MYKOLO ROMERIO UNIVERSITETO
EKONOMIKOS IR FINANSŲ VALDYMO FAKULTETO
INFORMATIKOS IR STATISTIKOS KATEDRA

ŽILVINAS JUCIUS
INFORMATIKOS TEISĖ

ASMENS DUOMENŲ TEISINĖ APSAUGA TVARKANT DUOMENIS POLICIJOS INFORMACINĖSE SISTEMOSE

Magistro baigiamasis darbas

Darbo vadovas-
Doc. dr. Darius Štitilis

Vilnius, 2005

TURINYS

ĮVADAS 3
1. ASMENS DUOMENYS, JŲ SAMPRATA IR REGLAMENTAVIMAS 5
1.1. Asmens duomens samprata 5
1.2. Asmens duomenų apsaugos reglamentavimas 7
1.3. Duomenų valdytojai policijos įstaigose 11
2. ASMENS DUOMENŲ TVARKYMAS IR POLICIJOS INFORMACINĖS SISTEMOS 17
2.1. Duomenų tvarkymo principai 17
2.2. Informacijos poreikis policijoje 22
2.3. Policijos programinis paketas ir jame tvarkomi asmens duomenys 24
2.4. Asmens kodas informaciniuose registruose 34
2.5. Teisė į informaciją tvarkant duomenis viešose duomenų rinkmenose 43
2.6. Informacinių sistemų priežiūra 46
3. ASMENS DUOMENŲ TVARKYMAS VAIZDO STEBĖJIMO PRIEMONĖMIS 49
3.1. CCTV sistemos ir jų atsiradimo prielaidos 49
3.2. Vaizdo apdorojimo sistemos Vilniaus policijoje 51
3.3. Vaizdo stebėjimo sistemų teisinio reguliavimo ir praktikos analizė 57
4. IŠVADOS IR PASIŪLYMAI 68
LITERATŪROS SĄRAŠAS 71
Įstatymai 71
Tarptautiniai dokumentai 71
Kita literatūra 72
Interneto tinklapių adresai 74
SANTRAUKA 75
SUMMARY 76

ĮVADAS

Kiekvienas asmuo turi teisę į asmeninio ir šeimos gyvenimo, namų ir korespondencijos privatumą.

- Europos žmogaus teisių ir pagrindinių laisvių konvencija [1]

Asmens duomenų apsauga yra neatsiejama nuo vienos svarbiausių žmogaus teisių – teisės į privataus gyvenimo neliečiamumą, užimančios svarbią vietą kiekvieno žmogaus gyvenime. Demokratinės valstybės sąlygomis yra svarbu nustatyti pusiausvyrą tarp viešųjų ir privačių interesų, žmogaus teisės gauti ir skleisti informaciją ir teisės į pagarbą jo privačiam ir šeimos gyvenimui.

Teisė į privatų gyvenimą yra viena iš naujausių žmogaus teisių Lietuvoje. Asmens privataus gyvenimo apsaugai skiriama pakankamai dėmesio, tačiau šių nuostatų įgyvendinimas yra nepakankamas, todėl svarbu, kad kiekvienas žmogus, nepaisant įvairių rizikos veiksnių, visų pirma susijusių su informacijos technologijų plėtra, jaustųsi saugus tokiame pasaulyje.

Sparčiai vystantis naujoms technologijoms, pasauliniu mastu susiduriama su problema – kaip sudaryti palankias sąlygas informacijos technologijų plėtrai ir sukurti saugią teisinę aplinką, kurioje būtų ginama žmogaus teisė į privataus gyvenimo neliečiamumą. Iškilo naujų pavojų asmens privataus gyvenimo neliečiamumui. Kompiuterinių technologijų atsiradimas, įgalino valdžią ir teisėsaugos institucijas kaupti informaciją apie asmenis, sukūrė sąlygas naujiems privatumo pažeidimams.

Kompiuteriniai tinklai iškėlė dar didesnę grėsmę asmens privatumui, nes sudarė galimybę tvarkyti informaciją, susijusią su asmens duomenimis, o teisėsaugos institucijas įgalino sekti asmenį tiesiog gatvėje pasinaudojant moderniomis vaizdo kameromis - CCTV[2].

