



11750/02/EN
WP 89

Nuomonė dėl asmens duomenų tvarkymo vaizdo stebėjimo priemonėmis

Priimta 2004 m. vasario 11 d.

Darbo grupė buvo įsteigta vadovaujantis Direktyvos 95/46/EB 29 straipsniu. Tai nepriklausomas ES patariamasis organas duomenų apsaugos ir privatumo klausimais. Jos uždaviniai išdėstyti Direktyvos 95/46/EB 30 straipsnyje ir Direktyvos 97/66/EB 14 straipsnyje.

Sekretariatą teikia Europos Komisijos E direktoratas (paslaugos, intelektinė ir industrinė nuosavybė, žiniasklaida ir duomenų apsauga), Generalinis vidaus rinkos direktoratas, B-1049 Brussels, Belgium, Office No C100-6/136. Interneto adresas: www.europa.eu.int/comm/privacy

DARBO GRUPĖ ASMENŲ APSAUGAI TVARKANT ASMENS DUOMENIS

Sudaryta pagal Europos Parlamento ir Tarybos 1995 m. spalio 24 d. direktyvą 95/46/EB¹,
atsižvelgiant į šios Direktyvos 29 ir 30 straipsnių 1(a) ir 3 dalis,
atsižvelgiant į jos Procedūros taisykles ir ypač į 12 ir 14 straipsnius,

PRIĖMĖ ŠIA NUOMONĖ:

1. Įžanga

Europoje per pastaruosius kelerius metus vis daugiau valstybinių ir privačių įstaigų įsirengia vaizdo atgaminimo sistemas. Ši aplinkybė sukėlė gyvus debatus Bendrijoje ir atskirose valstybėse narėse dėl būtinų sąlygų ir apribojimų, taikytinų vaizdo stebėjimo įrangos įrengimui, ir būtinų duomenų subjektų apsaugos nustatymo.

Pastaraisiais metais sukaupta patirtis ir Direktyvos 95/46/EB perkėlimas į nacionalinį lygmenį parodė didžiulį uždarų sistemų, kamerų ir kitų sudėtingesnių prietaisų, kurie yra naudojami įvairiausiose sferose, paplitimą.

Be to, prieinamų technologijų plėtra, kompiuterizavimas ir prietaisų mažėjimas, taip pat jų panaudojimas intranetuose ir internete gerokai padidina vaizdo ir garso įrašymo įrangos teikiamas galimybes.

Be tvarkymo operacijų darbo santykių kontekste, ką Darbo Grupė jau aptarė detaliame dokumente (*Nuomonė 8/2001 dėl asmens duomenų tvarkymo darbo santykių kontekste*²), vaizdo stebėjimo technikos paplitimą lengvai gali įvertinti visi piliečiai. Taip pat stiprėja vaizdo stebėjimo sistemų jungimo tendencija.

Neišsami pagrindinių taikymo būdų analizė rodo, kad vaizdo stebėjimas gali tarnauti visiškai skirtingiems tikslams³, kuriuos galima sugrupuoti į kelias pagrindines sritis:

¹ Official Journal 1995-11-23 no. L 281, p. 31, paskelbta:

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

² WP 48, priimta 2001 m. rugsėjo 13 d., skelbiama:

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

³ Skirtingos vaizdo stebėjimo sistemos yra įrengiamos:

- a) visuomeniniuose ir (arba) visuomenės lankomuose pastatuose ar šalia jų, pvz., muziejuose, maldos vietose ar šalia paminklų, norint išvengti nusikaltimų ir (arba) mažesnių vandalizmo aktų,
- b) stadionuose ir sporto kompleksuose, ypač dėl konkrečių renginių,
- c) transporto sektoriuje ir ryšium su kelių eismu, siekiant kontroliuoti eismą magistralėse ir greitkeliuose ar kitur, arba nustatyti greičio ribojimo ir (arba) eismo taisyklių pažeidimus miestų centruose ar kitur, kontroliuoti metropoliteno patalpas, siekiančias metro linijas, stebėti degalines ir taksi automobilių vidų,
- d) neteisėto elgesio mokyklų prieigose prevencijai ir (arba) nustatymui, taip pat ryšium su nepilnamečių užkabinėjimu,
- e) ligoninių patalpose operacijų metu ir (arba), pavyzdžiui, teikiant pagalbą per atstumą, arba stebint pacientus intensyviosios priežiūros skyriuose ir (arba) vietose, kur sunkiai sergantys ir (arba) dėl karantino izoliuoti pacientai yra hospitalizuoti,
- f) oro uostuose, laivuose ir pasienio zonose tam, kad būtų galima stebėti kontrabandininkus ir palengvinti nepilnamečių ir kitų dingusių asmenų paiešką,
- g) privačių detektyvų,

- 1) asmenų apsauga,
- 2) nuosavybės apsauga,
- 3) visuomenės interesai,
- 4) nusikaltimų nustatymas, prevencija ir kontrolė,
- 5) galimybė gauti įrodymus,
- 6) kiti teisėti interesai.

Vaizdo kamerų ir panašių prietaisų įrengimui taikomos skirtingos sąlygos.

Kai kuriais atvejais, vadovaujantis konkrečiomis valstybės narės nuostatomis, naudoti vaizdo įrašymo sistemą gali būti privaloma, pavyzdžiui, tokių atvejų pasitaikė keliose kazino, arba sistema gali tarnauti tikslui, kuris yra labai svarbus duomenų subjekto giminaičiams, pavyzdžiui, ieškant dingusių vaikų ir suaugusiųjų. Antra vertus, galima paminėti tokio naudojimo kraštutinius atvejus, daugiausia susijusius su trečiosiomis šalimis, kai veidų atpažinimo sistema naudota tam, kad būtų užkirstas kelias bigamijai, arba kai vietos policijos valdžia nusprendė viešai rodyti sunkaus gyvenimo kalėjime vaizdus, negavusi nuteistųjų sutikimo.

Taigi, nors vaizdo stebėjimas tam tikromis aplinkybėmis yra pateisinamas, yra atvejų, kai vaizdo kameros apsaugai naudojamos impulsyviai, nepakankamai apgalvojus būtinas sąlygas ir nepasirengus. Kartais taip daroma dėl ekonominės naudos, kurią gauna daugybė viešųjų įstaigų, arba dėl geresnių draudimo sąlygų pasiūlymų, jei naudojama vaizdo stebėjimo įranga.

Yra pastebimas su vaizdo stebėjimu susijęs psichologinis efektas, kuris ne visada teisingai, visuomenės yra suprantamas kaip „neįkainojamas įrankis“ nusikaltimų atskleidimui.

Todėl tai yra įvairi, nuolat besivystanti sritis, kurioje naudojami keli metodai.

Šiame darbo dokumente pateikiama pirminė analizė, pradedant nuo esančių iš dalies skirtingų taisyklių, taip pat nuo labai smulkių atskirų nacionalinių įstatymų nuostatų, kurias reikia susisteminti ir suderinti.

Šiame darbo dokumente nagrinėjamas stebėjimas, skirtas įvykių, situacijų ir reiškinių stebėjimui iš nuotolio, tačiau čia tiesiogiai nesvarstomi kiti atvejai, kai apie konkrečius įvykius yra skelbiama atsitiktinai ir (arba) tendencingai, pavyzdžiui, dėl vietos valdžios ir (arba) parlamento veiksmų skaidrumo.

Be to, čia pateikiami principai taikomi vaizdo atkūrimui, galbūt siejant su garsiniais ir (arba) biometriniais duomenimis, pavyzdžiui, pirštų atspaudų duomenimis⁴.

Paminėtų principų gali būti paisoma, kai jie taikytini konkrečiai asmens duomenų gautų naudojant ne vaizdo įrašymo priemones, bet kitus stebėjimo būdus, t. y. distancinio valdymo priemones, pavyzdžiui, satelitinę GPS sistemą, tvarkymui.

h) prekybos centruose bei parduotuvėse ir šalia jų, ypač jei jose prekiaujama prabangos prekėmis, kad būtų galima gauti įrodymų, jei padaromas nusikaltimas, taip pat prekių pardavimo ir (arba) pirkėjų apibūdinimo tikslais,

i) privačiose valdose ir šalia jų esančiose teritorijose dėl apsaugos ir tam, kad būtų gauti įrodymai, jei įvykdomas nusikaltimas,

j) žurnalistiniais ir reklamos tikslais, kurių siekti padeda „web“ arba „online“ (sujungtos su kompiuteriu) kameros, naudojamos turistų ir reklamuojant, kai paplūdimiuose ar šokių aikštelėse klientai ir lankytojai filmuojami vienodais intervalais be jokio įspėjimo.

⁴ Direktyvos 95/46/EB taikymo biometriniais duomenimis klausimas yra aptartas Darbo Grupės atskirame dokumente.

Šis darbo dokumentas visų pirma skirtas atkreipti dėmesį į daugybę kriterijų, padedančių nustatyti, ar tam tikros vaizdo stebėjimo sistemos įdiegimas yra teisėtas ir tinkamas.

