



11750/02/EN
WP 67

**Darbinis dokumentas dėl
asmens duomenų tvarkymo vaizdo stebėjimo priemonėmis**

Priimta 2002 m. lapkričio 25 d.

ASMENŲ APSAUGOS, ATSIŽVELGIANT Į ASMENS DUOMENŲ TVARKYMĄ, DARBO GRUPĖ

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 pastraipas, atsižvelgiant į jos Procedūros taisykles ir ypač į 12 ir 14 straipsnius,

priėmė šį darbo dokumentą.

1. Įžanga

Europoje per pastaruosius kelerius metus vis daugiau valstybinių ir privačių įstaigų įsirengia vaizdo atgaminimo sistemas. Ši aplinkybė sukėlė gyvus debatus Sąjungos lygyje ir atskirose Šalyse Narėse dėl būtinų sąlygų ir apribojimų, taikytinų vaizdo stebėjimo prietaisų įrengimui, ir būtinų duomenų subjektų apsaugos nustatymo.

Per pastaruosius metus sukaupta patirtis ir Direktyvos 95/46/EB perkėlimas į nacionalinį lygmenį parodė, kad labai padaugėjo uždaru sistemų, kamerų ir sudėtingesnių prietaisų, kurie yra naudojami įvairiausiose sferose.

Be to, turimos technologijos tobulinimas, kompiuterizavimas ir prietaisų mažėjimas gerokai padidina vaizdo ir garso įrašymo prietaisų teikiamas galimybes, taip pat ryšium su jų paskleidimu intranetuose ir internete.

Be tvarkymo operacijų darbo santykių kontekste, apie ką jau buvo kalbėta Darbo Grupės detaliame dokumente (*Nuomonė 8/2001 apie asmens duomenų tvarkymą darbo santykių kontekste*²), vaizdinio sekimo technikos gausėjimą lengvai gali įvertinti visi piliečiai.

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

- 1) asmenų apsauga,
- 2) nuosavybės apsauga,

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., paskelbta:

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

³ Skirtingos vaizdo stebėjimo sistemos yra įrengiamos:

a) visuomeniniuose ar/arba visuomenės lankomuose pastatuose ar šalia jų, pvz., muziejuose, maldos vietose ar paminkluose, norint išvengti nusikaltimų ir/arba mažesnių vandalizmo aktų,

b) stadionuose ir sporto įrangoje, ypač prieš konkrečius renginius,

c) transporto sektoriuje ir ryšium su kelių eismu, siekiant kontroliuoti eismą magistralėse ir greitkeliuose arba nustatyti greičio ribojimo ir/arba eismo taisyklių pažeidimus miestų centruose, kontroliuoti metropolitenų patalpas, siekiant tunelių linijas, stebėti degalines ir taksi automobilių vidų,

d) kad būtų užkirstas kelias neteisėtam elgesiui ir/arba jis nustatytas mokyklų prieigose, taip pat ryšium su nepilnamečių užkabinėjimu,

e) medicinos įrangoje operacijų metu ir/arba teikiant pagalbą per atstumą, 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 būtų lengviau ieškoti dingusių nepilnamečių ir kitų asmenų,

g) privačių detektyvų,

h) supermarketuose 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 vaizdavimo tikslais,

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

Taip pat galima būtų skirstyti asmeninio naudojimo ir viešojo naudojimo pagrindu.

Skirtingos apsaugos priemonės taikomos įdiegiant vaizdo kameras ir panašius prietaisus.

Kai kuriais atvejais, remiantis konkrečiomis Šalies Narės nuostatomis, naudoti vaizdo įrašymo sistemą iš tikrųjų yra privaloma, pavyzdžiui, tokių atvejų pasitaikė keliose kazino, arba sistema tarnauja 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, nepaprašiusi nuteistųjų sutikimo.

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

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

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

Ši analizė nepriklauso nuo naudojamų metodų ir yra taikoma visiems vaizdo stebėjimo būdams.

Šiame darbo dokumente nagrinėjamas stebėjimas, kai įvykiai, situacijos ir atsitikimai yra stebimi iš nuotolio, tuo tarpu čia nesvarstomi kiti atvejai, kada apie konkrečius įvykius yra skelbiama atsitiktinai ir/arba tendencingai, pavyzdžiui, dėl vietos valdžios ir/arba parlamento veiksmų aiškumo.

Kiekvienas operatorius tada galės tiksliau apibrėžti čia pateiktus nurodymus ir atitinkamoje sferoje, ir atsižvelgiant į ateities technologijų vystymąsi, kuri Darbo Grupė siekia iširti.

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

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 biometrijoje klausimas yra aptartas Darbo Grupės atskirame dokumente.

Svarbiausių principų reikia paisyti, kai jie taikytini konkrečiai, ryšium su tvarkymu asmens duomenų, gautų naudojant ne vaizdo įrašymo priemones, bet kitus stebėjimo būdus, t.y. distancinio valdymo priemones, pavyzdžiui, satelitinę GPS sistemą.

Šis darbo dokumentas skirtas, visų pirma, kad būtų atkreiptas dėmesys 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 šalių narių institucijos turi įvertinti vaizdo stebėjimą apskritai, taip pat skatinti selektyvų ir sisteminių požiūrį į šiuos dalykus. Dėl vaizdo atkūrimo sistemų greito plitimo visuomeninėse ir privačiose sferose, neturėtų atsirasti nepateisinamų piliečių teisių ir pagrindinių laisvių apribojimų, kitaip piliečiai gali būti priversti patirti neproporcingas duomenų rinkimo procedūras, dėl kurių bus masiškai nustatoma jų tapatybė kai kuriose viešose ir privačiose vietose.

b) Gali būti nustatytos vaizdinio sekimo metodų evoliucijos kryptys, kad būtų užkirstas kelias vystymuisi programinės įrangos, kuri remiasi veidų atpažinimu ir vaizduojamo žmogaus elgesio studijavimu bei prognozavimu nuo neapgalvotai atliekamo iki dinaminio-prevencinio stebėjimo – priešingo tradiciniam statiškam sekimui, kurio tikslas daugiausia yra dokumentuoti ypatingus įvykius ir jų autorius. Ši nauja stebėjimo forma gali automatiškai atpažinti asmenų veido bruožus, taip pat ir jų „nenormalų“ elgesį, taikant automatizuotus pavojaus signalus ir užuominas, o tai gali sukelti diskriminacijos grėsmę.

2. Tarptautiniai teisės aktai

a) Žmogaus teisių ir pagrindinių laisvių konvencija.

Privatumo apsauga yra užtikrinta Žmogaus teisių konvencijos 8 straipsnyje⁵.

Rotaru byloje⁶ Teismas nutarė, kad jokiose vidaus teisės nuostatose nėra numatyta Valstybinės galios naudojimo apribojimų (numatymas iš anksto). Įstatyme nėra numatyta, kokios rūšies informacija gali būti įrašoma, nenumatytos žmonių kategorijos, kurioms stebėjimo priemonės, pvz., informacijos rinkimas ir laikymas, gali būti taikomos, koks informacijos saugojimo laikotarpis ir kaip ilgai informacija gali būti laikoma, kokiomis sąlygomis tokių priemonių galima imtis ir kokios tvarkos reikia laikytis. Teismas pažymėjo, kad įstatyme⁷ nėra aiškių, detalių nuostatų dėl asmenų, įgaliotų ieškoti informacijos bylose, bylų pobūdžio, tvarkos, kurios reikėtų laikytis, ir kaip gauta informacija gali būti naudojama.

Amann'o byloje⁸ Teismas priminė, kad telefono skambučių privačiose ar verslo patalpose apsauga yra numatyta Konvencijos 8 straipsnyje. Teismas taip pat nutarė, kad

⁵ Žiūrėti į nuorodas apie Orwell ir kameros Malone byloje (1984 m. rugpjūčio 2 d.).