Vaizdo stebėjimas gali būti efektyvi nusikaltimų prevencijos ar jų išaiškinimo priemonė, tačiau nepakankamas šių sistemų teisinis reglamentavimas gali sukelti grėsmę privataus gyvenimo saugumui. Ši sparčiai besivystanti stebėjimo sfera reikalauja specifinio ir konkretaus reguliavimo, norint sumažinti pažeidimų galimybę.

Susirūpinimą žmogaus teisių apsaugos požiūriu kelia ir vis dažnesnis nepagrįstas asmens kodo panaudojimas kuris sukuria galimybes prieiti prie daugelio asmenų asmens duomenų ir taip pažeisti jų privatų gyvenimą. Žinant konkretaus žmogaus asmens kodą, galima nesunkiai sujungti į visumą

[1] Europos žmogaus teisių ir pagrindinių laisvių konvencija, V.Ž., 1995, Nr. 40-987.
[2] Terminą „vaizdo stebėjimo kameros“ reikia suprasti abstrakčiai, nesigilinant į technines jų charakteristikas. Technine prasme CCTV suprantama dvejopai: pirma, kaip kabelinė televizija, antra, kaip skaitmeninė vaizdo stebėjimo sistema.

įvairiose įstaigose turimą informaciją apie asmenį ir taip sužinoti viską apie konkretaus žmogaus gyvenimą.

Pasirinktos temos aktualumas išryškėja stebint visuomenės sužavėjimą technologinės revoliucijos atneštomis galimybėmis, kurios kartu kelia ir daug neaptartų problemų, kurias visuomenė turėtų neatidėliodama spręsti, o viena didžiausių problemų – žmogaus teisių apsauga.

Darbo tema **-** Asmens duomenų teisinė apsauga tvarkant duomenis policijos informacinėse sistemose.

Šio darbo **tyrimo objektas** – asmens duomenų teisinis reglamentavimas viešosios policijos sektoriuje[3], esminį dėmesį skiriant toms teisės aktų nuostatoms, kurios yra jautriausios šiandieninei visuomenei, asmens privatumo vertybei, taip pat reiškiniai, veikiantys vaizdo stebėjimo kamerų (CCTV) poveikį visuomenės saugumo būklei.

Pagrindinis **darbo tikslas** – išanalizuoti asmens duomenų tvarkymo policijos informacinėse sistemose teisinius aspektus.

Rašant magistrinį baigiamąjį darbą naudotasi sisteminės analizės, kontentinės (turinio) analizės, dokumentų analizės, loginiu, lyginamuoju ir statistiniu metodais.

Magistrinio **baigiamojo darbo uždaviniai**:

1. Aptarti esamas policijos informacines sistemas ir jose tvarkomus asmens duomenis, pateikti normatyvinius pasiūlymus, siekiant sklandaus laipsniško policijos informacinių sistemų standartizavimo ir unifikavimo.
2. Pateikti asmens duomenų apsaugos įstatyme reglamentuojančių duomenų apsaugą normų problematiką siejant ją su policijos sektoriumi.
3. Išanalizuoti teisės normas, reglamentuojančias vaizdo stebėjimų kamerų (CCTV) naudojimą viešose vietose, bei nustatyti jų veiksmingumą, pateikti teisines rekomendacijas šioje srityje.

Iškelti uždaviniai sprendžiami trijose darbo dalyse.

Pirmoje darbo dalyje aptariama asmens duomens samprata, teisinė bazė, kuri reguliuoja informacijos privatumo ir asmens duomenų apsaugą remiantis nacionaliniais ir Europos Sąjungos teisės aktais, bendrieji asmens duomenų apsaugos klausimai, duomenų valdytojai policijos informacinėse sistemose.

[3] Didelė dalis informacinių sistemų naudojamų kriminalinėje ar kitose ne viešosios policijos rūšyse reglamentuoja teisės aktai kurie skirti „riboto naudojimo“ todėl darbe pagrindinai nagrinėjama tik viešosios policijos informacinės sistemos ir jų reglamentavimas.

Antrojoje dalyje aptariami bendrieji duomenų tvarkymo principai ir sąlygos, pateikiama policijos informacinių sistemų samprata, poreikis, valdymo perspektyvos, analizuojama informacijos privatumo ir duomenų saugumo priežiūra.