Tačiau reikia atsižvelgti ir į šiuos aspektus:

a) Atitinkamos valstybių narių institucijos turi įvertinti vaizdo stebėjimą apskritai, taip pat skatinti selektyvų ir sisteminių požiūrį į šiuos dalykus. Dėl vaizdo kaupimo sistemų greito plitimo visuomeninėse ir privačiose sferose neturi atsirasti nepateisintų piliečių teisių ir pagrindinių laisvių apribojimų, kitaip piliečiai gali būti priversti patirti neproporcingas duomenų rinkimo procedūras, dėl kurių bus masiškai nustatoma jų tapatybė daugelyje viešųjų ir privačių vietų.

b) Gali būti įvertintos vaizdo stebėjimo metodų evoliucijos kryptys, kad būtų užkirstas kelias vystymuisi programinės įrangos, kuri remiasi veidų atpažinimu ir vaizduojamo žmogaus elgesio studijavimu bei prognozavimu nuo atliekamo neapgalvotai iki dinaminio-prevencinio stebėjimo – priešingo tradiciniam statiškam sekimui, kurio tikslas daugiausia yra dokumentuoti ypatingus įvykius ir jų autorius. Ši nauja stebėjimo forma remiasi automatinio asmenų veido bruožų ir jų „nenormalaus“ elgesio atpažinimo, jungimu su automatizuotais pavojaus signalais ir užuominomis, kurios gali sukelti diskriminacijos grėsmę.

2. TARPTAUTINIAI TEISĖS AKTAI

a) Žmogaus teisių ir pagrindinių laisvių konvencija.

Privatumo apsauga yra užtikrinta Žmogaus teisių konvencijos 8 straipsnyje.

b) Europos Tarybos Konvencija Nr. 108/1981 dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu.

Šios Konvencijos veikimo sritis nėra ribota, kaip kad Direktyvos 95/46/EB veikimo sritis apima tik pirmąjį ramstį (žr. žemiau). Vaizdo stebėjimo veikla, sukianti asmens duomenų tvarkymą, patenka į šios Konvencijos taikymo sritį. Pagal šią Konvenciją įkurtas Konsultacinis komitetas konstatavo, kad balsai ir atvaizdai yra laikomi asmens duomenimis, jei jie suteikia informaciją apie asmenį, dėl ko jo tapatybė gali būti nustatoma, net jei ir netiesiogiai.

Šiuo metu Europos Taryba baigia rengti pagrindinių principų rinkinį dėl asmenų apsaugos ryšium su duomenų rinkimu ir tvarkymu vaizdo stebėjimo priemonėmis. Šie principai turėtų patikslinti duomenų subjektui taikomas apsaugos priemones, nurodytas Europos Tarybos dokumentų nuostatose.

c) Europos Sąjungos Pagrindinių teisių chartija.

Europos Sąjungos Pagrindinių teisių chartijos 7 straipsnyje yra numatyta privatus ir šeimos gyvenimo, namų ir ryšių apsauga, o 8 straipsnyje – asmens duomenų apsauga.

3. STEBĖJIMAS PAGAL DIREKTYVĄ 95/46/EB

Specifinės, asmeninės informacijos, įeinančios į garsinius ir vaizdinius duomenis, tvarkymo ypatybės yra išryškintos Direktyvoje 95/46/EB (toliau – Direktyva), kurioje apie tai aiškiai kalbama keliuose punktuose.

Direktyva užtikrina privatumo ir privataus gyvenimo apsaugą, taip pat platesnį asmens duomenų apsaugos diapazoną, atsižvelgdama į fizinio asmens pagrindines teises ir laisves (1 str., 1 par.).

Didelė dalis vaizdo stebėjimo priemonėmis surenkamos informacijos yra susijusi su asmenimis, kurių tapatybė yra ir (arba) gali būti nustatyta, kurie buvo nufilmuoti, kai jie įeidavo į visuomenines ir (arba) visuomenei prieinamas patalpas. Toks asmuo gali tikėtis mažiau privatumo, tačiau jis nesitiki visiškai netekiantis savo teisių ir laisvių, taip pat ir tų, kurios liečia jo privačią sferą bei atvaizdą.

Reikėtų aptarti ir teisėtai esančių valstybės teritorijoje asmenų teisę laisvai judėti, kuri garantuojama Europos Žmogaus teisių ir pagrindinių laisvių konvencijos Papildomo protokolo Nr. 4 2 straipsnyje.

Ši judėjimo laisvė gali būti varžoma tik tada, kai tai būtina demokratinėje visuomenėje ir atitinka konkretų tikslą, kurio yra siekiama. Duomenų subjektai turi teisę naudotis savo judėjimo laisve, nepatirdami pernelyg didelio psichologinio poveikio dėl savo judėjimo ir elgesio, taip pat neturi būti detaliam kontroliuojami, pvz., sekamas jų judėjimas ir (ar) skelbiami „pavojaus signalai“, kurie veikia programinės įrangos, kuri automatiškai, be jokio žmogaus įsikišimo, „interpretuoja“ asmens spėjimai įtartiną elgesį – atsižvelgiant į neproporcingą vaizdo stebėjimo sistemų taikymą, kai kuriose viešosiose ir (arba) visuomenei prieinamose patalpose, pagrindu.

Su fiziniu asmeniu susijusių garsinių ir vaizdinių duomenų tvarkymo specifiškumas yra pabrėžiamas Direktyvos pirmosiose konstatuojamosiose dalyse. Šalia žemiau dėstomo svarstymo dėl taikymo srities, šios Direktyvos konstatuojamosiose dalyse ir atitinkamuose straipsniuose aiškinama, kad:

a) iš esmės Direktyva yra taikoma šioje srityje, suvokiant vykstančių pokyčių svarbą, visuomenės informuotumo lygį ir būdus surinkti, persiųsti, manipuliuoti, įrašyti, saugoti ar perduoti su fiziniais asmenimis susijusius garsinius ir vaizdinius duomenis (žr. konstatuojamąjį dalį Nr. 14),

b) Direktyvoje pateikti apsaugos principai taikomi bet kokiai informacijai, įskaitant ir garsinę bei vaizdinę informaciją, apie asmenis, kurių tapatybė yra nustatyta arba gali būti nustatyta, atsižvelgiant į visas priemones, pagrįstai naudojamas valdytojo ar kito asmens, kad būtų nustatyta minėtų asmenų tapatybė (žr. 2 straipsnio a) punktą ir konstatuojamąjį dalį Nr. 26).

Be išdėstytų konkrečių nuorodų, Direktyva aiškiai parodo, kaip veikia atskiros jos nuostatos, susijusios su:

1) *duomenų kokybe*. Atvaizdai turi būti tvarkomi teisingai bei teisėtai ir tiksliai, apibrėžtais, aiškiais ir teisėtais tikslais. Atvaizdai turi būti naudojami vadovaujantis principu, kad duomenys turi būti adekvatūs, tinkami ir nepertekliniai, bei toliau tvarkomi su šiais tikslais suderinamu būdu; taip pat jie turi būti saugomi ribotą laiką ir t.t. (žr. 6 straipsnį);

2) *duomenų tvarkymo teisėtumo kriterijais*. Remiantis šiais kriterijais, asmens duomenų tvarkymą vaizdo stebėjimo priemonėmis yra svarbu pagrįsti bent viena būtina sąlyga, paminėta 7 straipsnyje: nedviprasmišku sutikimu, būtinais sutartiniais įsipareigojimais, teisinių prievolių laikymusi, duomenų subjekto gyvybinių interesų apsauga,

visuomenės labai atliekamos užduoties vykdymu arba tvarkymu įgyvendinant oficialius įgaliojimus, interesų derinimu;

3) *ypatingų duomenų kategorijų* tvarkymu, kuris yra apsaugos priemonių, taikomų ypatingiems duomenims arba duomenims, susijusiems su pažeidimais vykdant vaizdo stebėjimą, objektas (pagal 8 straipsnį);

4) duomenų subjekto *informavimu* (žr. 10 ir 11 straipsnius);

5) *duomenų subjekto teisėmis*, ypač teisė gauti informaciją ir teisė prieštarauti tvarkymui, remiantis privalomu teisėtu pagrindu (žr. 12 ir 14 a straipsnius);

6) apsaugos priemonėmis, taikomomis ryšium su *automatiniais individualiais sprendimais* (pagal 15 straipsnį);

7) tvarkymo operacijų *saugumu* (17 straipsnis);

8) *pranešimu apie tvarkymo operacijas* (pagal 18 ir 19 straipsnius);

9) tvarkymo operacijų, galinčių kelti konkretų pavojų duomenų subjekto teisėms ir laisvėms, *išankstine patikra* (pagal 20 straipsnį) ir

10) *duomenų perdavimu trečiosioms šalims* (pagal 25 straipsnį ir kt.).

Garsinių ir vaizdinių duomenų tvarkymo specifiškumas galiausiai yra pripažįstamas Direktyvos paskutiniame straipsnyje, kuriame Komisija įsipareigoja ištirti, kaip Direktyva yra taikoma aptariamajam dalykui, ir pateikti atitinkamus reikalingus pasiūlymus atsižvelgiant į informacijos technologijų vystymąsi ir informacinės visuomenės progreso lygį (žr. 33 straipsnį).

4. VAIZDO STEBĖJIMUI TAIKOMOS NACIONALINĖS NUOSTATOS

Keliose valstybėse narėse atlikti tyrimai dėl vaizdo stebėjimo, paremti konstitucinėmis nuostatomis⁵ arba konkrečiais teisės aktais, potvarkiais ar kitais sprendimais, išleistais kompetetingų nacionalinių institucijų⁶.