⁶ Rotaru prieš Rumuniją, 2000 m. gegužės 4 d.

⁷ Pagal 45 skyrių, RŽT yra įgaliota saugoti ir naudoti archyvus, priklausiusius ankstesnėms žvalgybos tarnyboms, veikusioms Rumunijos teritorijoje, ir leido inspektuoti RŽT dokumentus, gavus direktoriaus sutikimą.

⁸ Amann prieš Šveicariją, 2000m. vasario 16 d.

reikalavimas „numatyti“ reiškia, jog įstatyme pakankamai tiksliai formuluojama, kad kiekvienam asmeniui – jei reikia, suteikus jam atitinkamą konsultaciją – suteikiama teisė reguliuoti, kaip jis turėtų elgtis⁹. Teismas pridūrė, jog 8 straipsnyje reikalaujama, kad vidaus teisėje būtų nustatytos teisinės apsaugos priemonės nuo savavališko valstybinių institucijų kišimosi. Įstatymas turi pakankamai tiksliai numatyti kompetetingų institucijų diskretiškumo ribas ir naudojimosi juo būdą, atsižvelgiant į teisėtą kalbamosios priemonės taikymą, kad individui būtų suteikta pakankama apsauga nuo savavališko kišimosi. Teismo sprendime išaiškintas klausimas dėl asmenų, kurių pokalbių klausomasi „atsitiktinai“, kaip telefoninio pokalbio, kurį įrašo valdžios institucijos, „privalomųjų dalyvių“.

Dėl kortelės sukūrimo ir saugojimo, Teismas be kita ko nurodė, kad taisyklės neatitiko Konvencijos 8 straipsnio reikalavimų, nes jose nebuvo jokių aiškių nurodymų dėl valstybinei institucijai suteiktų galių rinkti, įrašinėti ir saugoti informaciją vykdymo apimties ir sąlygų. Jose nebuvo tiksliai apibrėžta, kokiomis sąlygomis gali būti kuriamos kortelės, kokių reikia laikytis procedūrų, kokią informaciją galima saugoti ar kokie komentarai gali būti draudžiami.

b) Asmenų apsaugos ryšium su automatinio asmens duomenų tvarkymu Europos Konvencijos Nr. 108/1981 Taryba.

Šios Konvencijos veikimo sritis nėra ribota, kaip Direktyvos 95/46/EB. Vaizdo stebėjimo veikla, sukianti asmens duomenų tvarkymą, įeina į šios Konvencijos taikymo sritį. Įkurtas šios Konvencijos Konsultacinis komitetas konstatavo, kad balsai ir atvaizdai yra laikomi asmens duomenimis, jei jie teikia informaciją apie asmenį, net netiesiogiai sudarantys galimybę nustatyti jo/jos tapatybę.

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 teisės aktų nuostatose.

c) Europos Sąjungos Pagrindinių teisių chartija.

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

3. Stebėjimas pagal Direktyvą 95/46/EB.

Garsinių ir vaizdinių duomenų, įeinančių į informaciją apie asmenį, specifinės tvarkymo ypatybės yra išryškintos Direktyvoje 95/46/EB (toliau vartojama „Direktyva“), kurioje apie tai aiškiai kalbama keliuose punktuose.

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

Vaizdo stebėjimo priemonėmis surenkamos informacijos didelė dalis susijusi su asmenimis, kurių tapatybė yra nustatyta ir/arba gali būti nustatyta, nufilmuotais, kai jie įeidavo į visuomenines ir/arba visuomenei prieinamas patalpas, kuriose judėdamas asmuo gali tikėtis mažiau privatumo, tačiau visiškai neatimant visų teisių ir laisvių, kurios liečia ir jo asmeninę sferą bei atvaizdą.

⁹ Žr. kitas bylas, kaip, pvz., Malone prieš Jungtinę Karalystę teismo sprendimą 1984 rugpjūčio 2 d., Serija A, Nr.82, P. 31-32, § 66.

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

Judėjimo laisvė gali būti varžoma tik tada, kai tai būtina demokratinėje visuomenėje, ir turi atitikti konkretų tikslą, kurio 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., stebimas jų elgesys, kai kuriose viešosiose ir/arba visuomenei prieinamose patalpose neproporcingai naudojant vaizdo stebėjimą.

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

a) iš esmės Direktyva yra taikoma šioje srityje, atsižvelgiant į surinkimo, manipuliavimo ir kitokio ypatingos kategorijos asmens duomenų naudojimo būdų vystymosi svarbą (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 straipsnį, a) poskyrį ir konstatuojamąją dalį Nr. 26).

Be išdėstytų konkrečių nurodymų, Direktyva aiškiai parodo, kaip veikia atskiros jos nuostatos, susijusių su

1) *Duomenų kokybe*. Vaizdai turi būti tvarkomi teisingai bei teisėtai ir tiksliai apibrėžtais, aiškiais, teisėtais tikslais. Vaizdai turi būti naudojami, remiantis principu, kad duomenys turi būti tikslūs, aktualūs bei nepertekliniai, ir toliau netvarkomi tuo būdu, kuris yra nesuderinamas su šiais tikslais; turi būti saugomi ribotą laiką ir t.t. (žr. 6 straipsnį),

2) *Duomenų tvarkymo teisėtumo kriterijai*. Remiantis šiais kriterijais, asmens duomenų tvarkymą vaizdo stebėjimo priemonėmis yra svarbu pagrįsti bent viena būtina sąlyga, paminėta 7 straipsnyje – nedviprasmišku sutikimu, būtiniais sutartiniais įsipareigojimais, būtinai laikytis teisinės prievolės, saugoti duomenų subjekto gyvybinius interesus, tvarkyti vykdant visuomenės labai atliekamą užduotį arba įgyvendinant oficialius įgaliojimus, derinant interesus,

3) *Ypatingų duomenų kategorijų tvarkymas*, kuris yra apsaugos priemonių, taikomų ypatingiems duomenims arba vaizdo stebėjimo pažeidimų duomenims, objektas (pagal 8 straipsnį),

4) Duomenų subjekto *informavimas* (žr. 10 ir 11 straipsnius),

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

6) Apsaugos priemonės, taikomos ryšium su *automatiniais individualiais sprendimais* (pagal 15 straipsnį),

7) Tvarkymo operacijų *saugumas* (17 straipsnis),

8) *Pranešimas apie tvarkymo operacijas* (pagal 18 ir 19 straipsnius),

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

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

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

4. Vaizdo stebėjimui taikomos nacionalinės nuostatos

Keliose šalyse narėse išstudijuotos su vaizdo stebėjimu susijusios bylos, remiantis konstitucinėmis nuostatomis¹⁰, konkrečiais įstatymais, potvarkiais ar kitais sprendimais, išleistais kompetetingų nacionalinių valdžios organų¹¹.

Keliose šalyse taip pat yra taikomos konkrečios nuostatos, nepaisant tos aplinkybės, kad vaizdo stebėjimas sukelia asmens duomenų tvarkymą. Pagal šias nuostatas, CCTV ir panašią stebėjimo įrangą instaliuoti ir išdėstyti galima tik iš anksto leidus administracinei institucijai, kurią gali, visiškai ar iš dalies, atstovauti nacionalinė duomenų apsaugos institucija. Tokie nurodymai gali skirtis, atsižvelgiant į tai, ar už atitinkamos įrangos naudojimą yra atsakingi privatūs, ar valstybiniai subjektai.