Trečiojoje dalyje analizuojamas vaizdo kamerų panaudojimo policijos veikloje teisinis reglamentavimas. Pateikta teises aktų lyginamoji analizė bei vaizdo stebėjimo sistemų įdiegimo ir vykdymo proporcingumas bei aptariamos problemos šioje srityje.

Magistriniame darbe akcentuojamas teorinis ir praktinis privatumo užtikrinimo galimybių tyrimas, pritaikant literatūros šaltinių, straipsnių, apklausų, diskusijų, konferencijų medžiagas, privatumą reglamentuojančių Lietuvos Respublikos ir Europos Sąjungos teisės aktų analizės, faktinių duomenų bei palyginamosios analizės metodus. Toks darbo organizavimas padėjo nuosekliai analizuoti ir spręsti iškeltus uždavinius bei padėti pagrindus tolesniems Lietuvos privatumo užtikrinimo policijoje tyrimams.

Magistrinį darbą sudaro 70 psl., jame pateiktos nedidelės lentelės, iliustracijos, grafikai bei schemos.

1. ASMENS DUOMENYS, JŲ SAMPRATA IR REGLAMENTAVIMAS

1.1. Asmens duomens samprata

Asmens teisė į privatumą ir slaptumą žinoma jau nuo seno. Dar Biblijoje gausu asmens teisės į privatumą pasireiškimo pavyzdžių. Turėjo praeiti daug laiko, kol ši teisė tarptautiniu mastu buvo įtvirtinta kaip visuotinai pripažinta socialinė vertybė – 1948 m. JT Visuotinėje žmogaus teisių deklaracijoje (12 str.), 1950 m. EŽTK 8 str. Šiuose pamatiniuose žmogaus teisių šaltiniuose asmens teisė į privatumą, slaptumą įtvirtinta kaip pagrindinė, fundamentali (nors be abejo – ne absoliuti) žmogaus teisė.

Asmens duomens sąvoka šiuo metu yra apibrėžta trijuose tarptautiniuose teisės aktuose: Duomenų apsaugos direktyvoje, Strasbūro konvencijoje dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu, EBPO Rekomendacijoje dėl asmens privatumo apsaugos ir asmens duomenų judėjimo tarp valstybių narių gairių. Visuose teisės aktuose pateikiamos sąvokos atsirado, esant centralizuotai asmens duomenų tvarkymo sistemai, kurioje priėjimas prie asmens duomenų galėjo būti tik fizinis, o kopijavimas ir kitoks rinkimas ar perdavimas buvo gan sudėtingas.

Lietuvos Respublikos Asmens duomenų teisinės apsaugos įstatymo (toliau - ADTAĮ) 2 straipsnio 1 dalyje apibrėžiama, kad „**asmens duomenys** – bet kuri informacija, susijusi su fiziniu asmeniu – duomenų subjektu, kurio tapatybė yra žinoma arba gali būti tiesiogiai ar netiesiogiai

nustatyta pasinaudojant tokiais duomenimis kaip asmens kodas, vienas arba keli asmeniui būdingi fizinio, fiziologinio, psichologinio, ekonominio, kultūrinio ar socialinio pobūdžio požymiai“.[4]

Pagal Duomenų apsaugos direktyvos 95/46/EB 2 str. ***asmens duomenys*** *reiškia bet kurią informaciją, susijusią su asmeniu (duomenų subjektu), kurio tapatybė yra nustatyta arba gali būti nustatyta; asmuo, kurio tapatybė gali būti nustatyta yra tas asmuo, kurio tapatybė gali būti nustatyta tiesiogiai ir netiesiogiai, ypač pasinaudojus nurodytu asmens identifikavimo kodu arba vienu ar keliais to asmens fizinei, fiziologinei, protinei, ekonominei, kultūrinei ar socialinei tapatybei būdingais veiksniais.*

Tiek pagal 1981 m. Europos Tarybos konvenciją “Dėl asmenų apsaugos, susijusios su automatizuotu asmens duomenų apdorojimu”, tiek pagal EBPO Rekomendaciją “Dėl asmens privatumo apsaugos ir asmens duomenų judėjimo tarp valstybių narių gairių” *asmens duomenys apibrėžiami kaip bet kokia informacija, susijusi su identifikuotu ar identifikuotinu asmeniu.*