Keliose šalyse taip pat yra taikomos konkrečios nuostatos, nepaisant aplinkybės, kad vaizdo stebėjimas sukelia asmens duomenų tvarkymą. Pagal šį reglamentavimą, CCTV ir panašios stebėjimo įrangos instaliavimas ir išdėstymas galimas tik iš anksto leidus administracinei institucijai, kurią visiškai ar iš dalies gali atstovauti nacionalinė duomenų apsaugos institucija. Toks reglamentavimas gali skirtis, atsižvelgiant į tai, ar už atitinkamos įrangos naudojimą yra atsakingi privatūs, ar valstybiniai subjektai.

Kitose šalyse vaizdo stebėjimas nėra konkrečių įstatymų objektas, tačiau duomenų apsaugos institucijos dirba tam, kad užtikrintų tinkamą bendrųjų duomenų apsaugos nuostatų taikymą, *inter alia* pateikdamos nuomones, rekomendacijas ar elgesio kodeksus, pvz., kurie

⁵ Žr. Portugalijos Konstitucinio Teismo Sprendimą 255/2002. Teismas nusprendė, kad „elektroninių stebėjimo prietaisų naudojimas ir piliečių stebėjimas, vykdomas privačių apsaugos institucijų yra teisės į privataus gyvenimo saugojimą, kuriam skirtas Konstitucijos 26 straipsnis, ribojimas arba suvaržymas“.

⁶ Mažiausiai vienoje šalyje (Belgijoje – Gaia byla) dėl atvaizdų rinkimo ne pagal duomenų apsaugos įstatymus buvo atsisakyta leistinių įrodymų Teisme.

jau yra priimti Jungtinėje Karalystėje ir rengiami Italijoje.

Belgija	DAI nuomonės, ypač 1999 m. gruodžio 13 d. nuomonė 34/1999, susijusi su atvaizdų tvarkymu, ypač naudojant vaizdo stebėjimo sistemas; 2000 m. sausio 10 d. nuomonė 3/2000 susijusi su vaizdo stebėjimo sistemų panaudojimu prie įėjimų į gyvenamuosius namus.
Danija	<p>2000 m. vasario 1d. Konsolidacijos aktas Nr. 76 dėl vaizdo stebėjimo draudimo. Šis aktas apskritai uždraudžia privatiems asmenims vykdyti vaizdo stebėjimą viešose gatvėse, keliuose, skveruose ar bet kokiose kitose panašiose vietovėse, visų naudojamose kelionėms. Vis dėl to šis draudimas turi konkrečių išimčių.</p> <p>2002 m. birželio 3 d. DAI sprendimas dėl vaizdo stebėjimo, vykdomo didelės grupės prekybos centrų ir „gyvų“ transliacijų internete iš baro.</p> <p>2003 m. liepos 1 d. DAI sprendimas kuriame nurodoma, kad vaizdo stebėjimas, vykdomas privačiai eksploatuojamame viešame transporte, turi būti proporcingas ir vykdomas griežtai laikantis taisyklių, nustatytų Danijos Duomenų apsaugos akte.</p> <p>2003 lapkričio 13 d. DAI sprendimas, nustatantis konkrečius ribojimus viešųjų institucijų vykdomam vaizdo stebėjimui.</p>
Suomija	<p>Suomijoje nėra jokių specialių teisės aktų dėl vaizdo stebėjimo, bet įvairiuose įstatymuose yra nuostatų dėl vaizdo stebėjimo ir kitokio techninio stebėjimo, priežiūros ar kontrolės.</p> <p>Klausimai dėl vaizdo stebėjimo ir pokalbių įrašymo yra dažnai užduodami ir mes turėjome keletą atvejų.</p> <p>Pavyzdžiui, Duomenų apsaugos ombudsmenas yra pareiškęs savo nuomonę dėl telefono pokalbių įrašymo klientų aptarnavimo ir darbo sferoje (įrašo numeriai 1061/45/2000 ir 525/45/2000).</p> <p>Mūsų biuras yra išleidęs brošiūrą „Privatumas vaizdo stebėjime“ (Asiaa tietosuojasta 4/2001 Yksitysyiden suoja kameravalvonnassa http://www.tietosuoja.fi/uploads/03wamgvxuybt4ti.rtf)</p>
Prancūzija	<p>1978 m. sausio 6 d. aktas Nr. 78-17 dėl tvarkymo, bylų ir laisvių (CNIL)</p> <p>1994 m. birželio 21 d. DAI rekomendacija Nr. 94-056</p> <p>DAI vadovas, susijęs su vaizdo stebėjimu darbo vietoje: http://www.cnil.fr/thematic/index.htm; kitais klausimais (pvz., internetinių kamerų)⁷</p> <p>Konkretus aktas, susijęs su vaizdo stebėjimu dėl visuomenės saugumo viešose vietose: 1995 m. sausio 21 d. Aktas Nr. 95-73 dėl saugumo (pataisytas 2000m. rugsėjo 19 d. Ordonnance 2000-916)</p> <p>1996 m. spalio 17 d. Dekretas Nr. 96-926 ir 1996 m. spalio 22 d. Aplinkraštis dėl Akto Nr. 95-73 įgyvendinimo.</p>

⁷ Žr. Prancūzijos Commission Nationale de l'Informatique et des Libertés metines ataskaitas.

Graikija	<p>1) 2000 m. sausio 28 d. raštas Nr. 390, susijęs su uždaros sistemos televizija Atėnų metropolitene</p> <p>2) 2000 m. rugsėjo 26 d. direktyva Nr. 1122 dėl uždaros sistemos televizijos</p> <p>3) Sprendimas Nr. 84/2002 dėl uždaros sistemos televizijos viešbučiuose</p>
Vokietija	<p>2001 m. Federalinio Akto 6 b skyrius.</p> <p>Sienų apsaugos įstatymo 25 skyrius.</p> <p>Tolesni reglamentai dėl vaizdo stebėjimo, vykdomo policijos, Länder Policijos įstatymuose.</p> <p>Bilis uždraudžiantis slapta vaizdo stebėjimą yra svarstomas Parlamente.</p>
Airija	<p>1998 m. ir 2003 m. Duomenų apsaugos aktas. Bylos studija Nr. 14/1996 (CCTV naudojimas)</p>
Italija	<p>Asmens duomenų apsaugos kodekso 134 skyrius (2003 m. birželio 30 d. įstatyminis dekretas Nr. 196, numatantis elgesio kodekso priėmimą)</p> <p><i>Garante</i> sprendimai: 2002 m. balandžio 10 d. Nr. 2 (raginantis priimti elgesio kodeksus), 2001 m. rugsėjo 28 d. (bankuose taikomi biometrinių ir veidų atpažinimo metodai) ir 2000 m. lapkričio 29 d. (vadinamasis „vaizdo stebėjimo dekalogas“)</p> <p>1999-06-22 Prezidento dekretas Nr. 250 (reguliuojantis transporto priemonių judėjimą miestų centruose ir draudžiamose zonose)</p> <p>1992-11-14 Dekretas Nr. 433 ir Aktas Nr. 4/1993 (taikomas muziejams, valstybinėms bibliotekoms ir archyvams)</p> <p>2000-02-04 Įstatyminis dekretas Nr. 45 (dėl keleivinių laivų nacionaliniuose laivybos keliuose)</p> <p>1970-05-20 Akto Nr. 300 4 skyrius (vadinamasis Darbininko Statutas)</p>
Liuksemburgas	<p>2002-08-02 Įstatymo dėl asmenų apsaugos ryšium asmens duomenų tvarkymu 10 ir 11 straipsniai</p>
Nyderlandai	<p>1997 m. Duomenų apsaugos institucijos ataskaita su gairėmis dėl vaizdo stebėjimo, ypač dėl asmenų ir nuosavybės apsaugos viešose vietose. Gairių, išleistų 1997 m., atnaujinimas bus parengtas 2004 m.</p> <p>2003 m. vaizdo kamerų stebėjimo tyrimas visuose Olandijos municipalitetuose</p> <p>Žemuosiuose rūmuose priimti Bausmių kodekso pakeitimai, kurie praplėtė baudžiamojo nusižengimo apimtį iki fotografavimo/filmavimo neinformavus visuomenę prieinamose vietose, įsigalioję nuo 2004 m. sausio 1 d.</p> <p>Vyriausybė siūlo pakeisti Vietinį Vyriausybės aktą, kuris aiškiai nurodo miesto taryboms ir merams naudoti vaizdo stebėjimo sistemas viešose teritorijose dėl visuomenės interesų tik esant konkrečioms sąlygoms</p>

	(pavyzdžiui, periodiškai įvertinti vaizdo stebėjimo efektyvumą).
Portugalija	1998 m. liepos 22d. Dekretas-Įstatymas 231/98 (privati saugos veikla ir savisaugos sistemos) 1998 m. rugpjūčio 4 d. Įstatymas 38/98 (priemonės, kurių reikia imtis prievartos sporto renginiuose atveju) 2001 m. rugsėjo 28 d. Dekretas-Įstatymas 263/01 (dėl šokių vietų) 2002 m. balandžio 12 d. Dekretas-Įstatymas 94/2002 (dėl sporto renginių)
Ispanija	<i>Ley organica</i> Nr. 4/1997 (saugos agentūrų viešose vietose atliekamas vaizdo stebėjimas) <i>Real Dekreto</i> Nr. 596/1999, įgyvendinantis Aktą Nr. 4/1997
Švedija	Vaizdo stebėjimas yra konkrečiai reglamentuotas Akte (1998:1506) dėl slapto vaizdo stebėjimo (atliekant baudžiamąjį tyrimą) ⁸ . Bendram vaizdo stebėjimui paprastai reikalingas grafystės administracinės tarybos leidimas. Tačiau, pavyzdžiui, pašto skyrių, bankų ir parduotuvių stebėjimui nėra reikalingi leidimai. Slaptas vaizdo stebėjimas turi būti vykdomas tik su teismo leidimu. Grafystės administracinės tarybos sprendimai gali būti skundžiami Teisingumo kancleriui. Vaizdo įrašymas skaitmeniniu būdu yra laikomas asmens duomenų tvarkymu ir patenka į Duomenų inspekcijos Tarybos priežiūros sferą, kuri nėra konkrečiai reguliuojama Bendrojo vaizdo stebėjimo akte. Tyrimų komisija yra publikavusi pranešimą dėl vaizdo stebėjimo (SOU 2002:110).
Jungtinė Karalystė	2000 m. CCTV praktikos kodeksas (Informacijos komisionierius), šiuo metu peržiūrimas.