Kitose šalyse vaizdo stebėjimas nėra aptartas konkrečiuose įstatymuose, vis dėlto, duomenų apsaugos institucijos dirba tam, kad užtikrintų tinkamą bendrųjų duomenų apsaugos nuostatų taikymą, pateikdamos nuomones, rekomendacijas ar elgesio kodeksus, pvz., kurie jau yra priimti JK ir projektai rengiami Italijoje.

Belgija	DAI nutarimai, ypač <i>Avis d'initiative</i> Nr. 34/1999 1999 m. gruodžio 13 d., Nr. 3/2000 2000 m. sausio 10 d. ir Nr. 10/2000 2000 m. balandžio 3 d.
Prancūzija	1995 m. sausio 21 d. Aktas Nr. 95-73 dėl apsaugos (pataisytas Ordonnance 2000-916 2000m. rugsėjo 19 d.) 1996 m. spalio 17 d. Dekretas Nr. 96-926 ir 1996 spalio 22d. Aplinkraštis dėl Akto Nr. 95-73 (CNIL) įgyvendinimo.
Graikija	2000 m. sausio 28 d. DAI nutarimas (Atėnų metropolitenas)
Vokietija	2000 m. Federalinio Akto 6 skyrius.
Airija	Bylos studija Nr. 14/1996 (CCTV naudojimas)

¹⁰ Žr. Portugalijos Konstitucinio Teismo Sprendimą 255/2002. Teismas nusprendė, kad „elektroninių stebėjimo prietaisų naudojimas privačiose apsaugos institucijose ir jų vykdomas piliečių kontroliavimas yra teisės į privataus gyvenimo saugojimą, kuriam paskirtas Konstitucijos 26 straipsnyje, ribojimas arba suvaržymas“.

¹¹ Mažiausiai vienoje šalyje (Belgijoje – Gaia byla) dėl vaizdinių duomenų rinkimo ne pagal duomenų apsaugos įstatymus buvo atsisakyta leistinų įrodymų Teisme.

Italija	2001-12-28 Įstatyminio akto Nr. 467 20 skyrius (numatantis etikos kodekso priėmimą) Garante nutarimai Nr. 2 2002 m. balandžio 10d. (paremiantis etikos kodekso priėmimą), 2001 m. rugsėjo 28 d. (biometrija ir veidų atpažinimo metodai, taikomi bankuose) ir 2000 m. lapkričio 29 d. (vadinamasis „vaizdo stebėjimo dekalogas“) Prezidento dekretas Nr. 250 1999-06-22 (reguliuojantis naudojimąsi transporto priemonėmis miestų centruose ir draudžiamose zonose) Dekretas Nr. 433 1992-11-14 ir Aktas Nr. 4/1993 (taikomas muziejams, valstybinėms bibliotekoms ir archyvams) Įstatyminis aktas Nr. 45 2000-02-04 (keleiviniai laivai nacionaliniuose laivybos keliuose) Akto Nr. 300 4 skyrius 1970-05-20 (vadinamasis Darbininko Statutas)
Jungtinė Karalystė	CCTV vidaus taisyklės 2000 (Informacijos komisaras)
Ispanija	Ley organica Nr. 4/1997 (apsaugos agentūrų viešose vietose atliekamas vaizdo stebėjimas) Real Dekreto Nr. 596/1999, įgyvendinantis Aktą Nr. 4/1997
Portugalija	Dekretas-Įstatymas 231/98 1998m. liepos 22d. (privati apsaugos veikla ir savisaugos sistemos) Įstatymas 38/98 1998 m. rugpjūčio 4 d. (priemonės, kurių reikia imtis prievartos sporto renginiuose atveju) Dekretas-Įstatymas 263/01 2001 m. rugsėjo 28 d. (šokių vietos) Dekretas-Įstatymas 94/2002 2002 m. balandžio 12 d. (sporto renginiai)

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

5. Sritis, 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 įstatymai¹², tikslais. Vis dėlto, daugelyje šalių narių, perimant Direktyvą 95/46/EB, šios problemos nušviestos bendrai, nustatant konkrečius pavyzdžius.

A) Kai kuriose šalyse išvardintais tikslais atliekamoms tvarkymo operacijoms bet kokių atveju numatomos apsaugos priemonės pagal Konvenciją Nr. 108/1981 ir atitinkamas Europos Tarybos rekomendacijas, tam tikras nacionalines nuostatas (žr. Direktyvos 95/46/EB 3(2) straipsnį ir konstatuojamąją dalį Nr. 16). Atsižvelgiant į specifinius bruožus ir esančias konkrečias nuostatas dėl policijos ar teismo organų vykdomos tyrimo veiklos nacionalinio saugumo tikslais¹³ – kur gali būti naudojamas „slaptas“ vaizdo stebėjimas, t.y. vykdomas

¹² Žr. įžanginę dalį 16.

¹³ Šiuo atveju galima remtis Europos žmogaus teisių teismo principais, išdėstytais Rotaru prieš Rumuniją byloje, nagrinėtoje 2000 m. gegužės 4 d. Žr. aukščiau.

nesuteikiant informacijos – šios kategorijos tvarkymas šiame dokumente nebus detaliai aptariamas.

Tačiau Darbo Grupė norėtų pabrėžti, kad panašiai, kaip kelios kitos asmens duomenų tvarkymo operacijos, kurioms netaikoma Direktyva, atliekant vaizdo stebėjimą, remiantis visuomenės saugumo reikalavimais arba kriminalinių nusikaltimų tyrimo, prevencijos ir kontrolės tikslais, reikia paisyti Žmogaus teisių ir pagrindinių laisvių konvencijos 8 straipsnyje išdėstytų reikalavimų, remtis konkrečiomis visuomenei žinomomis nuostatomis, sieti ir derinti su *konkrečios* rizikos ir *konkrečių* nusikaltimų prevencija, pvz., vietose, kur gali kilti tokia rizika arba ryšium su visuomeniniais renginiais, kurių metu gali būti įvykdyti tokie nusikaltimai¹⁴. Reikia atsižvelgti į vaizdo stebėjimo sistemų daromą poveikį, pvz., į tą faktą, kad neteisėti veiksmai gali persikelti į kitas vietas ar sektorius, ir duomenų valdytojas visada turi būti aiškiai apibūdinamas, kad duomenų subjektas galėtų vykdyti savo teises.

Pastarasis reikalavimas susijęs su ta aplinkybe, kad vaizdinis sekimas vis dažniau policijos vykdomas kartu su kitomis valdžios institucijomis (pvz., vietiniais valdžios organais) ir/arba privačiomis organizacijomis (bankais, sporto asociacijomis, transporto kompanijomis), dėl ko kyla rizika, kad taps neaiškūs individualūs vaidmenys ir atsakomybė dėl atliekamos užduoties¹⁵.

B) Antra, Direktyva netaikoma, kai fiziniai subjektai atlieka tvarkymo operacijas tik užsiimdami asmenine ir namų ūkio veikla (žr. 3(2) straipsnį ir įžanginę dalį Nr. 12).

Nors aukščiau minėtos sąlygos galioja, jei vaizdinio stebėjimo priemonės įdiegiamos tam, kad galima būtų iš nuotolio stebėti, kas vyksta kieno nors namo viduje, pvz., užkirsti kelią vagystėms arba ryšium su vadinamąja elektronine šeima, jos negalioja, jei vaizdinio sekimo įranga instaliuojama išorėje arba šalia privačių valdų, siekiant saugoti nuosavybę ir/arba užtikrinti apsaugą.