Platus apibrėžimo spektras apima visokią informaciją, susijusią su fiziniu asmeniu, net lengvai gaunamą ir neesminę informaciją ir duomenis. Sąvoka „informacija“ apima garso, vaizdo, genetinius duomenis, pirštų atspaudus ir t.t. Kaip matyti, asmens duomenų apibrėžimas akcentuoja du kriterijus - tiesioginį ir netiesioginį asmens tapatybės nustatymą. Tai teoriškai leidžia apimti labai daug duomenų, kurie turi labai menką ryšį su konkrečiu asmeniu. Todėl, duomenys gali būti asmeniniai netgi, jeigu jų pagalba asmuo gali būti identifikuotas tik kombinacijoje su kitais - pagalbiniais duomenimis. Tuo pačiu, yra nustatomi tam tikri apribojimai identifikuotinumo kriterijų atžvilgiu - identifikacija turi būti galima nepanaudojus neprotingas laiko, darbo ir pan. sąnaudų.

Direktyvos 95/46/EB įžanginė 26 citata teigia, kad norint nustatyti, ar asmens tapatybė gali būti nustatyta, reikėtų atsižvelgti į visas priemones, kuriomis galėtų pasinaudoti duomenų valdytojas ar bet kuris kitas asmuo minėto asmens identifikacijai. Direktyvos apibrėžimas pateikia asmens duomenų sąryšio koncepciją. Asmens duomenys tarsi sugrupuojami į dvi kategorijas: identifikatorius ir kitus duomenis. Identifikatoriai nurodo konkretų realų asmenį. Fizinis asmuo paprastai identifikuojamas pagal tokią informaciją kaip vardas, pavardė, amžius, gimimo data, akių spalva ir t. t. arba pagal jam suteiktą tam tikrą numerį (kodą), pavyzdžiui, asmens kodą, vairuotojo pažymėjimo numerį. Tipiškiausias identifikatoriaus pavyzdys – asmens kodas, registracijos numeris, leidimo numeris ir pan. Visi duomenys, identifikatoriaus susieti su asmens duomenų subjektu, tampa asmens duomenimis. Jeigu identifikatoriaus nėra, duomenys nebetenka asmens duomenų statuso, nors ir susiję su realiu asmeniu. Vis dėlto asmeninė informacija gali tapti asmens

[4] Lietuvos Respublikos Asmens duomenų teisinės apsaugos įstatymas // V.Ž., 1996, Nr. 63-1479

duomeniu, tai yra tapti pakankama identifikuoti tam tikrą asmenį ne vien tik identifikatoriaus pagalba. Taip gali atsitikti tais atvejais, kai asmeninės informacijos sankaupa, sistema, kurios atskiri elementai yra susiję su konkrečiu asmeniu, tačiau vienareikšmiškai negali patvirtinti jo tapatybės, įgauna naują savybę, kuria negali pasižymėti jos sudedamosios dalys – identifikuoti konkretų asmenį.[5] Šioje vietoje kyla asmeninės informacijos ir asmens duomens santykio problema. Asmeninė informacija savaime nėra ir negali būti asmens duomeniu iki tol, kol ją susiejus su kita asmenine informacija arba identifikatoriumi tampa įmanomas konkretaus asmens identifikavimas.[6] Asmeninės informacijos ir asmens duomens santykio klausimas itin svarbus tuo, kad asmens duomenų apsaugos reikalavimai taikomi ne bet kokiai asmeninei informacijai, o tik tokiai, kurios pagalba galima konkretaus asmens identifikacija.

Asmens duomenys apie rasinę kilmę, politinius, religinius ar kitus įsitikinimus, taip pat duomenys apie teistumą, sveikatą ar intymų gyvenimą pagal 1981 m. Europos Tarybos konvenciją "Dėl asmenų apsaugos, susijusios su automatizuotu asmens duomenų apdorojimu" priskiriami specialioms asmens duomenų apsaugos kategorijoms ir negali būti apdorojami automatizuotai, nebent nacionalinėje teisėje būtų numatyta tinkama jų apsauga. Duomenų apsaugos direktyva 95/46/EB tokio pobūdžio duomenis įvardija kaip ypatingus asmens duomenis[7] ir leidžia jų tvarkymą tik ypatingais atvejais.

Asmens duomenis pagal duomenų (informacijos) valdytoją ir informacijos turinį galima būtų grupuoti taip:

valstybės turimi duomenys apie asmenį;

medicininiai įrašai apie asmenį;

asmens mokymosi įrašai;

kreditiniai asmens duomenys;

kiti duomenys apie asmenį.