Papildomi svarbūs kontrolės dokumentai taip pat priimti Islandijoje (Akto Nr. 77/2000 4 skyrius), Norvegijoje (2000-04-14 Akto Nr. 31 VII antraštė), Šveicarijoje (Federalinio komisieriaus rekomendacija) ir Vengrijoje (2000-12-20 DAI rekomendacijos).

5. SRITYS, KUR DIREKTYVA 95/46/EB VISIŠKAI AR IŠ DALIES NETAIKOMA

Direktyva netaikoma garsinių ir vaizdinių duomenų tvarkymui visuomenės saugumo, gynybos, valstybės saugumo ir valstybės veiksmų baudžiamosios teisės srityje ir (arba) kitokios veiklos, kuriai netaikomi Bendrijos įstatymai⁹, tikslais. Vis dėlto, daugelis valstybių narių, perimdamos Direktyvą 95/46/EB, apėmė šiuos klausimus bendrai, nustatydamos konkrečias išimtis.

A) Kai kuriose šalyse išvardytais tikslais atliekamoms tvarkymo operacijoms bet kokių atveju taikomos apsaugos priemonės pagal Konvenciją Nr. 108/1981 ir atitinkamas Europos Tarybos rekomendacijas, taip pat tam tikras nacionalines nuostatas (žr. Direktyvos

⁸

⁹ Žr. 16 konstatuojamąją dalį.

95/46/EB 3(2) straipsnį ir konstatuojamąją dalį Nr. 16). Atsižvelgiant į specifinius bruožus ir esančias konkrečias nuostatas, taip pat susijusias su policijos ar teismo organų vykdoma tyrimo veikla nacionalinio saugumo tikslais¹⁰, kur gali būti atliekamas „slaptas“ vaizdo stebėjimas, t.y. vykdomas neinformuojant, tokios kategorijos tvarkymas šiame dokumente detalai nebus aptariamas.

Tačiau Darbo Grupė norėtų pabrėžti, kad panašiai, kaip vykdant kelias kitas asmens duomenų tvarkymo operacijas, kurioms atliekant vaizdo stebėjimą netaikoma Direktyva, dėl visuomenės saugumo arba kriminalinių nusikaltimų tyrimo, prevencijos ir kontrolės tikslais, reikia laikytis Žmogaus teisių ir pagrindinių laisvių konvencijos 8 straipsnyje išdėstytų reikalavimų, remtis konkrečiomis visuomenei žinomomis nuostatomis, sieti ir išlaikyti proporciją su *konkrečios* rizikos ir *konkrečių* nusikaltimų prevencija, pvz., vietose, kur gali kilti tokia rizika, arba visuomeniniuose renginiuose, kurių metu gali būti įvykdyti tokie nusikaltimai¹¹. Reikia atsižvelgti į vaizdo stebėjimo sistemų daromą poveikį, pvz., į tą faktą, kad neteisėti veiksmai gali persikelti į kitas vietas ar sektorius, todėl duomenų valdytojas visada turi būti aiškiai nurodytas, kad duomenų subjektai galėtų įgyvendinti savo teises.

Pastarasis reikalavimas taip pat yra susijęs su aplinkybe, kad vaizdo stebėjimas vis dažniau yra vykdomas policijos kartu su kitomis valdžios institucijomis (pvz., vietinės valdžios organais) ir (arba) privačiomis organizacijomis (bankais, sporto asociacijomis, transporto kompanijomis), dėl ko kyla rizika, kad taps neiškus kiekvieno individualus vaidmuo ir atsakomybė už atliekamą užduotį¹².

B) Antra, Direktyva netaikoma, kai fizinis asmuo atlieka tvarkymo operacijas tik užsiimdamas asmenine ar namų ūkio veikla (žr. 3(2) straipsnį ir konstatuojamąją dalį Nr. 12).

Nors aukščiau minėtos sąlygos galioja, jei vaizdo stebėjimo priemonės įdiegiamos tam, kad galima būtų iš nuotolio stebėti, kas vyksta kieno nors namo viduje, pvz., siekiant užkirsti kelią vagystėms arba ryšium su vadinamąja e-šeima, jos netaikomos, jei vaizdo stebėjimo įranga įrengiama išorėje arba šalia privačių valdų, siekiant saugoti nuosavybę ir (arba) užtikrinti saugumą.

Pastaraisiais atvejais gali būti, kad dėl durų stebėjimo sistema išdėstoma ne individualių savininkų jiems priklausančiose prieigose, bet kelių susitarusių savininkų, konsorciumo ar bendrasavininkų, kad galima būtų stebėti keletą įėjimų ir aplinką prie namų, o tokiai veiklai yra taikoma Direktyva.

Tačiau, kai sistema naudojasi tik individuali šeima ir stebimos tik vienos durys, laiptų aikštelė, automobilių stovėjimo vieta ir t.t., faktas, kad Direktyva netaikoma, dėl naudojimo išimtinai asmeniniais tikslais, kaip ir dėl duomenų neprieinamumo trečiosioms šalims, neatleidžia sistemos valdytojo nuo įstatymais garantuojamų teisių ir jo kaimynų bei kitų

¹⁰ Šiuo atveju galima remtis Europos žmogaus teisių teismo principais, išdėstytais Rotaru prieš Rumuniją byloje, nagrinėtoje 2000 m. gegužės 4 d. Žr. aukščiau.

¹¹ Pavyzdžiui, Prancūzijoje 1996-10-22 išleistas aplinkraštis apie izoliuotas vietas ir vėlai naktį uždaromas parduotuves.

¹² Reikšmingas rizikos pavyzdys yra kelių Italijos municipalitetų vykdoma veikla, siekiant vaizdo stebėjimo priemonėmis stebėti viešąsias vietas, kur naktimis renkasi prostitutės. Kai kurie municipalitetai praeityje skelbė – labai abejotinai – kad jie yra kompetetingi užkirsti kelią šiam reiškiniiui, kai kiti municipalitetai išleido įsakymus, tik draudžiančius prostitučių klientams parkuoti savo mašinas ir (arba) važiuoti tose vietose, grasindami atsiųsti nuotraukas jiems į namus, jei šie nepaklustų. Italijos institucija priėmė nutarimą, siekdama išaiškinti, kokia atsakomybė gresia už atitinkamų nuostatų pažeidimą.

asmenų interesų gerbimo. ES valstybėse narėse šias teises ir interesus saugo, nepriklausomai nuo duomenų apsaugos principų, bendrieji (civilinės teisės) nuostatai, skirti asmens teisių, atvaizdo, šeimos gyvenimo ir privačios sferos apsaugai. Tik pagalvokite, pavyzdžiui, apie kamerą, nustatytą prie buto lauko durų tokiu kampu, kuris leidžia sistemiskai nufilmuoti medicinos klinikos ir (arba) teisinės firmos, esančios tame pačiame aukšte, klientus ir taip neteisėtai kištis į profesines paslaptis.

Ypatingą dėmesį reikia skirti vaizdo įrangos orientavimui, žinučių ir informacijos iškabinimui ir savalaikiam įrašytų vaizdų ištrynimui, kuris turi būti atliktas per kelias valandas, jei nebuvo įsilaužimo į namus ar jokių nusikaltimų.

C) Pagaliau Direktyvos 9 straipsnyje numatyta, kad valstybės narės nustato kai kurių jos nuostatų išimtis ar nukrypimus nuo jos, kai tvarkymas atliekamas tik žurnalistiniais arba literatūrinės ar meninės raiškos tikslais, ypač garsinėje-vaizdinėje srityje (žr. konstatuojamąją dalį Nr.17). Turi būti nustatomos tik tokios išimtys, kurios suderina teisę į privatumą su taisyklėmis, reguliuojančiomis raiškos laisvę¹³. Todėl ypatingo atidumo reikalauja „web“ kamerų ir (arba) „on line“ kamerų įrengimas, kad nebūtų asmenų apsaugos klaidų ir spragų, kai vaizdo stebėjimo priemonės gali būti naudojamos reklamos ir turizmo skatinimo tikslais¹⁴.