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

Kai sistema naudojasi tik individuali šeima ir stebimos tik vienos durys, laiptų aikštelė, automobilių stovėjimo vieta ir t.t., faktas, kad Direktyva netaikoma, kai sistema naudojama išimtinai asmeniniais tikslais ir duomenys neperduodami trečiosioms šalims, sistemos valdytojo neatleidžia nuo įstatymais garantuojamų teisių ir jo kaimynų bei kitų asmenų interesų gerbimo. ES šalyse narėse šios teisės ir interesai saugomi, nepaisant duomenų apsaugos principų, bendrųjų (civilinės teisės) nuostatų, skirtų asmens teisių,

Čia galima nurodyti Žmogaus teisių Europos teismo išdėstytus principus byloje Rotaru prieš Rumuniją, kuri nagrinėta 2000 m. gegužės 4 d. Žr. Aukščiau.

¹⁴ Pavyzdžiui, Prancūzijoje 1996-10-22 išleistas aplinkraštis, liečiantis izoliuotas vietas ir vėlai naktį uždaromas parduotuves.

¹⁵ Reikšmingas rizikos pavyzdys yra kelių Italijos municipalitetų vykdoma veikla, siekiant stebėti vaizdinėmis sekimo priemonėmis viešąsias vietas, kur naktimis renkasi prostitutės. Kai kurie municipalitetai praeityje skelbė – labai abejotinai – kad jie yra kompetetingi užkirsti kelią šiam reiškiniui, 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 valdžia priėmė nutarimą, aiškinantį, kokios atsakomybės gresia už atitinkamų nuostatų pažeidimą.

atvaizdo, šeimos gyvenimo ir privačios sferos apsaugai – tik pagalvokite, pavyzdžiui, apie kamerą, nustatytą prie buto lauko durų tokiu kampu, kuris leidžia sistemiškai nufilmuoti medicinos klinikos ir/arba teisinės firmos, esančios tame pačiame aukšte, klientus ir taip neteisėtai kištis į profesines paslaptis.

Ypatingą dėmesį reikia skirti video įrangos orientavimui, žinučių ir informacijos siuntimui 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 šalys narės nustato kai kurių jos nuostatų išimtis, kai tvarkymas atliekamas tik žurnalistiniais sumetimais arba meninės ar literatūrinės raiškos tikslais, ypač garsinėje-vaizdinėje srityje (žr. konstatuojamąją dalį Nr.17). Tik turi būti nustatomos išimtys, kai reikia derinti privatumo teisę ir taisykles, reguliuojančias raiškos laisvę¹⁶. 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 tikslais¹⁷.

6. Vaizdo stebėjimas ir asmens duomenų tvarkymas

Atsižvelgiant į minėtas įvairias situacijas, Darbo grupė laikosi nuomonės, kad reikia atkreipti dėmesį į tai, kad ši Direktyva taikoma vaizdinių ir garsinių duomenų rinkimui CCTV ir kitų vaizdo stebėjimo sistemų priemonėmis, įskaitant tuos atvejus, kai tokią sistemą įrengęs subjektas gali nesuvokti, kad yra tvarkomi asmens duomenys.

Vaizdų įrašymas apima asmens duomenis

- a) net jei jie naudojami uždaro rato sistemoje,
- b) net jei jie nesiejami su smulkia informacija apie asmenį,
- c) net jei jie neliečia asmenų, kurių veidai buvo nufilmuoti, nors gali apimti kitokią informaciją, pvz., automobilio numerį ar PIN skaičius, užfiksuojamus stebint bankomatus,
- d) nepaisant priemonės, kurioje yra įrašyti vaizdai (pvz., nuotraukos, nufotografuotos prie įėjimų į miesto centrus, stacionarios ir/arba mobilios vaizdo sistemos, tokios kaip nešiojami televizoriai, spalvoti ir/arba balta-juoda atvaizdai), naudojamos technikos (analoginės ir skaitmeninės, laidinės ar optinio kabelio priemonės), įrangos tipo (stacionari, besisukanti, mobili), vaizdo atgaminimo ypatybių (pvz., nepertraukiamas priešinamas pertraukiamam, kurį iliustruoja atvejai, kai vaizdas atgaminamas tik tada, jei nepaisoma greičio ribojimo ir tai nesujungia su visiškai atsitiktinai atliktu nesuderintu filmavimu) ir naudojamų komunikacijos priemonių, pvz., ryšys su „centru“ ir/arba vaizdo perdavimas tolesniems terminalams, ir t.t...

Akivaizdu, kad vaizdiniai ir garsiniai duomenys sietini su fiziniais asmenimis, kurių tapatybė yra nustatyta ar gali būti nustatyta.

¹⁶ Žr. Duomenų apsaugos įstatymo ir žiniasklaidos Darbo grupės Rekomendaciją 1/97.

¹⁷ Milane slapta įrengta prie metro stoties laiptų „web“ kamera tiesiogiai į Tinklą perduodavo praeinančių moterų slaptų vietų vaizdus tik, atrodytų, žurnalistiniais tikslais. Tai, kad vaizduojamo asmens tapatybės nebuvo galima nustatyti, neleido nacionalinei duomenų apsaugos institucijai imtis kokių nors veiksmų ryšium su šiuo reikalu.

Pagal Direktyvą, tapatybės nustatymas gali kilti derinant duomenis su trečiosios pusės informacija arba atskirais atvejais taikant konkrečią techniką ir/arba konkrečius prietaisus.

Todėl 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, reikalaujančių suteikti įgaliojimus visuomenės saugumo tikslais.

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

Pagaliau reikia atkreipti dėmesį į tai, kad asmens duomenys taip pat yra tvarkomi, jei vaizdai yra tik gaunami ir tik peržiūrimi, nebūtinai ateityje jie yra saugomi ar klasifikuojami konkrečiuose duomenų bankuose.

Galima ginčytis, kad tik vaizdų rinkimas nesiskiria nuo to, jei žmogus tam tikroje vietoje stebėtų, kas vyksta aplinkui. Į tai galima atsakyti, kad pagal Direktyvą (2 straipsnis b) paantraštė) į „tvarkymo“ sąvoką įeina ne tik rinkimas, o vaizdo stebėjimo sistema stebimus įvykius vaizduoja kiek kitaip, lyginant su žmogaus akimis; iš tikrųjų, ji leidžia sustabdyti vaizdą, kurį keliuose monitoriuose gali stebėti keli žmonės, išsaugo jį atmintyje, detalizuoja ir juo manipuliuoja, ir t.t.

7. Duomenų valdytojo prievolės ir tinkamos apsaugos priemonės

A) Tvarkymo teisėtumas

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

Reikia imtis visų tinkamų priemonių, užtikrinančių, kad vaizdo stebėjimas atitinka duomenų apsaugos principus ir yra vengiama netinkamo kišimosi į privatų gyvenimą¹⁸.

Šiuo atžvilgiu reikia atkreipti dėmesį, kokie geriausi veiksmai gali būti numatomi, remiantis priežiūros institucijų rekomendacijomis ir kitais savireguliacijos aktais.

Taip pat būtina peržiūrėti esančias vidaus teisės nuostatas, įskaitant konstitucinius principus, civilinės ir kriminalinės teisės nuostatas, ypač taikomas „droit a l’image“ (teisei į atvaizdą)¹⁹ ar nuolatinės gyvenamosios vietos apsaugai; būtina atsižvelgti į precedentų teisę, kuri galėjo nurodyti, kad patalpos, skirtingai nuo nesiejamų su namų valda, pvz., viešbučių

¹⁸ Neseniai bankas ir vietos policija negalėjo įvykdyti kliento prašymo iš kamera nufilmuotų vaizdų išgauti vagies atvaizdo, kuris, pavogęs kliento banko kortelę, neteisėtai ją panaudojo, kad iš bankomato paimtų pinigų, tariamai remdamiesi „privataus gyvenimo slaptumu“.

¹⁹ Prancūzijoje ir Belgijoje ši teisė reikalauja „pirminio sutikimo“.

kambariai, biurai, poilsio kambariai, drabužinės, vidinės telefono būdelės, t.t., turi būti laikomos privačiomis.