Kadangi magistriniame darbe bus aptariama asmens duomenų tvarkymas policijos informacinėse sistemose, mus domins tik pirmoji ir paskutinioji asmens duomenų grupės.

1.2. Asmens duomenų apsaugos reglamentavimas

Šiame skyriuje trupai išvardinsiu pagrindinius teisės aktus kuriais reglamentuojama asmens duomenų apsauga užsienio valstybėse ir Lietuvoje.

---

[5] M.Civilka Asmens duomenų apsaugos teisinis reguliavimas interneto kontekste. http://www.itc.tf.vu.lt/mokslas/mokslas.html prisijungimo laikas: 2004-11-28

[6] ten pat

[7] Ypatingi asmens duomenys išskiriami ir Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo 2 str.// V.Ž., 1996, Nr. 63-1479

Tarptautiniai Teisės aktai, susiję su Asmens Duomenų Apsauga

- 1948 m. JT Visuotinė žmogaus teisių deklaracija (12 str.);
- 1950 m. Europos žmogaus teisių ir pagrindinių laisvių konvencija (EŽTK) (8str.); Įtvirtinus asmens teisę į privatumą buvo pradėti pagrindai asmens duomenų apsaugai;
- 1980 m. EBPO Asmens privatumo apsaugos gairės; Tarybos rekomendacijos nėra teisiškai privalomos ir greičiau išreiškia politinę, moralinę valstybių narių valiai ir įsipareigojimus. EBPO Taryba rekomendavo, kad Valstybės narės savo nacionalinėje įstatymų leidyboje atsižvelgtų į principus, užtikrinančius privatumo apsaugą ir individo laisves, įtvirtintus Gairėse.
- 1981 m. Europos Tarybos šalių narių Konvenciją dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS, Nr. 108)[8]. Konvencijos tikslas – užtikrinti, „kad, tvarkant asmens duomenis automatizuotai, visų šalių teritorijose bus gerbiamos kiekvieno asmens, nepaisant jo tautybės ir gyvenamosios vietos, teisės ir pagrindinės laisvės, o svarbiausia, jo teisė į privatų gyvenimą.“[9] Konvenciją pasirašiusios šalys įsipareigojo dėl asmens duomenų rinkimo principų, jų kaupimo tikslingumo ir duomenų saugumo.
- 1990 m. EBPO Informacinių sistemų saugumo apsaugos gairės. Jų principai - nėra teisiškai įpareigojantys. Siūlo minimalias asmens duomenų apsaugos garantijas, kurios turėtų būti įtrauktos į nacionalinius įstatymus. Gairės taikomos kompiuterizuotoms asmens duomenų byloms tiek privačiajam, tiek ir viešajame sektoriuje. Be abejo, Valstybių narių pasirinkimu jų taikymas gali būti praplėstas ir rankiniu būdu tvarkomoms asmens duomenų byloms;
- 1995 m. **95/46/EB**; Direktyva dėl asmenų apsaugos, tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (Asmens duomenų apsaugos direktyva). Priėmus šį teisės aktą Europos Sąjungos lygmenyje, kiekviena šalis-narė turi užtikrinti, kad jos nuostatos bus efektyviai pritaikytos jų teisės sistemai. (nacionalinei teisės aktų bazei). Direktyvos 17 straipsnyje išdėstomi pagrindiniai reikalavimai asmens duomenų tvarkymo Valstybės narės turi numatyti, „kad duomenų valdytojas privalo įgyvendinti tinkamas technines ir organizacines priemones, skirtas apsaugoti, kad asmens duomenys nebūtų netyčia ar neteisėtai sunaikinti ar netyčia prarasti, pakeisti, neleistinai atskleisti ar palikti prieinami, ypač, kai tvarkomus duomenis tenka perduoti tinklu, taip pat apsaugoti nuo bet kokių kitų neteisėtų tvarkymo būdų;
- 1995 m. buvo priimta Europolo konvencija. Vykdydamas savo misiją Europolas valdo kompiuterizuotą informacijos sistemą. Ją sudaro: informacinė sistema ir analizei skirtos bylos. Europolas savo užduotims, numatytoms Konvencijoje atlikti naudoti gali tik valstybių narių

[8] Convention for the protection of individuals with regard to automatic processing of personal data (ETS Np. 108), http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm; prisijungimo laikas: 2005-03-19.

