudojimo ribas, siekiant garantuoti piliečių garbę ir asmens ar šeimos privatumą, ir pilną šių teisių panaudojimą.

1995 m. Darbo Akto 5-as straipsnis nusako darbdavio išsipareigojimą vykdyti savo darbo išsipareigojimus atitinkamai gerai valiai ir darbštumui. Kitaip tai laikoma kontrakto pažeidimu (54.2 straipsnis).

Darbo Akto 18-as straipsnis skelbia, kad "Darbuotojo asmens, spintelių ir asmens daiktų tikrinimas gali būti atliekamas tik tuomet, kai tai būtina įmonės turto ir kitų įmonės darbuotojų apsaugojimui, tik darbo vietoje ir darbo laiku. Patikrinimo metu darbuotojo orumas ir privatumas turi būti gerbiamas aukščiausiu lygiu, ir patikrinimas atliekamas dalyvaujant teisėtam darbuotojų atstovui, arba, jam nesant, kitam įmonės darbuotojui, jei tik tai įmanoma."

Darbo Akto 20-as straipsnis skirtas darbdavio valdymo, tikrinimo, organizavimo ir kontroliavimo galių. Darbdavys gali imtis bet kokių tinkamų priemonių darbuotojų pareigoms tikrinti ir kontroliuoti, visada gerbdamas žmogišką orumą.

1995 m. Darbo rizikos prevencijos įstatymas nustato darbdavio pareigą konsultuoti darbuotojus, gerokai iš anksto, apie sprendimų, susijusių su (be kita ko) darbo planavimu ir organizavimu kompanijoje, įvedimu, ir naujų technologijų įvedimą, taip pat bet ką, susijusį su pasekmėmis darbuotojo saugumui ir sveikatai, jei tai išplaukia iš įrangos parinkimo, darbo sąlygų apibrėžimo ir adekvatumo bei aplinkos faktorių darbo vietoje.

Darbo Aktas ir 1985 m. Sąjungų laisvės Aktas vysto darbuotojo teisę į kolektyvinį atstovavimą kaip jų teisę dalyvauti įmonės veikloje per kolektyvinį atstovą (personalo delegatus ir kompanijų komitetus) ir Sąjungų atstovus.

Civilinis Kodeksas 1903-iame straipsnyje skelbia, kad darbdaviai yra tiesiogiai atsakingi prieš trečiąsias šalis dėl nuostolių, kuriuos padarė jų darbuotojai vykdydami savo užduotis.

Kriminalinio Kodekso 197-as str. numato atsakomybę už kito asmens privačios korespondencijos perėmimą siekiant atskleisti asmens paslaptį ar privatų gyvenimą.

6.1.6 Prancūzija

Prancūzijos Civilinio Kodekso 9-as straipsnis garantuoja kiekvienam individui teisę į privataus gyvenimo gerbimą, net darbo vietoje darbo metu.

Pagal 1991 m. įstatymą “Dėl komunikacijų slaptumo”, darbdavys negali priesti prie privačios darbuotojo komunikacijos, išskyrus teismo įgaliojimo leidimu, arba kai įsikišimas atliekamas dėl “geros valios”. Pastarąjį terminą interpretavo CNIL (Prancūzijos duomenų apsaugos institucija) kaip leidžiantį stebėti žinučių dydį ir apimtį, taip pat pridėdama dokumento formata, be ne skaityti elektroninius laiškus.

Prancūzijos Civilinio Kodekso L. 121-8 straipsnyje, darbdavys negali rinkti asmeninės su darbuotoju susijusios informacijos prieš tai neatkreipęs į tai darbuotojo dėmesio. Tai reiškia, kad darbuotojas turi būti informuotas apie stebėjimo priemonių, įdiegtų darbdavio, egzistavimą.

Neocel byloje [Cass. Soc. 20/11/91 (RDS 1992(2), 77)] buvo pripažinta, kad Civilinis Kodeksas draudžia slaptą darbuotojų stebėjimą.

Neseno Nikon France skundo nagrinėjimo eigoje Prancūzijos Aukščiausiasis Teismas (Socialiniai Rūmai) spalio 2 d. nusprendė, kad darbuotojai turi teisę į savo privatumo gerbimą, ir tai reiškia, kad jo darbdavys negali priesti prie asmeninių žinučių, išsiunčiamų ar gaunamų darbuotojo, turinio.

Toje pačioje byloje darbuotojas išsiuntė asmeninį laišką kompiuteriu, kurį jis naudojo darbo tikslais, nežiūrint fakto, kad jo darbdavys aiškiai uždraudė asmeninį sistemos naudojimą. Teismas nusprendė, kad faktas jog darbuotojas nepakluso darbdavio nurodymui nepateisina laiškų skaitymo.