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

Šis konkretus klausimas yra keliamas todėl, kad kai kurios vietos valdžios institucijos neturi kompetencijos viešosios tvarkos ir visuomenės reikaluose ir, to nepaisydamos, užsiima papildoma veikla stebėjimo tikslais. Taip pat ir stebėjimu, kuris aiškinamas nusikaltimų kontroliavimu, o iš tikrųjų norima gauti įrodymų, jei būtų padaryti kriminaliniai pažeidimai.

B) Tikslų konkretumas, detalizavimas ir teisėtumas

Duomenų valdytojas turi užtikrinti, kad tikslai, kurių jis siekia, nėra neaiškūs ar dviprasmiški, kad galima būtų nustatyti tikslius kriterijus, įvertinant, ar tikslai, kurių siekiama tvarkant, yra suderinti (žr. Direktyvos 6 b) straipsnį).

Šis aiškumas 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, prisilaikant Direktyvos 20 straipsnio.

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

Atitinkami tikslai turi būti aptarti dokumente, kuriame reikėtų apibendrinti ir kitus svarbius privatumo politikos bruožus, atsižvelgiant į tokius svarbius klausimus, kaip laiko fiksavimas, kada vaizdinė medžiaga yra trinama, galimi duomenų subjekto prašymai, norint gauti informaciją, ir/arba teisinės konsultacijos dėl duomenų.

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, kai turi būti vykdomos teisinės prievolės - buvo minėta veikla kazino - arba 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 oficialiosios valdžios nurodymą, galbūt laikantis konkrečių taisyklių, pvz., atskleisti kelių eismo pažeidimus arba smurtinį elgesį viešojo transporto priemonėse didelio nusikalstamumo vietose – pagal Direktyvos 7 e) straipsnį; antraip duomenų valdytojas gali siekti teisėto intereso, kuris nėra viršesnis už duomenų subjekto interesus ar pagrindines teises ir laisves (žr. 7 straipsnio f)).

Abiem atvejais, nors labiau antruoju, ypatingas tvarkymo operacijų pobūdis reikalauja tiksliai apsvarstyti užduoties apimtį, pajėgumus ir duomenų valdytojo teisėtus interesus.

Paviršutiniškumas ir neturintis pagrindo užduoties ir pajėgumų apimties plėtimas turi būti neabejotinai uždrausti atliekant šią analizę.

Dėl skirtingų interesų derinimo, ypatingą dėmesį reikia skirti, iš anksto išklausus suinteresuotus puses, tam, kad saugomi interesai gali prieštarauti sistemos įdiegimui, tam tikrų duomenų išsaugojimo organizavimu arba kitomis tvarkymo operacijomis²⁰.

Pagaliau duomenų subjekto sutikimas turi būti vienareikšmis ir remtis aiškia informacija. Sutikimas turi būti pateikiamas atskirai ir konkrečiai dėl stebėjimo veiklos valdose, kur vyksta privatus asmens gyvenimas.

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

Tvarkymo vaizdo stebėjimo priemonėmis operacijos visada turi remtis tiksliais teisinėmis nuostatomis, jei jas vykdo valstybinės institucijos.

D) Vaizdo stebėjimo naudojimo proporcingumas

Principas, kad duomenys turi būti adekvatūs ir proporcingi tikslams, kurių siekiama, reiškia, kad CCTV ir panaši vaizdo stebėjimo įranga gali būti išdėstoma tik remiantis subsidiariumu, arba kitaip tariant:

1) tikslais, kurie pilnai pateisina tokios sistemos naudojimą.

Administracijos subjektai neturi diegti VS įrangą dėl mažų pažeidimų, pvz., norėdami sustiprinti rūkymo mokyklose ir kitose viešose vietose draudimą arba uždraudus palikti nuorūkas ir šiukšles viešose vietose.

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

Nors proporcinga vaizdo stebėjimo ir apsaugos sistema gali būti laikoma teisėta, jei kartojasi užpuolimai autobusuose atokesnėse vietose ar prie autobusų stotelių, taip nebus, jei sistema naudojama, norint 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 šiukšlių dėžių nėra.

Proporcingumą reikia vertinti pagal griežtesnį kriterijų, kai kalbama apie visuomenei neprieinamas patalpas.

Šiuo atžvilgiu gali būti naudingas pasikeitimas informacija ir patirtimi tarp kompetetingų šalių narių institucijų²².

2) šios sistemos gali būti diegiamos, jei kitos apsaugos ir saugumo priemonės, neatkuriančios vaizdo – pvz., kovojant su vandalizmu dedamos šarvuotos durys, automatiniai

²⁰ 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 nėra pagrindo manyti, kad bus atmesti duomenų subjekto, kuris nusipelno apsaugos, interesai.

²¹ Šiuo atveju galima remtis Portugalijos DAI 8 skyriumi dėl duomenų, susijusių su asmenimis, įtariamų dalyvavus neteisėtoje ir/arba kriminalinėje veikloje.

²² Tai leistų geriau derinti kontrolės būdus ir administracinius sprendimus, kurie kartais skyrėsi, kaip atsitiko, pavyzdžiui, su Bingo salėmis.

vartų įdiegimas ir valymo įranga, jungtinės aliarmo sistemos ir t.t. – pasirodė nepakankamos ir/arba netinkamos, siekiant išvardintų teisėtų tikslų.

Aukščiau pateikti svarstymai taikomi augančiam vaizdo stebėjimo naudojimui savisaugos ir nuosavybės apsaugos tikslais, pirmiausia šalia viešųjų pastatų ir biurų, taip pat aplink esančiose teritorijose. Toks naudojimas reikalauja įvertinti 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 saikingi, apima tikslų įvertinimą *organizavimo proporcingumo*, taikomo duomenų tvarkymui, jei jo teisėtumas buvo patvirtintas.

Reikia atkreipti dėmesį į *filmavimo organizavimą*, atsižvelgiant į šiuos klausimus:

- a) vizualinį kampą ryšium su tikslais, kurių siekiama²³, pvz., jei stebima vieša vieta, kampas turi būti taip nustatytas, kad neleistų matyti detalių ir/arba kūno bruožų, kurie nėra susiję su siekiamais tikslais, arba šalia esančių privačių teritorijų, ypač jei yra įdiegta vaizdo mastelio keitimo funkcija,
- b) filmavimui naudojamos įrangos tipą, pvz., ar ji yra stacionari, ar mobili,
- c) faktinio instaliavimo organizavimą, pvz., kamerų išdėstymo, fiksuoto vaizdo ir/arba besisukančių kamerų naudojimas ir t.t.,
- d) galimybę didinti ir/arba keisti vaizdo mastelį, kai jis yra filmuojamas arba po to, pvz., dėl vaizdų saugojimo,
- e) vaizdo stabdymo funkcijų,
- f) ryšį su „centru“, kad galima būtų siųsti garsinius ir/arba vaizdinius aliarmo signalus,
- g) veiksmus, kurių imamasi dėl vaizdo stebėjimo, pvz., įėjimų uždarymas, stebintio personalo iškvietimas, t.t.

Antra, reikia apsvarstyti *sprendimus dėl vaizdų saugojimo ir jo periodo*, kuris turi būti pakankamai trumpas ir atitikti individualaus atvejo konkrečias ypatybes.

Kai kuriais atvejais gali pakakti sistemos, leidžiančios matyti vaizdus uždarame rate, pvz., kasas 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. Šios taisyklės išimtis būtų atvejais, kai yra gaunamas pavojaus signalas

²³ Konkrečių atsargumo priemonių, kurių reikia imtis dėl vizualinio kampo, pavyzdžių galima rasti dvejose Italijos Duomenų apsaugos institucijos išleistose nuostatose. 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 apsaugą, 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 ir transporto priemonės vidų.

arba pateiktas prašymas, kuris vertas ypatingo dėmesio; tokiais atvejais nėra pagrindo laukti policijos ar teismo instancijų sprendimo.