6. VAIZDO STEBĖJIMAS IR ASMENS DUOMENŲ TVARKYMAS

Atsižvelgiant į įvairias minėtas situacijas, Darbo grupė laikosi nuomonės, kad reikia atkreipti dėmesį į tai, kad Direktyva 95/46/EB taikoma asmens duomenų tvarkymui automatinio ar iš dalies automatinio būdu, įskaitant vaizdinių ir garsinių duomenų tvarkymą CCTV ir kitomis vaizdo stebėjimo sistemomis, ir dalį rinkmenos sudarančių asmens duomenų, tvarkymą kitokiu nei automatinio būdu.

Vaizdo ir garso duomenys, kurie susiję su fiziniu asmeniu, kurio tapatybė yra arba gali būti nustatyta, yra asmens duomenys:

a) net jei jie naudojami uždaroje sistemoje, net jei jie nėra susiję su asmens ypatybėmis,

b) net jei jie nesusiję su asmenimis, kurių veidai buvo nufilmuoti, nors apima kitokią informaciją, tokią kaip, pavyzdžiui, automobilio numeris ar PIN skaičiai, užfiksuojami stebint bankomatus,

c) nepaisant tvarkymo priemonės, (pvz., stacionarios ir (arba) mobilios vaizdo sistemos, tokios kaip nešiojami televizoriai, spalvoti ir (arba) balta-juoda atvaizdai), naudojamos technikos (laidinės ar optinio kabelio priemonės), įrangos tipo (stacionari, besisukanti, mobili), vaizdo įrašymo ypatybių, (pvz., nepertraukiamas priešinamas nutraukiamam, kuris gali būti, kai vaizdas įrašomas tik tada, kai nepaisoma greičio ribojimo ir toks įrašymas nesusijęs su visiškai atsitiktiniu, nesuderintu filmavimu) ir naudojamų komunikacijos priemonių (pvz., ryšys su „centru“ ir (arba) vaizdo perdavimas tolesniems terminalams), ir t.t.

Pagal Direktyvą, tapatybė gali būti nustatyta derinant duomenis su trečiosios šalies turima informacija arba atskirais atvejais taikant konkrečią techniką ir (arba) prietaisus.

¹³ Žr. Darbo grupės duomenų apsaugos įstatymui ir žiniasklaidai Rekomendaciją 1/97.

¹⁴ Milane slapta įrengta prie metro stoties laiptų „web“ kamera tiesiogiai į Tinklą perduodavo praeinančių moterų slaptų vietų vaizdus tik, atrodytų, žurnalistiniais tikslais. Dėl to, kad vaizduojamo asmens tapatybės nebuvo galima nustatyti, neleido nacionalinei duomenų apsaugos institucijai imtis kokių nors veiksmų.

Dėl to duomenų valdytojas pirmiausia turi patikrinti, ar vaizdo stebėjimas sukelia asmens duomenų tvarkymą, kadangi tai siejama su asmenimis, kurių tapatybė gali būti nustatyta. Jeigu taip, Direktyva taikoma nepaisant nacionalinių nuostatų, papildomai reikalaujančių suteikti įgaliojimus visuomenės saugumo tikslais.

Pavyzdžiui, tai iliustruotų atvejais, kai prie išėjimo iš banko ar jo viduje pritvirtinama įranga, kuri leidžia nustatyti klientų tapatybę; ir atvirkščiai, tam tikromis aplinkybėmis Direktyva netaikoma aplinkos tyrinėjimo vaizdams, kurie negali būti didinami ar neapima su fiziniais asmenimis susijusios informacijos, bet renkami vandens išteklių ar atliekų tvarkymo vietų nustatymui, taip pat prietaisams, pateikiantiems eismo greitkeluose didelės apimties vaizdus.

7. DUOMENŲ VALDYTOJO PRIEVOLĖS IR TINKAMOS APSAUGOS PRIEMONĖS

A) Tvarkymo teisėtumas

Atsižvelgiant į tvarkymo teisėtumo reikalavimą (žr. Direktyvos 6 a) straipsnį), duomenų valdytojas turi iš anksto įsitikinti, kad stebėjimas atitinka bendrąsias ir specifines šiai sričiai taikomas nuostatas – susijusius įstatymus, nutarimus, etikos kodeksus. Šios nuostatos gali būti pateikiamos dėl visuomenės saugumo ir kitų, su asmens duomenų apsauga nesusijusių, tikslų, pvz., poreikiu gauti konkrečių administravimo institucijų *ad-hoc* įgaliojimą ir laikytis jų instrukcijų.

Reikia imtis visų tinkamų priemonių, siekiant užtikrinti, kad vaizdo stebėjimas atitinka duomenų apsaugos principus ir yra vengiama netinkamo kišimosi į privatų gyvenimą¹⁵.

Šiuo atžvilgiu reikia atkreipti dėmesį į geriausią praktiką, kuri gali būti aprašoma priežiūros institucijų parengtose rekomendacijose ir kituose savireguliacijos aktuose.

Taip pat būtina peržiūrėti likusias vidaus teisės nuostatas, įskaitant konstitucinius principus, civilinės ir kriminalinės teisės nuostatas, ypač taikomas „droit a l’image“ (teisei į atvaizdą)¹⁶ ar nuolatinės gyvenamosios vietos apsaugai; būtina atsižvelgti į precedentų teisę, kurios sprendimuose galėjo būti nustatyta, kad patalpos, skirtingai nuo tų, kurios siejamos su namų valda, pvz., viešbučių kambariai, biurai, poilsio kambariai, drabužinės, vidinės telefono būdelės, t.t., turi būti laikomos privačiomis.

Kai stebėjimo prietaisai yra įrengti privačių subjektų arba valstybinių įstaigų, ypač vietos institucijų, tariamai dėl saugumo ar nusikaltimų išaiškinimo, prevencijos ir kontrolės, reikėtų ypač atidžiai apibrėžti minėtus tikslus ir informuoti apie juos, kaip ir apie tikslus, kuriuos teisėtai gali vykdyti duomenų valdytojas, atsižvelgiant į tai, kad pagal įstatymą tam tikras visuomenines funkcijas gali atlikti konkretūs ne valdžios subjektai, pvz., teisėsaugos organai.

Šis klausimas yra keliamas ypač dėl to, kad kai kurios vietos valdžios institucijos, neturinčios tiesioginės kompetencijos viešosios tvarkos ir visuomenės saugumo

¹⁵ Neseniai bankas ir vietos policija neįvykdė kliento prašymo iš kamera prie ATM nufilmuotų vaizdų išgauti vagies, kuris, pavogęs kliento banko kortelę, neteisėtai ją panaudojo ir neteisėtai iš bankomato paėmė pinigus, atvaizdą, tariamai remdamiesi „privataus gyvenimo slaptumu“.

¹⁶ Prancūzijoje ir Belgijoje ši teisė reikalauja „išankstinio sutikimo“.

reikaluose, to nepaisydamos visgi užsiima papildoma stebėjimo veikla, taip pat ir tokiu stebėjimu, kuris dažnai priskiriamas nusikaltimų kontroliavimui, o iš tikrųjų skirtas įrodymų, jei būtų padaryti kriminaliniai pažeidimai, gavimui.

B) Tikslų konkretumas, detalizavimas ir teisėtumas

Duomenų valdytojas turi užtikrinti, kad jo siejami tikslai būtų aiškūs ir nedviprasmiški, taip pat kad galima būtų nustatyti tikslus vertinimo kriterijus ar siejami tvarkymo tikslai yra suderinti (žr. Direktyvos 6 b) straipsnį).

Šis atskyrimas būtinas turint omenyje tai, kad tikslai yra pateikiami informacijoje duomenų subjektui ir atitinkamuose pranešimuose, taip pat ryšium su išankstine patikra, kuri gali būti atliekama, atsižvelgiant į tvarkymą, pagal Direktyvos 20 straipsnį.

Reikia aiškiai atmesti galimybę, kad surinkta vaizdinė medžiaga gali būti naudojama kitiems tikslams, ypač ryšium su techninėmis atgaminimo galimybėmis, pvz., aiškiai uždraudžiant dauginimą.

Atitinkami tikslai turi būti aptarti dokumente, kuriame turi būti apibendrintos ir kitos svarbios privatumo politikos ypatybės, atsižvelgiant į tokius svarbius klausimus: laiko, kada vaizdinė medžiaga yra trinama fiksavimas dokumente, galimi duomenų subjekto prašymai, norint gauti informaciją, ir (arba) teisėtas naudojimas duomenimis.

C) Tvarkymo teisėtumo kriterijai

Duomenų valdytojas turi įsitikinti, kad vaizdo stebėjimas atitinka ne tik A) dalyje minėtas konkrečias nuostatas, bet ir bent vieną iš tvarkymo teisėtumo kriterijų pagal Direktyvos 7 straipsnį, konkrečiai dėl asmens duomenų apsaugos.

Nepaisant rečiau pasitaikančių atvejų, pagal Direktyvos 7 e) straipsnį, kai turi būti vykdomos teisinės prievolės – buvo minėta kazino veikla – arba kai tvarkymas reikalingas, kad būtų apsaugoti gyvybiniai interesai, pvz., pacientų nuotolinis stebėjimas intensyvios priežiūros skyriuose, dažnai iš duomenų valdytojo reikalaujama, kad jis atliktų užduotį dėl visuomenės interesų arba pagal oficialios institucijos, galbūt laikantis konkrečių taisyklių, nurodymą, pvz., atskleisti kelių eismo pažeidimus arba smurtinį elgesį viešojo transporto priemonėse didelio nusikalstamumo vietose; antraip duomenų valdytojas gali siekti teisėto intereso jei duomenų subjekto interesai ar pagrindinės teisės ir laisvės nėra viršesnės (žr. 7 f) straipsnį).