[9] Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108) su Europos Tarybos Ministrų Komiteto priimtomis pataisomis//Valstybės Žinios, 2001, Nr.: 32-1059.

kompetentingos institucijos, kad užkirstų kelią ir kovotų su nusikaltimais, priskiriamais Europolo kompetencijai.

• 1997 m. 97/66/EB; Direktyva reglamentuojanti privatumo apsaugą telekomunikacijų srityje. Direktyva numato, kad šalys-narės privalo užtikrinti komunikacijų konfidencialumą nacionalinėmis teisinėmis priemonėmis.

• 2000 m. ES Pagrindinių teisių chartija Chartijos 8 str. formuojamas asmens duomenų apsaugos reikalavimas ir nustatoma, kad kiekvienas turi teisę į savo asmens duomenų apsaugą.

• 2002 m **2002/58/EB** dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje. Šios direktyvos ketvirtame straipsnyje „Saugumas" apibrėžiami du pagrindiniai reikalavimai informacijos saugumui. Tai, kad „viešai prieinamų elektroninių ryšių paslaugų teikėjas turi imtis tinkamų techninių ir organizacinių priemonių, kad užtikrintų savo paslaugų saugumą, o tam tikrais atvejais tokių priemonių imasi kartu su viešųjų ryšių tinklo teikėju, kad užtikrintų ir paties tinklo saugumą. Ši direktyva pakeitė iki tol galiojusią direktyvą Nr. 97/66/EB[10] dėl asmens duomenų tvarkymo ir privatumo apsaugos telekomunikacijų sektoriuje.

Pagrindiniai nacionaliniai teisės aktai, susiję su asmens duomenų apsauga

• LR Konstitucija, kurioje privatumo teisę kiekvienam LR piliečiui garantuoja 22 straipsnio[11] nuostatos, kurios skelbia:

- Žmogaus privatus gyvenimas neliečiamas.
- Asmens susirašinėjimas, pokalbiai telefonu, telegrafo pranešimai ir kitoks susižinojimas neliečiami.
- Informacija apie privatų asmens gyvenimą gali būti renkama tik motyvuotu teismo sprendimu ir tik pagal įstatymą.
- Įstatymas ir teismas saugo, kad niekas nepatirtų savavališko ar neteisėto kišimosi į jo asmeninį ir šeimyninį gyvenimą, kėsinimosi į jo garbę ir orumą.

• 1996 metų Lietuvoje priimamas ADTAĮ įstatymas, o 2003 m. nauja įstatymo redakcija. Įstatymas suderintas su Europos Sąjungos direktyva 95/46/EB, ir „reglamentuoja santykius, kurie atsiranda tvarkant asmens duomenis automatiniu būdu, taip pat neautomatiniu būdu, tvarkant asmens duomenų susistemintas rinkmenas. Įstatymas nustato fizinių asmenų kaip duomenų subjektų teises, šių teisių apsaugos tvarką, juridinių ir fizinių asmenų teises, pareigas ir atsakomybę tvarkant asmens duomenis".

• Lietuvos Respublikos 1997m Vyriausybės nutarimas Nr. 952 „Dėl duomenų saugos valstybės ir

[10] Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, OJ L 24/1, 30/01/1998.
[11] Lietuvos Respublikos Konstitucija// Valstybės žinios. 1992, Nr. 33-1014.