Galima pateikti kitą pavyzdį, kai sistema, aptinkanti be leidimo miestų centruose ar važiuoti uždraustose vietose naudojamas transporto priemonės, 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 savaitės, pvz., video stebėjimo vaizdai gali būti naudojami, nustatant žmogaus tapatybę, kuris žvalgėsi po banko patalpas prieš įvykdydamas apiplėšimą.

Trečia, reikia kreipti dėmesį į *bylas, kuriose žmogaus tapatybės nustatymą palengvina asmens veido atvaizdų susiejimas su kita informacija apie užfiksuotą elgesį ir/arba veikla*, pvz., tokiu atveju, kai siejami klientų banke atvaizdai ir veikla nesunkiai nustatomu laiku.

Šiuo atžvilgiu reikia paisyti aiškų skirtumą tarp vaizdo stebėjimo priemonėmis, išdėstytomis prie įėjimo 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 aptartas sprendimas, kurį reikia priimti dėl *galimo duomenų perdavimo trečiosioms šalims*, kuris neturėtų įtraukti su vaizdo stebėjimo veikla nesusijusių subjektų, ir jų pilnu ar daliniu paskelbimu užsienyje ar kompiuteriniuose tinkluose, taip pat remiantis atitinkamos apsaugos nuostatomis, žr. Direktyvos 25 straipsnį ir kt.

Yra akivaizdu, jog reikalavimai, kad vaizdai turi būti tinkami ir saikingi, taikomi ir skirtingų vaizdo stebėjimo sistemų valdytojų turimos informacijos derinimui.

Išvardinti apsaugos būdai turėtų įgyvendinti principą, kuris kelių šalių vidaus įstatymuose nurodomas kaip *asmens duomenų naudojimo nuosaikumo principas*, kurio tikslas yra – neleisti tvarkyti asmens duomenų arba kiek yra įmanoma tai sumažinti.

Šis principas turi būti taikomas visuose sektoriuose, atsižvelgiant į tai, kad daug tikslų galima pasiekti ir nenaudojant asmens duomenų arba naudojant anoniminius duomenis, net jei iš pradžių gali atrodyti, kad reikia naudoti asmeninę informaciją.

Išdėstyti svarstymai taikytini, jei yra pateisinamas poreikis modernizuoti verslo resursus²⁴ ar pagerinti vartotojams teikiamas paslaugas²⁵.

F) Informacija duomenų subjektams

Atvirai ir tinkamai naudojant vaizdo stebėjimo įrangą, pagal Direktyvos 10 ir 11 straipsnį, duomenų subjektai turi gauti atitinkamą informaciją.

Duomenų subjektai turi būti informuojami pagal Direktyvos 10 ir 11 straipsnius. Jie turi žinoti, kad vykdomas vaizdo stebėjimas, ir net jei jis susijęs su visuomeniniais įvykiais,

²⁴ Tai galėtų būti toks atvejis, kai reikia suskaičiuoti, kiek kasos aparatų yra laikoma atidarytų tuo pačiu metu prekybos centre, atsižvelgiant į pirkėjų skaičių, arba kai reikalaujama suformuoti geriausius praėjimus pirkėjams prekybos centre.

²⁵ Kad būtų lengviau pasiekti darbo vietą ir/arba konkrečią transporto priemonę, kai reikia kontroliuoti tapatybę, asmens kortelės su nuotrauka gali užtekti, nediegiant veidų atpažinimo sistemos.

renginiais ar reklama („web” kameros), jie privalo turėti išsamią informaciją apie stebimas vietas.

Nėra būtina labai tiksliai nurodyti, kur yra išdėstyta stebėjimo įranga, tačiau stebėjimo prasmė turi būti tiksliai paaiškinta.

Informacija turi būti statoma priimtinu atstumu nuo stebimos vietos – skirtingai nuo kelelių atveju, kai buvo manoma, kad informacinių skydų išdėstymas 500 metrų atstumu nuo stebimų zonų yra priimtinas –, atsižvelgiant į filmavimo organizavimą.

Informacija turi būti matoma ir gali būti pateikta labai glaustai, jeigu tik ji bus efektyvi; joje gali būti simbolių, kurie pasirodė esą naudingi, ryšium su informavimu apie vaizdo stebėjimą ar informacija, kad rūkyti uždrausta, kurie gali skirtis, atsižvelgiant į tai, ar vaizdai yra įrašomi, ar ne. Visais atvejais turi būti nurodomi vaizdo stebėjimo tikslai ir atitinkamas valdytojas. Informacijos apimtis turi būti derinama prie individualios vietos.

Konkretūs, pagrįsti informacijos reikalavimų ribojimai leidžiami tik atvejais, nurodytais Direktyvos 13 straipsnyje (ir 10 bei 11 straipsniuose), pvz., laikini apribojimai gali būti taikomi ryšium su teisėto tyrimo metu gynybos advokato surinktais duomenimis arba vykdamas teisę į gynybą tokiam laikotarpiui, kol dėl informacijos rengimo gali kilti pavojus, kad nebus pasiekti norimi tikslai.

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 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 ribotam fizinių asmenų skaičiui ir tik tais tikslais, kurių siekiama, naudojant vaizdo stebėjimo priemones, arba ryšium su atitinkamos įrangos priežiūra, kad galima būtų įsitikinti, ar ji gerai veikia; kitu atveju, tai gali būti atliekama prašant duomenų subjektui arba policijos ar teismo institucijoms teisėtai reikalaujant dėl nusikaltimo tyrimo.

Kai vaizdo stebėjimo tikslas yra nusikaltimų prevencija, tyrimas ir kontroliavimas, sprendimas dėl dviejų priėjimo būdų naudojimo – vienas priklausys valdytojui, o kitas policijai – gali būti naudingas, užtikrinant, kad vaizdus peržiūri tik policijos, o ne neturintis tam įgaliojimo, personalas, nepažeidžiant duomenų subjekto įstatymais patvirtintos teisės gauti informaciją, jam pateikus prašymą per trumpą laiko tarpą, kol vaizdai yra saugomi.

B) Turi būti imtasi tinkamų apsaugos priemonių, kad neatsitiktų Direktyvos 17 straipsnyje minimi įvykiai, įtraukiant informacijos, kuri gali padėti apsaugoti duomenų subjekto, trečiosios šalies ar paties duomenų valdytojo teisę, paskleidimą, taip pat atsižvelgiant į manipuliavimo, pakeitimo ar įkalčių sunaikinimo prevenciją.

C) Įrašytų vaizdų kokybė taip pat svarbi, ypač jei kelis kartus naudota ta pati įrašymo priemonė, dėl ko gali kilti rizika, kad nepavyks gerai ištrinti anksčiau įrašytų vaizdų.

D) Pagaliau yra labai svarbu, kad konkrečiai vaizdo stebėjimą vykdančios operatoriaus būtų tinkamai mokomi ir žinotų, ką reikia daryti, kad jų veikla visiškai atitiktų būtinus reikalavimus.

H) Duomenų subjekto teisės

Surinktų asmens duomenų individualios ypatybės nedraudžia duomenų subjektui įgyvendinti savo teises, nurodytas Direktyvos 14 (ir 13) straipsnyje, ypač akcentuojama teisė nesutikti su tvarkymu, turint teisėtą pagrindą.

Duomenų subjekto teisė užmiršti ir teisė į paprastai trumpą vaizdų saugojimo laiką 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 apsaugoma ir trečiosios šalies teisė.