Abiem atvejais, nors labiau antruoju, ypatingas tvarkymo operacijų pobūdis reikalauja atidžiai apsvarstyti užduoties apimtį, pajėgumus ir duomenų valdytojo teisėtus interesus. Paviršutiniškumas ir neturintis pagrindo užduoties ir pajėgumų apimties plėtimas turi būti visiškai uždrausti atliekant šią analizę.

Dėl skirtingų interesų derinimo, iš anksto išklausus suinteresuotas puses, ypatingą dėmesį reikia skirti galimybei, kad saugotini interesai gali prieštarauti sistemos įdiegimui ar tam tikrų duomenų išsaugojimo organizavimui, arba kitomis tvarkymo operacijomis¹⁷.

Pagaliau duomenų subjekto sutikimas turi būti vienareikšmis ir remtis aiškia

¹⁷ Pagal naujojo Vokietijos federalinio duomenų apsaugos akto, įsigaliojusio 2001 m. gegužės 23 d., 6b skyrių, leidžiama stebėti visuomenei prieinamas vietas optinėmis ir elektroninėmis priemonėmis, jei *inter alia* nėra pagrindo manyti, kad saugotini duomenų subjekto interesai yra viršesni.

informacija. Sutikimas turi būti pateikiamas atskirai ir konkrečiai dėl stebėjimo veiklos valdose, kur vyksta privatus asmens gyvenimas¹⁸.

Tvarkymo teisėtumas pasiekiamas taip pat ir atsižvelgiant į Direktyvos nuostatas, numatančias konkrečius duomenų, susijusių su nusikaltimais, apsaugos būdus (žr. Direktyvos 8(5) straipsnį)¹⁹.

Papildomų priemonių ir veiksmų turi būti imtasi pagal išankstinės patikros mechanizmą dėl išankstinio tvarkymo įvertinimo, jei vaizdo stebėjimas sukelia konkrečią riziką asmens teisėms ir laisvėms (žr. Direktyvos 95/46/EB 20 straipsnį).

Jei tvarkymo vaizdo stebėjimo priemonėmis operacijos vykdomos valstybinių institucijų, jos visada turi remtis tiksliais teisinėmis nuostatomis.

D) Vaizdo stebėjimo naudojimo proporcingumas

Principas, kad duomenys turi būti adekvatūs ir proporcingi siekiamiems tikslams, reiškia, kad CCTV ir panaši vaizdo stebėjimo įranga gali būti išdėstoma tik remiantis subsidiarumu, arba kitaip tariant – tikslais, kurie pilnai pateisina tokios sistemos naudojimą.

Proporcingumo principas reikalauja, kad šios sistemos būtų diegiamos, jei kitos fizinės ar loginės prevencijos, apsaugos ir (arba) saugumo priemonės, nereikalaujančios vaizdo atkūrimo, pvz., šarvuotos durys kovojant su vandalizmu, automatinių vartų ir leidimų įrangos įdiegimas, jungtinės aliarmo sistemos, geresnis ir stipresnis apšvietimas gatvėse naktį ir t.t., pasirodė nepakankamos ir (arba) netinkamos, siekiant išvardintų teisėtų tikslų.

Tas pats principas taikomas ir parenkant tinkamą technologiją, konkrečius įrangos panaudojimo kriterijus ir duomenų tvarkymo detalizavimo veiksmus, tai taip pat susiję su prieigos taisyklėmis ir saugojimo terminu.

Administracijos subjektams neturi būti leidžiama įdiegti VS įrangą dėl mažų pažeidimų, pvz., norint sustiprinti rūkymo mokyklose ir kitose viešose vietose draudimą arba draudimą palikti nuorūkas ir šiukšles viešose vietose.

Kitaip tariant, atsižvelgiant į siekiamus tikslus kiekvienu konkrečiu atveju reikia taikyti *adekvatumo principą*, kuris iš valdytojo pusės reikalauja *duomenų mažinimo prievolės*.

Nors proporcinga vaizdo stebėjimo ir apsaugos sistema gali būti laikoma teisėta, jei įvyksta keletas prievartos atvejų netoli stadionų, ar jei atokesnėse vietose kartojasi užpuolimai autobusuose ar prie autobusų stotelių, ji nebus teisėta, jei bus skirta užkirsti kelią vairuotojų įžeidinėjimams ir transporto priemonių purvinimui, kaip aiškinta duomenų apsaugos institucijai, arba nustatant tapatybę piliečių, atsakingų už mažus administracinius pažeidimus, pvz., už tai, kad paliko šiukšlių maišus prie šiukšlių dėžių ir (arba) vietose, kur šiukšlinti draudžiama, arba nustatant asmenis, atsakingus už vagystes plaukimo baseinuose.

Proporcingumą reikia vertinti pagal griežtesnį kriterijų, kai kalbama apie visuomenei

¹⁸ Ypatingas dėmesys turi būti skirtas galiojančio sutikimo išreiškimui, pagal Direktyvos 95/46/EB 2 h) straipsnį („bet koks savanoriškai ir žinomai duotas konkretus duomenų subjekto pareiškimas, kuriuo duomenų subjektas nurodo savo sutikimą, kad būtų tvarkomi su juo susiję duomenys“), tuo atveju, kai įrengiamas vaizdo stebėjimas bendro naudojimo patalpose (namų bendrijose ir pan.).

¹⁹ Šioje vietoje galima paminėti Portugalijos akto Nr. 67/98 8 straipsnį, kiek tai susiję su duomenimis apie asmenis, įtariamus dalyvavus neteisėtoje ir (arba) kriminalinėje veikloje.

neprieinamas patalpas.

Šiuo atžvilgiu gali būti naudingas pasikeitimas informacija ir patirtimi tarp kompetetingų valstybių narių institucijų²⁰.

Aukščiau pateikti svarstymai taikomi augančiam vaizdo stebėjimo naudojimui savisaugos ir nuosavybės apsaugos tikslais, pirmiausia šalia viešųjų pastatų ir biurų, taip pat aplink juos esančiose teritorijose. Toks naudojimas reikalauja įvertinti bendroju požiūriu netiesioginį masinio vaizdo stebėjimo taikymo poveikį, pvz., ar kelių prietaisų įdiegimas iš tikrųjų yra efektyvi atgrasymo priemonė ir ar pažeidėjai ir (arba) vandalai gali paprasčiausiai persikelti į kitas vietas ir užsiimti kita veikla.

E) Proporcingumas, vykdant vaizdo stebėjimą

Principas, pagal kurį duomenys turi būti adekvatūs, tinkami ir nepertekliniai, apima tikslų *organizavimo proporcingumo*, taikomo duomenų tvarkymui, jei jo teisėtumas buvo patvirtintas, įvertinimą.

Pirmiausia reikia atkreipti dėmesį į *filmavimo organizavimą*, atsižvelgiant į šiuos klausimus:

a) į vizualinį kampą ryšium su tikslais, kurių siekiama²¹, pvz., jei stebima vieša vieta, kampas turi būti nustatytas taip, kad neleistų matyti šalia esančių privačių teritorijų arba detalių ir (arba) kūno bruožų, kurie nėra susiję su siekiamais tikslais, ypač jei yra įdiegta vaizdo mastelio keitimo funkcija,

b) į filmavimui naudojamos įrangos tipą, pvz., ar ji yra stacionari, ar mobili,

c) į faktinio instaliavimo organizavimą, pvz., kamerų išdėstymo, fiksuoto vaizdo ir (arba) besisukančių kamerų naudojimą ir t.t.,

d) į galimybę didinti ir (arba) keisti vaizdo mastelį filmavimo metu arba po to, t. y. ryšium su saugomais vaizdais ir galimybe sulieti ar ištrinti asmeninius atvaizdus,

e) į vaizdo stabdymo funkcijas,

f) į ryšį su „centru“, garsinių ir (arba) vaizdinių aliarmo signalų siuntimui,

g) į veiksmus, kurių imamas dėl vaizdo stebėjimo, pvz., įėjimų uždarymą, stebėtojo personalo iškvietimą, t.t.

Antra, reikia apsvarstyti *sprendimus dėl vaizdų saugojimo ir jo trukmės*, kuri turi būti pakankamai trumpa ir atitikti individualaus atvejo konkrečias ypatybes.

²⁰ Tai leistų geriau derinti kontrolės būdus ir administracinius sprendimus, kurie kartais skyrėsi, kaip atsitiko, pavyzdžiui, su Bingo salėmis.

²¹ Konkrečių atsargumo priemonių, kurių reikia imtis dėl vizualinio kampo, pavyzdžių galima rasti dvejose Italijos Duomenų apsaugos institucijos išleistose sąlygose. Sveikatos apsaugos įstaiga, planavusi pristatyti paslaugą, leidžiančią giminaičiams nuolat iš atstumo stebėti pacientus, kurie yra komos būsenoje, izoliuoti ir (arba) rimtai sergantys, intensyvios priežiūros skyriuose, buvo priversta suvokti, jog reikia tinkamai organizuoti stebėjimą, kad tuo pačiu metu nebūtų matomi ir kiti pacientai. Kitoje byloje Institucija nurodė administracinei policijos valdžiai, kad sistema, aptinkanti greičio ribojimo pažeidimus, turi filmuoti tik atitinkamas lenteles, o ne transporto priemonės vidų.