Teismas laikėsi nuomonės, kad ribotas kasdieninis elektroninio pašto/interneto naudojimas turėtų būti leidžiamas, jei toks naudojimas neįtakoja darbuotojo kasdieninio profesinio gyvenimo. Taip pat buvo rekomenduota, kad sutartyje visada turi būti aprašymas, ar jie yra profesiniai, ar asmeniniai.

Po viešo konsultavimosi dėl kiber-stebėjimo detalių principų projekto, kuris prasidėjo 2001 m. kovą, Prancūzijos Nacionalinė duomenų apsaugos institucija (CNIL) 2002-m.

vasario 5 d. priėmė nutartį, kuri rekomendavo (be kita ko) stebėjimo darbo vietoje klausimo sprendimą per tolesnes diskusijas. Papildomai socialiniai partneriai skiria specialų asmens duomenų apsaugos įgaliotinį.

6.1.7 Airija

Airijos Konstitucijos 40.3.1 straipsnis garantuoja, kad Valstybė savo teisės aktais gerbs ir, jei tai įgyvendinama, savo teisės aktais gins asmenines piliečio teises. Šios piliečio “asmens teisės”, arba “neišmatuojamos teisės”, kaip jos vadinamos Airijos precedentinėje teisėje, vis plėtojasi. Teisė į privatumą jau buvo pripažinta Airijos precedentinėje teisėje kaip viena iš piliečio asmeninių teisių.

6.1.8 Italija

Pagal Italijos teisę, teismo orderis yra būtinas tam, kad būtų galima prieiti prie darbuotojo elektroninio pašto žinučių.

Italijos Konstitucijos 15 straipsnis garantuoja korespondencijos ir bet kokios kitos komunikacijos formos laisvę ir slaptumą.

Šios nuostatos svarbą pripažino Italijos Garante (duomenų apsaugos institucija) elektroninio pašto stebėjimo kontekste. Jie 1999 m. liepos 12 d. Nuomonėje deklaravo, kad elektroninis paštas turi tą pačią konfidencialumo privilegiją, kaip ir tradicinis paštas, ir taip pat jie pažymėjo, kad 1993 m. Aktas (nr. 547) Dėl nusikaltimų susijusių su kompiuteriu ir 1997 m. dekretu (nr. 513) Dėl elektroninių dokumentų, taip pat nurodė, kad elektroninis paštas reikia tokios pačios apsaugos, kaip ir tradiciniam.

Dar detaliau, Nuomonė nurodė, kad elektroninės žinutės, cirkuliuojančios tarp riboto priėjimo naujienų grupių ir elektroninio pašto adresų sąrašai, naudojant darbuotojo įrangą, turi būti laikomi privačia korespondencija, ir darbdavys neturi jų prieiti.

Garante šiuo metu svarsto galimybę išleisti nuorodas elektroninio pašto stebėjimo srityje, atsižvelgdama į visus Darbo grupės darbinis dokumentus.

Italijos duomenų apsaugos teisė (Įstatymas Nr. 675/1996) sekcijoje 43(2) skelbia, kad jis neįtakoja galiojančios darbo santykių teisės, susijusios su darbuotojo teisėmis (Įstatymas Nr. 300/1970). Pastarojo Akto 4 straipsnis paskelbia už įstatymo ribų darbuotojų sekimą patį savaime, ir leidžia tik technologiją, kuri netiesiogiai gali tapti darbuotojų sekimu, jei atitinkama profesinė sąjunga su tuo sutinka, ir yra specialūs reikalavimai organizacijos, produkcijos ir/ar veiklos saugumui.

6.1.9 Liuksemburgas

Kol kas nėra sudarytos sekcijos.

6.1.10 Nyderlandai

Olandų Konstitucijos 10-as straipsnis skelbia, kad kiekvienas turi teisę į savo privatumo gerbimą.

Konstitucijos imperatyvas, kuris gali būti naudojamas interpretacijai, pateiktas 660-oje Civilinio Kodekso dalyje.

Ši dalis skelbia, kad darbdaviai turi daryti ar susilaikyti nuo darymo veikų, kurias geras darbdavys darytų ar susilaikytų nuo darymo panašiomis aplinkybėmis. Dar daugiau, Civilinio Kodekso 611-a dalis nustato darbdavio ir darbuotojo santykius ir gerą veiklą. Ši dalis, atsižvelgiant į konstitucines garantijas, gali būti interpretuojama kaip garantuojanti darbuotojo privatumą.

Darbo sąlygų Akto 5.1-5.3 straipsnis nustato, kad darbuotojai turi būti informuoti tuo atveju, jei darbdavys juos stebi, ir kad darbdavių tarybos ir profesinės sąjungos turi būti informuotos, ir kai kuriais atvejais, turi duoti sutikimą bet kuriai iš šių priemonių. Ypač Darbo tarybų teisė pabrėžia, kad darbo taryba turi būti informuojama, išklaudyta ir sutikti su stebėjimu darbo vietoje.