Bet kokie ribojimai, grindžiami pastangomis atkurti vaizdus, kai tokios pastangos yra aiškiai neproporcingos dėl trumpo vaizdų saugojimo laikotarpio, turi būti išdėstyti išimtinai pirminiuose įstatymuose (žr. Direktyvos 13(1) straipsnį), atsižvelgiant į duomenų subjekto teisę į gynybą ryšium su svarstomuoju laikotarpiu atsitikusiais konkrečiais įvykiais.

I) Papildomos apsaugos priemonės ryšium su konkrečiomis tvarkymo operacijomis

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

Neturėdama tikslo sudaryti išsamų sąrašą, kur vaizdo stebėjimas gali būti taikomas, Darbo Grupė norėtų akcentuoti, kad reikia kreipti didesnę dėmesį – iš esmės, kur yra tinkama, atliekant Direktyvos 20 straipsnyje minimą išankstinę tvarkymo operacijų patikrą – į kelis kontekstus, kada renkami vaizdai, susiję su asmenimis, kurių tapatybė yra arba gali būti nustatyta, kadangi šie kontekstai turi būti įvertinti, remiantis 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,

b) galimas vaizdinių ir biometrijos duomenų, pvz., pirštų antspaudų, sujungimas (pvz., prie įėjimų į bankus),

c) balso identifikavimo sistemos naudojimas,

d) įdiegimas, remiantis proporcingumo principais ir konkrečiomis nuostatomis, indeksavimo sistemų, taikomų vaizdo įrašams ir/arba jų vienalaikio automatinio atstatymo, ypač per tapatybės nustatymo duomenis, sistemoms,

e) veido atpažinimo sistemų naudojimas, kurios gali nustatyti praeinančių asmenų maskuotę, pvz., netikras barzdas ar perukus, tačiau svarbiausia jų funkcija yra nusitaikyti į įtariamus pažeidėjus – pvz., sistemų galėjimas automatiškai nustatyti tam tikrų asmenų tapatybę, remiantis šablonais ir/arba standartiniais identifikavimo požymių komplektais, kuriuos sudaro tam tikri išorės bruožai (asmens odos, akių spalva, išsišovę skruostikauliai ir t.t.) arba remiantis iš anksto apibrėžtu nenormaliu elgesiu (staigūs judesiai, pakartotinis perėjimas, net konkrečiais intervalais, transporto priemonės parkavimo būdas ir t.t.). Todėl čia

žmogaus įsikišimas yra tinkamas ir dėl tokiomis atvejais pasitaikančių klaidų ir kaip minima f) punkte žemiau,

f) galimybė automatiškai aptikti maršrutus ir pėdsakus ir/arba rekonstruoti ar numatyti asmens elgesį,

g) automatiniai sprendimai, besiremiantys asmens profiliu 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 apie asmens duomenų tvarkymą darbo santykių kontekste, priimtoje 2001 m. rugsėjo 13 d., ir Darbo dokumente *Dėl elektroninės komunikacijos sekimo darbo vietoje*, priimto 2002 m. gegužės 29 d.²⁶, ši Darbo Grupė jau atkreipė dėmesį į keletą principų, skirtų apsaugoti duomenų subjektų teises, laisves ir orumą darbo santykių kontekste.

Be abiejuose aukščiau minėtuose dokumentuose pateiktų svarstymų, pagal jų pritaikymo vaizdo stebėjimui laipsnį, yra tikslinga pabrėžti, kad vaizdo stebėjimo sistemos, tiesiogiai taikomos kontroliuoti kokybę ir darbo apimtį iš nuotolio, todėl įtraukiančios asmens duomenų tvarkymą, paprastai neturi būti leidžiamos.

Visai kitaip yra, kai vaizdo stebėjimo sistemos yra išdėstomos dėl gamybos ir/arba darbo saugumo reikalavimų, kur taip pat stebima iš nuotolio, nors netiesiogiai²⁷.

Įdiegimo patirtis parodė, kad nereikėtų stebėti patalpų, kurios skirtos darbuotojų privačiam naudojimui arba jose nenumatyta atlikti darbo užduotis – tualetai, dušas, rakinamos spintelės ir rekreacinės zonos; vaizdai, renkami norint apsaugoti turta ir/arba dėl rimtų pažeidimų tyrimo, prevencijos ir kontrolės, neturi būti naudojami kaltinant darbuotoją mažais disciplinos pažeidimais; darbuotojams visada turi būti leidžiama paduoti priešieškinius, naudojantis surinkta vaizdo medžiaga.

9) Išvados

Darbo Grupė pateikė šio darbo dokumento projektą, siekdama suvienodinti nacionalinių priemonių, priimtų pagal vaizdo stebėjimo Direktyvą 95/46/EB, taikymą.

.....

Taip pat yra labai svarbu, kad šalys narės numatytų, kuo reikia vadovautis ryšium su gamintojų, paslaugų teikėjų ir platintojų veikla, bei tyrėjų, atsižvelgiant į technologijų, programinės įrangos ir techninių prietaisų, kurie atitinka šiame dokumente nurodytus principus, vystymąsi.

²⁶ Abu dokumentus galima rasti šiuo adresu:

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

²⁷ 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 gaunamą informaciją, prisilaikant duomenų apsaugos įstatymų; kitais atvejais reikia siekti pirminio susitarimo su darbuotojų atstovais arba profesinių sąjungų organizacijomis dėl stebėjimo sistemos įdiegimo, stebėjimo trukmės ir kitokio filmavimo. Keliose šalyse gali prirėkti valstybinio įsikišimo, jei susijusios šalys negali susitarti.

29 STRAIPSNIO DARBO GRUPĖS DARBO DOKUMENTAS VIDEO STEBĖJIMAS IR DUOMENŲ APSAUGA SANTRAUKA

Per paskutiniuosius kelerius metus Europos valstybinėse ir privačiose įstaigose vis dažniau naudojamos vaizdo atpažinimo sistemos. Šiuo darbo dokumentu visų pirma siekiama atkreipti dėmesį į daugybę kriterijų, įvertinant ar vaizdo stebėjimo sistemos instaliavimas yra teisėtas ir tinkamas fizinių asmenų, kurių tapatybė yra nustatyta arba gali būti nustatyta, atžvilgiu.

Dokumente pateikiama pirminė analizė, kuri pradedama nuo iš dalies skirtingų taisyklių aptarimo, nuo priimtų labai detalių nacionalinių įstatymų nuostatų, į kurias būtina žvelgti sistemiškiau ir harmoningiau. Šiai analizei neturi reikšmės naudojama įranga ir ji apima visus vaizdo stebėjimo būdus apskritai.

Be to, dokumente nagrinėjami principai taikomi vaizdo atpažinimui, kiek galima siejant su garso ir/arba biometriniiais duomenimis, pvz., pirštų antspaudais.

Kiekvienas operatorius galės patikslinti pateiktus nurodymus ir dėl atitinkamos srities ir dėl ateities technologijų vystymosi, kuri Darbo grupė siekia iširti.

1. STEBĖJIMAS PAGAL DIREKTYVĄ 95/46/EB

Asmeninės informacijos, įtrauktos į garso ir vaizdo duomenis, tvarkymo specifinės ypatybės yra akcentuojamos Direktyvoje 95/46/EB, kurioje apie jas aiškiai kalbama keletose vietose. Garso ir vaizdo duomenų tvarkymo specifiskumas ir ypatingumas yra pripažinti Direktyvos paskutiniame straipsnyje, kuriame Komisija įsipareigoja išnagrinėti Direktyvos taikymą šiuo klausimu, atsižvelgiant į informacinių technologijų vystymąsi (33 str.).