Kai kuriais atvejais gali pakakti sistemos, leidžiančios matyti vaizdus uždarame rate, kurie nėra įrašomi, pvz., kasos prekybos centre. Kitais atvejais, pvz., siekiant apsaugoti privačias valdas, gali būti pateisinamas vaizdo įrašymas kelioms valandoms ir automatinis jų ištrynimasis ne vėliau, kaip iki dienos pabaigos ar bent jau savaitės pabaigos. Šios taisyklės išimtis būtų atvejis, kai yra gaunamas pavojaus signalas arba pateiktas prašymas, kuris vertas ypatingo dėmesio. Tokiais atvejais yra pagrindas trumpą laiką laukti policijos ar teismo instancijų sprendimo.

Galima pateikti kitą pavyzdį, kai sistema, aptinkanti be leidimo miestų centruose ar važiuoti uždraustose vietose naudojamas transporto priemones, privalo įrašyti vaizdą tik tuo atveju, jei pažeidimas yra padaromas.

Reikia atkreipti dėmesį į proporcingumą, kai manoma, kad reikalingas trumpesnis saugojimo laikotarpis, kuris neturėtų viršyti savaitės²², pvz., vaizdo stebėjimo metu užfiksuoti vaizdai gali būti naudojami, nustatant žmogaus, kuris žvalgėsi po banko patalpas prieš įvykdydamas apiplėšimą, tapatybę.

Trečia, reikia kreipti dėmesį į *atvejus, kai žmogaus tapatybės nustatymą palengvina asmens veido atvaizdų susiejimas su kita informacija apie užfiksuotą elgesį ir (arba) veiklą*, pvz., tokiu atveju, kai susiejami klientų banke atvaizdai ir veikla nesunkiai nustatomu laiku.

Šiuo atžvilgiu reikia atkreipti dėmesį į aiškų skirtumą tarp vaizdo stebėjimo priemonėmis, išdėstytomis prieš įėjimą į banką, gautų atvaizdų laikino saugojimo ir tikrai labiau nepageidaujamo duomenų bankų steigimo, kuriuose saugomos banko klientų nuotraukos ir pirštų antspaudai, suteikti patiems klientams sutinkant.

Pagaliau turi būti aptarti sprendimai, kuriuos reikia priimti dėl *galimo duomenų perdavimo trečiosioms šalims*, kuris, iš esmės, neturėtų įtraukti su vaizdo stebėjimo veikla nesusijusių subjektų, ir jų viso ar dalinio paskelbimo užsienyje ar kompiuteriniuose tinkluose, taip pat remiantis atitinkamos apsaugos nuostatomis, žr. Direktyvos 25 straipsnį ir kt.

Akivaizdu, jog reikalavimas, kad vaizdai turi būti tinkami ir nepertekliniai, taikomas ir skirtingų vaizdo stebėjimo sistemų valdytojų turimos informacijos derinimui.

Išvardyti apsaugos būdai turėtų įgyvendinti principą, kuris kelių šalių vidaus įstatymuose nurodomas kaip *asmens duomenų naudojimo nuosaikumo principas*, kurio tikslas yra neleisti duomenų tvarkymo arba kiek yra įmanoma jį riboti.

Šis principas turi būti įgyvendinamas visuose sektoriuose, atsižvelgiant į tai, kad daugelį tikslų galima pasiekti ir nenaudojant asmens duomenų arba naudojant anoniminius duomenis, net jei iš pradžių gali atrodyti, kad pastarieji reikalauja asmeninės informacijos.

Išdėstyti svarstymai taikytini, jei yra pateisinamas poreikis modernizuoti verslo resursus²³ ar pagerinti vartotojams teikiamas paslaugas²⁴.

²² Danijos ir Švedijos DAI pareiškė nuomonę, kad vaizdo įrašai gali būti saugomi tik trumpą laiką ir tas laikas negali būti ilgesnis nei 30 dienų.

²³ Tai galėtų būti toks atvejis, kai reikia suskaičiuoti, kiek kasos aparatų turi būti laikoma atidarytų tuo pačiu metu prekybos centre, atsižvelgiant į pirkėjų skaičių, arba kai reikalaujama suformuoti geriausius praėjimus pirkėjams prekybos centre.

²⁴ Kai reikia kontroliuoti tapatybę, kad būtų lengviau pasiekti darbo vietą ir (arba) konkrečią transporto priemonę, asmens kortelės su nuotrauka kompiuterizuotoje laikmenoje, gali užtekti, nediegiant veidų atpažinimo sistemos.

F) Informacija duomenų subjektams

Atvirumas ir tinkamumas, naudojant vaizdo stebėjimo įrangą, reikalauja atitinkamos informacijos duomenų subjektui pateikimo pagal Direktyvos 10 ir 11 straipsnius.

Duomenų subjektai turi būti informuojami pagal Direktyvos 10 ir 11 straipsnius. Jie turi žinoti, kad vykdomas vaizdo stebėjimas. Net jei jis susijęs su visuomeniniais įvykiais, renginiais ar reklama („web“ kameros), jie privalo būti išsamiai informuojami apie stebimas vietas.

Nėra būtina labai tiksliai nurodyti, kur yra išdėstyta stebėjimo įranga, tačiau stebėjimo turinys turi būti paaiškintas nedviprasmiškai.

Informacija turi būti įrengiama priimtinu atstumu nuo stebimos vietos, atsižvelgiant į filmavimo organizavimą – skirtingai nuo kelių atvejų, kai buvo manoma, kad informacinių skydų išdėstymas 500 metrų atstumu nuo stebimų vietų bus priimtinas.

Informacija turi būti matoma ir gali būti pateikta labai glaustai, jeigu tik ji bus efektyvi: joje gali būti simbolių, kurie jau pasirodė esą efektyvūs, ryšium su informavimu apie vaizdo stebėjimą ir draudimą rūkyti, ir kurie gali skirtis, priklausomai nuo to, ar vaizdai yra įrašomi, ar ne. Visais atvejais turi būti nurodomi vaizdo stebėjimo tikslai ir atitinkamas valdytojas. Informacijos apimtis turi būti derinama prie konkrečios vietos²⁵.

Konkretūs, pagrįsti informacijos ribojimai gali būti leidžiami tik Direktyvos 10, 11 ir 13 straipsniuose nurodytais atvejais, pvz., laikini apribojimai gali būti taikomi ryšium su teisėto tyrimo metu gynybos advokato surinktais duomenimis arba vykdant teisę į gynybą tol, kol informacijos pateikimas gali kelti pavojų, kad nebus pasiekti konkretūs tikslai.

Pagaliau ypatingas dėmesys turi būti skirtas tinkamam informacijos akliems asmenims pateikimui.

G) Papildomi reikalavimai

Ryšium su papildomais reikalavimais, atsargumo priemonėmis ir apsaugos būdais, kurie yra minimi duomenų apsaugos įstatymuose ir apibendrinti aukščiau 3) punkte, taip pat atsižvelgiant į tai, kad reikia pranešti apie asmens duomenų tvarkymą ir į nepriklausomos institucijos priežiūros objektą pagal Direktyvos 18, 19 ir 28 straipsnius, Darbo Grupė nori ypač atkreipti dėmesį į šiuos klausimus:

a) Peržiūrėti įrašus ar jais naudotis turi būti leidžiama nustatytam ribotam fizinių asmenų skaičiui ir išimtinai tik tais tikslais, kurių siekiama, naudojant vaizdo stebėjimo priemones, arba prižiūrint atitinkamą įrangą, kad galima būtų įsitikinti, ar ji gerai veikia. Kitu atveju tai gali būti atliekama prašant duomenų subjektui arba policijos bei teismo institucijoms teisėtai reikalaujant dėl nusikaltimo tyrimo.

Kai vaizdo stebėjimo tikslas yra nusikaltimų prevencija, tyrimas ir kontroliavimas, sprendimas panaudoti du priegios raktus, iš kurių vienas priklausys valdytojui, o kitas policijai, daugeliu atvejų gali būti naudingas, užtikrinant, kad atvaizdus peržiūri tik policijos, o ne neturintis tam įgaliojimo, personalas, nepažeidžiant duomenų subjekto įstatyminės teisės per trumpą atvaizdų saugojimo laikotarpį pateikus prašymą gauti informaciją.

²⁵ Tai galėtų būti išreikšta „sluoksniuotu“ priėjimu.

b) Turi būti įgyvendintos tinkamos saugumo priemonės, kad neatsitiktų Direktyvos 17 straipsnyje minimi įvykiai, įskaitant informacijos, kuri gali padėti apsaugoti duomenų subjekto, trečiosios šalies ar paties duomenų valdytojo teisę, paskleidimą, tame tarpe ir atsižvelgiant į duomenų ar susijusių įkalčių manipuliavimo, pakeitimo ar sunaikinimo prevenciją.

c) Įrašytų vaizdų kokybė taip pat svarbi, ypač jei kelis kartus naudojama ta pati įrašymo priemonė, kas kelia riziką, kad nepavyks gerai ištrinti anksčiau įrašytų vaizdų.

d) Pagaliau yra labai svarbu, kad tiesiogiai vaizdo stebėjimą vykdančys operatoriai būtų tinkamai apmokyti ir žinotų, ką reikia daryti, kad jų veikla būtų visiškai suderinta su atitinkamais reikalavimais. Naudinga priemone gali būti ir valdytojų bei operatorių mokymai dėl atitinkamos rizikos ir tikslaus įrašytų asmenų tapatybės nustatymo būdų.