Pagal Duomenų apsaugos akto 8 straipsnį, stebėjimas yra leidžiamas tik tada, kai darbuotojai davė savo nedviprasmišką sutikimą, arba tvarkymas yra būtinas darbo sutarties įgyvendinimui, arba darbdavio teisinių įsipareigojimų įgyvendinimui, arba teisėtiems darbdavio tikslams.

1999 m. Olandijos duomenų apsaugos institucijos sprendime buvo nustatyta, kad nuolatinis elektroninio pašto stebėjimas yra neleistinas, kadangi nėra aiškaus ir teisėto tokio stebėjimo tikslo. Šis sprendimas taikomas net ir tada, kai darbdavio taisyklės aiškiai skelbia, kad darbuotojai neturi tikėtis privatumo.

2000 m. birželio 16 d. Regioninio Harlemo teismo sprendime buvo nurodoma “darbo vietos suasmeninimo koncepcija”, reiškianti kad ribos tarp privataus ir darbo gyvenimo nebėra aiškios. Šiame kontekste asmeniniai kontaktai darbe turi būti leidžiami.

6.1.11 Austrija

Europos Žmogaus teisių Konvencijos 8 straipsnis, nustatantis teisę į privatumą, yra tiesiogiai taikomas Austrijoje, ir jam Austrijos teisinėje sistemoje buvo suteiktas konstitucinių garantijų statusas. Dar daugiau, 2000 m. Duomenų apsaugos Akto (Datenschutzgesetz 2000) 1 straipsnis, kuris sukuria individų teisę į savo duomenų apsaugą, taip pat turi konstitucinės teisės statusą.

Duomenų apsauga darbo vietoje yra duomenų apsaugos fundamentalių teisių dalykas, išdėstytas Austrijos 2000 m. Duomenų apsaugos Akte (Datenschutzgesetz 2000).

Yra aiški nuostata 9, ss.11 dėl ypatingų duomenų darbo vietoje naudojimo. Pagal šią sekciją duomenų subjekto “interesai slaptume” nėra pažeidžiami, jei ypatingų asmens duomenų tvarkymas yra būtinas darbdaviui pagal jo teises ir pareigas darbo santykių srityje ir yra teisėtas pagal konkrečius teisės aktus.

Pagal Arbeitsverfassungsgesetz 96 straipsnį (Federal Law Gazette No. 22/1974) darbdavys negali imtis tam tikrų priemonių be atitinkamos darbo tarybos sutikimo. Tai liečia kontrolinių priemonių ir techninės instaliacijos įdiegimą, jei tokios priemonės pažeidžia asmens orumą. Dar daugiau, toks darbuotojų tarybos sutikimas yra būtinas net jei individualioje įdarbinimo sutartyje darbuotojai sutinka su tokiomis priemonėmis.

6.1.12 Portugalija

Portugalijos Konstitucija turi gana progresyvų požiūrį. Vietoje to, kad turėtų bendrą straipsnį dėl konstitucinio privatumo, 35 straipsnis nurodo duomenų apsaugą dėl kompiuterizuotos informacijos naudojimo. Portugalijos Konstitucijoje taip pat yra

6.1.15 Jungtinė Karalystė

2000 m. Tiriamųjų jėgų reguliavimo aktas buvo priimtas 2000 m. spalį ir padarė darbdavių ir kitų asmenų įsikišimą į darbuotojų skambučius ir elektroninį paštą be korespondencijos siuntėjo ir gavėjo sutikimo neteisėta veika.

Tačiau pagal Akto 4 (2) dalį, buvo priimtas Telekomunikacijų (teisėto verslo praktikos) (įsiskverbimo į komunikaciją) reguliacinis aktas 2000, kuris įgalino darbdavius *įsikišti be sutikimo* sekant ir įrašant komunikaciją, jei siekiama:

- 1 Nustatyti faktų, susijusių su verslu, egzistavimą.
- 2 Užtikrinti atitinkamų reguliacinių ir savireguliacinių taisyklių ir praktikos laikymąsi.
- 3 Išsiaiškinti darbuotojų pasiektus standartus.
- 4 Užkirsti kelią nusikaltimui ar jį nustatyti.
- 5 Užtikrinti sistemos saugumą ir efektyvų funkcionavimą.

Sutikimo reikalavimo išimtys yra plačios. Darbdaviai turi dėti visas pagrįstas pastangas, kad informuotų asmenį, kuris gali naudotis sistema, kuria perduodama komunikacija gali būti pažeista (3.2 dalis).

Darbdaviai, besiiimantys stebėjimo, kuris, kaip paprastai, reikalauja asmens duomenų tvarkymo, privalo elgtis pagal 1998 m. Duomenų apsaugos aktą. Informacijos įgaliotinis išleido konsultacijų praktikos kodekso projektą. Jis nustato, kaip Akto reikalavimai taikomi sekimui darbo vietoje praktiškai.