2. SRITYS, KURIOSE DIREKTYVA 95/46/EB VISAI ARBA IŠ DALIES NETAIKOMA

Vaizdo stebėjimui, vykdomam visuomenės saugumo, gynybos, valstybės saugumo ar valstybinės veiklos kriminalinės teisės sferoje tikslais, ir/arba kitokios veiklos, kurios neriboja Bendrijos teisė, tikslais, taip pat fizinio asmens atliekamam tvarkymui asmeniniais ar ūkio tikslais nėra taikomos Direktyvos nuostatos, kurios taip pat tik iš dalies taikomos tvarkymui žurnalistikos ar panašiais tikslais. Reikalavimai, nustatyti tarptautiniuose aktuose ar kitose nacionalinėse nuostatose (pvz., valstybės civilinės teisės sistemoje), garantuojančiuose asmens „*droit a l'image*“ (teisę į atvaizdą) ir asmens teises, taip pat turi būti gerbiami.

3. DUOMENŲ VALDYTOJO PAREIGOS IR TINKAMOS ATSARGUMO PRIEMONĖS

Darbo grupė akcentuoja, kad šios rekomendacijos yra tinkamos ryšium su vaizdo stebėjimo naudojimu. Jos skiriamos duomenų valdytojams, laikantis Direktyvos 95/46/EB nuostatų. Todėl viena iš atsargumo priemonių, kurių turėtų imtis duomenų valdytojas, yra patikrinti, ar vaizdo stebėjimas sukelia asmens duomenų tvarkymą, susijusį su asmenimis, kurių tapatybė gali būti nustatyta. Jei taip, Direktyva taikoma nepaisant nacionalinių nuostatų, kuriose papildomai reikalaujama įgaliojimo visuomenės saugumo tikslais.

A) Tvarkymo teisėtumas

Duomenų valdytojas turėtų patikslinti, ar stebint laikomasi bendrųjų ir specifinių šiai sričiai taikomų nuostatų. Reikia imtis visų tinkamų priemonių, užtikrinančių, kad vaizdo stebėjimas nepažeidžia duomenų apsaugos principų. Taip pat būtina patikslinti vidaus teisės

nuostatas, ypač dėl „*droit a l'image*“ (teisės į atvaizdą) arba dėl gyvenamosios vietos apsaugos.

B) Tikslų specifiškumas, specifikacija ir teisėtumas

Duomenų valdytojas turėtų užtikrinti, kad siekiami tikslai nėra nei neaiškūs, nei dviprasmiški. Reikėtų aiškiai riboti galimybę turimus vaizdus naudoti kitiems tikslams, ypač atsižvelgiant į technines reprodukcijos galimybes. Tinkami tikslai turėtų būti išvardinti Dokumente, kuriame turėtų būti apibendrintos ir kitos svarbios privatumo politikos ypatybės.

C) Tvarkymo teisėtumo kriterijai

Duomenų valdytojas turėtų patvirtinti, kad vaizdo stebėjimas atitinka ne tik A) dalyje minėtas specialias nuostatas, bet taip pat nors vieną iš tvarkymo teisėtumo kriterijų, pateiktų Direktyvos 7 straipsnyje. Vaizdo stebėjimo priemonėmis atliekamas tvarkymas, jei jį vykdo valstybinė įstaiga, visada turėtų remtis aiškiais teisinėmis nuostatomis.

D) Vaizdo stebėjimo naudojimo proporcingumas

Principas, kad duomenys turi atitikti norimus tikslus, visų pirma reiškia, kad CCTV ir panaši vaizdo stebėjimo įranga duomenų valdytojo gali būti išdėstoma remiantis subsidiariumu, tai reiškia tokiais tikslais, kurie iš tikrųjų pateisina tokios sistemos naudojimą, ir jei kitos apsaugos ir saugumo priemonės, nereikalaujančios vaizdo atkūrimo, pasirodo aiškiai nepakankamos ir/arba neatitinkančios teisėtų tikslų.

E) Vaizdo stebėjimo vykdymo proporcingumas

Duomenų valdytojas turėtų skirti reikiamą dėmesį į kelių šalių vidaus įstatymuose minimą *asmens duomenų naudojimo nuosaikumo* principą. Jie turėtų atidžiai nustatyti duomenų tvarkymo, jei tik jo teisėtumas yra patvirtintas, *proporciumą*. Pirmiausia reikėtų apgalvoti *filmavimo organizavimą*; antra, turi būti apsispręsta dėl *vaizdo išsaugojimo ir saugojimo laikotarpio*, kuris turi būti pakankamai trumpas ir derinamas pagal individualaus atvejo specifinius požymius. Trečia, reikėtų kreipti ypatingą dėmesį į atvejus, kai, *palengvinant asmens tapatybės nustatymą*, asmens veido atvaizdas siejamas su kita informacija apie užfiksuotą elgesį ir/arba veiklą. Būtina atsižvelgti į *galimą duomenų perdavimą trečiosioms šalims*.

F) Informacija duomenų subjektams

Duomenų subjektams turėtų būti teikiama tinkama informacija pagal Direktyvos 10 ir 11 straipsnius. Informacija turi būti *matoma* ir gali būti pateikta labai *apibendrinta* su ta sąlyga, kad tai yra *efektyvu*; tai gali būti *simboliai*, kurie pasirodė esantys efektyvūs ryšium su vaizdo stebėjimu ir informacija „nerūkoma“, galintys skirtis priklausomai nuo to, ar vaizdai yra įrašyti, ar ne. Vaizdo stebėjimo tikslai ir valdytojas visais atvejais turi būti tiksliai apibūdinti. Informacijos pobūdis turi būti derinamas pagal konkrečią aplinką.

G) Papildomi reikalavimai

Apie asmens duomenų tvarkymą turi būti informuojama ir jo priežiūrą vykdydys nepriklausoma įstaiga pagal Direktyvos 18, 19 ir 28 straipsnius. Darbo Grupė atkreipia dėmesį į tai, kad asmenų, galinčių naudotis vaizdo įrašais, teikiančių atitinkamas saugumo priemones, užtikrinančių tinkamą vaizdo kokybę ir vaizdo stebėjimu užsiimančių darbuotojų mokymu, kiekis turi būti ribotas.

H) Duomenų subjekto teisės

Duomenų valdytojais turėtų žinoti, kad duomenų subjektai gali pilnai naudotis savo teisėmis, išvardintomis Direktyvos 13 ir 14 straipsniuose, ir ypač atkreipti dėmesį į teisę nesutikti su tvarkymu, turėdami tam įtikinamą teisinį pagrindą. Bet kokie naudojimosi teisės apribojimai gali būti leidžiami išimtinai tik tada, jei juos nustato įstatymai (žr. Direktyvos 13(1) straipsnį).

I) Papildomos apsaugos priemonės ryšium su specifiniais tvarkymo veiksmis

Reikėtų drausti vaizdo stebėjimą, jei jis vykdomas išimtinai tik dėl asmenų rasinės kilmės, jų religinių ar politinių įsitikinimų, dėl dalyvavimo profsąjungose arba seksualinių polinkių (Direktyvos 8 straipsnis). Darbo grupė pabrėžia, kad reiktų kreipti didesnę dėmesį – kur tai atitinka Direktyvos 20 straipsnyje minėtą tvarkymo veiksmų išankstinę patikrą – į

konkrečias situacijas, kada renkami atvaizdai asmenų, kurių tapatybė yra nustatyta ar gali būti nustatyta, nes šios situacijos turėtų būti įvertintos, remiantis kiekvienu konkrečiu atveju; tai taikoma sujungtoms kelioms vaizdo stebėjimo sistemoms, vaizdo duomenų ir biometrinių duomenų sujungimui, balso ir/arba veido atpažinimo sistemų naudojimui, indeksavimo sistemų įgyvendinimui ir automatinio tvarkymo specialioms rūšims.