H) Duomenų subjekto teisės

Surinktų asmens duomenų individualios ypatybės nedraudžia duomenų subjektui įgyvendinti savo teises, nurodytas Direktyvos 13 ir 14 straipsniuose, o ypač akcentuojama teisė nesutikti su tvarkymu. Direktyva 95/46/EB tikrai leidžia duomenų subjektui konkrečiu atveju, turint teisėtą pagrindą, nesutikti su savo duomenų tvarkymu²⁶.

Duomenų subjekto teisė užmiršti ir paprastai trumpas vaizdų saugojimo laikas susiaurina duomenų subjektų teisės gauti asmens duomenis, kurie padeda nustatyti jų tapatybę, taikymo sritį. Tačiau ši teisė turi būti saugoma, ypač jei pateikiamas išsamus prašymas leisti tam tikrus vaizdus lengvai atstatyti. Reikia įvertinti ir tai, kad laikinai turi būti apsaugomos ir trečiosios šalies teisės.

Bet kokie ribojimai vaizdų atkūrimui, kai tokie ribojimai dėl trumpo vaizdų saugojimo laikotarpio yra aiškiai neproporcingi tyrimo, išlaidų ir resursų požiūriu, turi būti išdėstyti išimtinai pirminiuose teisės aktuose (žr. Direktyvos 13(1) straipsnį), atsižvelgiant į duomenų subjekto teisę į gynybą ryšium su svarstomuoju laikotarpiu atsitikusiais konkrečiais įvykiais.

I) Konkrečių tvarkymo operacijų papildomos apsaugos priemonės

Turi būti draudžiama vykdyti vaizdo stebėjimą išimtinai dėl asmenų rasės, jų religinių ar politinių įsitikinimų, narystės profesinėse sąjungose arba seksualinių įpročių (Direktyvos 8 straipsnis).

Neturėdama tikslo sudaryti išsamų sąrašą, kur vaizdo stebėjimas gali būti taikomas, Darbo Grupė norėtų akcentuoti, kad kur yra tinkama reikia kreipti didesnę dėmesį, atliekant Direktyvos 20 straipsnyje minimą išankstinę tvarkymo operacijų patikrą, į kelias situacijas, kada renkami vaizdai, susiję su asmenimis, kurių tapatybė yra arba gali būti nustatyta, kadangi šios situacijos turi būti įvertintos kiekvienu konkrečiu atveju.

Toliau nurodomi yra būtent šie atvejai, nes jie išplaukia iš patirties ir (arba) vyksta jų tyrimai:

a) nuolatinis ryšys tarp vaizdo stebėjimo sistemų, kurias valdo skirtingi duomenų valdytojai,

²⁶ Išskyrus kai kitaip yra nustatyta nacionaliniuose teisės aktuose.

- b) galimas vaizdo ir biometrinių duomenų, tokių kaip pirštų atspaudų, sujungimas (pvz., prie įėjimų į bankus),
- c) balso identifikavimo sistemų naudojimas,
- d) indeksavimo sistemų, taikomų vaizdo įrašams ir (arba) jų vienašakio automatinio atstatymo, ypač tapatybės nustatymo duomenims, įdiegimas, nepažeidžiantis proporcingumo principų ir paremtas konkrečiomis nuostatomis,
- e) veido atpažinimo sistemų naudojimas, kurios gali ne tik nustatyti praeinančių asmenų maskuotę, pvz., netikras barzdas ar perukus, bet ir yra skirtos įtariamiesiems pažeidėjams nustatyti. Pvz., sistemos gali automatiškai nustatyti tam tikrų asmenų tapatybę, remdamasi modeliais ir (arba) standartiniais identifikavimo požymių komplektais, kuriuos sudaro tam tikri išorės bruožai (asmens odos spalva, akys, išsišovę skruostikauliai ir t.t.) arba remdamasi iš anksto apibrėžtu nenormaliu elgesiu (staigūs judesiai, pakartotinis praėjimas, net ir konkrečiais intervalais, transporto priemonės parkavimo būdas ir t.t.). Todėl čia žmogaus įsikišimas yra tinkamas ir dėl tokiomis atvejais pasitaikančių klaidų, kaip minima f) punkte žemiau,
- f) galimybė automatiškai aptikti maršrutus bei pėdsakus ir (arba) rekonstruoti ar numatyti asmens elgesį,
- g) automatinį sprendimų priėmimą, kurie paremti asmens profailu ar protinga analize ir intervencinėmis sistemomis, nesusijusiomis su standartiniais aliarmo signalais, pvz., kai į patalpą įeinama, nepateikus būtinos identifikacijos, arba gaisro aliarmas.

8. VAIZDO STEBĖJIMAS DARBO SANTYKIŲ KONTEKSTE

Savo Nuomonėje Nr. 8/2001 dėl asmens duomenų tvarkymo darbo santykių kontekste, priimtoje 2001 m. rugsėjo 13 d., ir Darbo dokumente dėl elektroninės komunikacijos sekimo darbo vietoje, priimtame 2002 m. gegužės 29 d.²⁷, ši Darbo Grupė jau bendrais bruožais atkreipė dėmesį į keletą principų, skirtų duomenų subjektų teisėms, laisvėms ir orumui apsaugoti darbo santykių kontekste.

Be abiejuose aukščiau minėtuose dokumentuose pateiktų svarstymų, ta apimtimi, kuri taikytina vaizdo stebėjimui, yra tikslinga pabrėžti, kad vaizdo stebėjimo sistemos, skirtos nuotoliniu būdu tiesiogiai kontroliuoti darbo kokybę ir apimtis, todėl sukeliančios asmens duomenų tvarkymą, paprastai šiuo tikslu neturi būti leidžiamos.

Visai kitaip yra, kai laikantis tinkamų apsaugos priemonių vaizdo stebėjimo sistemos yra išdėstomos dėl gamybos ir (arba) darbo saugumo reikalavimų, kur taip pat stebima iš nuotolio, nors netiesiogiai²⁸.

Įdiegimo patirtis papildomai parodė, kad neturi būti stebimos patalpos, kurios yra skirtos darbuotojų privačiam naudojimui arba jose nenumatyta atlikti darbo užduotis, pvz., tualetai, dušas, rakinamos spintelės ir rekreacinės zonos. Vaizdai, renkami norint apsaugoti turtą ir (arba) dėl rimtų pažeidimų tyrimo, prevencijos ir kontrolės, neturi būti naudojami kaltinant darbuotoją mažais disciplinos pažeidimais ir darbuotojams visada turi būti leidžiama paduoti priešiškinis, naudojantis surinkta vaizdo medžiaga.

²⁷ Abu dokumentus galima rasti šiuo adresu:

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

²⁸ Šiais atvejais, šalia šiame dokumente pateiktų svarstymų, reikia atsižvelgti konkrečiai į poreikį gerbti teises, minimas kolektyviniuose susitarimuose, kurie kartais remiasi kolektyvine informacija apie darbuotojus ir (arba) jų profesinių sąjungų organizacijas – pvz., nekalbant apie individualiai pateikiamą informaciją, prisilaikant duomenų apsaugos įstatymų; kitais atvejais reikia siekti pirminio susitarimo su darbuotojų atstovais arba profesinių sąjungų organizacijomis dėl įdiegimo organizavimo, taip pat dėl stebėjimo trukmės ir kitokio filmavimo organizavimo. Keliuose šalyse gali prirėkti valstybinio įsikišimo, jei susijusios šalys negali susitarti.

Informacija turi būti suteikta darbuotojams ir kiekvienam teritorijoje dirbančiam asmeniui. Informacija turi apimti valdytojo tapatybę ir stebėjimo tikslą bei bet kokią kitą informaciją, kuri būtina užtikrinant sąžiningą tvarkymą atsižvelgiant į duomenų subjektą, pavyzdžiui, kokiais atvejais įrašai bus peržiūrėti įmonės vadovybės, įrašymo periodas ir kada įrašai bus perduoti teisėsaugos organams. Informacijos pateikimas, pavyzdžiui, simbolio pavaldumui, darbo santykių kontekste nelaikomas pakankamu.

9. IŠVADOS

Darbo Grupė parengė šį darbo dokumentą, siekdama suvienodinti nacionalinių priemonių dėl vaizdo stebėjimo, priimtų pagal Direktyvą 95/46/EB, taikymą.

* * *

Šiuo požiūriu taip pat yra labai svarbu, kad valstybės narės pateiktų vadovus apie gamintojų, paslaugų teikėjų ir platintojų, bei tyrėjų veiklą, atsižvelgiant į technologijų, programinės įrangos ir techninių prietaisų, kurie atitinka šiame dokumente nurodytus principus, vystymąsi.

* * *

Briuselis, 2003 m. birželio 13 d.
Darbo grupės vardu
Pirmininkas
Stefano RODOTA

Vertimą parengė

B. Jurgelevičienė
2004-03-22