savivaldybių informacinėse sistemose

- 2002 m. Lietuvos Respublikos Operatyvinės veiklos įstatymas Nr. 65-2633.
- Lietuvos Respublikos Vyriausybės 1997 m. rugsėjo 04 d. nutarimas Nr. 952 Dėl duomenų apsaugos valstybės ir vietos savivaldos informacinėse sistemose;
- 2001 m. Lietuvos Respublika ratifikavo Konvenciją dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108) su Europos Tarybos Ministrų Komiteto priimtomis pataisomis[12].
- 2002 m. Lietuvos Respublikos Vyriausybė patvirtino Elektroninės valdžios koncepciją[13]. Koncepcijos skyriuje „Informacijos saugumas ir vartotojų tapatybės nustatymas" sakoma, kad „e. valdžios projektai galės funkcionuoti, kai bus užtikrinta informacinių technologijų ir telekomunikacijų sauga, gyventojų interesų teisinė apsauga valstybės informacinėse sistemose"[14].
- 2001 m. Lietuvos Respublikos Vyriausybės nutarime „Dėl informacijos technologijų saugos valstybinės strategijos ir jos įgyvendinimo plano patvirtinimo[15] pateikiami pagrindiniai informacijos technologijų saugos valstybinės strategijos tikslai. Vienas iš tokių tikslų - plėtoti informacinių technologijų saugos teisinį reglamentavimą ir nustatyti e. verslo, kompiuterių tinklų, interneto tarnybinių stočių bei kitus saugumo reikalavimus.
- 2003 m. Lietuvos Respublikos Vyriausybės nutarimu „Dėl duomenų saugos valstybės ir vietos savivaldos informacinėse sistemose"[16] buvo patvirtinti bendrieji duomenų saugos reikalavimai, kurių pagrindinis tikslas sudaryti sąlygas saugiai tvarkyti automatizuotu būdu duomenis valstybės registruose ir kitose valstybės informacinėse sistemose.
- Teisę į privataus gyvenimo apsaugą ir jos gynimą reglamentuoja LR Civilinis Kodeksas kurio, 2.22 straipsnis reglamentuoja „Teise į atvaizdą", o 2.23 straipsnyje "Teisė į privatų gyvenimą ir jo slaptumą".
- 2004 m. balandžio 19 d. Lietuvos Respublikos Vyriausybės priėmė nutarimą Nr. 451 „Dėl valstybės informacinių sistemų steigimo ir įteisinimo taisyklių patvirtinimo"[17], kuriuo patvirtinamos valstybės informacinių sistemų steigimo ir taisyklės. Šių taisyklių 6 punktas nurodo, kad „Informacinės sistemos steigėjas, teikdamas derinti informacinės sistemos nuostatų projektą Vidaus

[12] Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108) su Europos Tarybos Ministrų Komiteto priimtomis pataisomis//Valstybės Žinios, 2001, Nr. 32-1059.
[13] Elektroninės valdžios koncepcija//Valstybės žinios, 2003, Nr. 2-54.
[14] Ten pat.
[15] Dėl informacijos technologijų saugos valstybinės strategijos ir jos įgyvendinimo plano patvirtinimo//Valstybės Žinios, 2001, Nr. 110-4006.
[16] Dėl duomenų saugos valstybės ir vietos savivaldos informacinėse sistemose//Valstybės Žinios, 1997, Nr. 83-2075; Valstybės Žinios, 2003, Nr. 2-45
[17] Dėl Valstybės informacinių sistemų steigimo ir įteisinimo taisyklių patvirtinimo//Valstybės Žinios, 2004, Nr. 58-2061.

reikalų ministerijai, kartu turi pridėti informacinės sistemos duomenų saugos nuostatus, parengtus vadovaujantis Tipiniais duomenų saugos nuostatais[18].“

- Lietuvos Respublikos Vyriausybės 2000 m. kovo 27 d. nutarimas Nr. 349 Dėl Asmens duomenų valdytojų valstybės registro įsteigimo ir šio registro nuostatų patvirtinimo;

Be aukščiau paminėtu teisės aktų Vidaus reikalų ministras savo įsakymais patvirtino visą eilę rekomendacijų ir nuostatų bei taisyklių. Reikėtų paminėti informacijos klasifikavimo pagal duomenų grupes rekomendaciją[19], Tipinius duomenų saugos nuostatus[20], Informacinių technologijų saugos atitikties vertinimo metodiką[21].

1.3. Duomenų valdytojai policijos įstaigose

Lietuvoje formuojasi valstybinis požiūris apie tai, kad asmens duomenų saugumas yra ne tik duomenų subjekto ar duomenų valdytojo problema. Siekiant užtikrinti veiksmingą duomenų apsaugą, didelis vaidmuo tenka priežiūros institucijai – Valstybinei duomenų apsaugos inspekcijai, kuri šioje srityje teikia rekomendacijas, registruoja duomenų valdytojus.

Duomenų valdytojas yra fiziniai arba juridiniai asmenys, tiek privačiame, tiek valstybiniame sektoriuje ar policijos įstaigose (gydytojas yra savo klientų duomenų valdytojas; įmonė yra savo klientų ir darbuotojų duomenų valdytoja; sporto klubas valdo savo narių duomenis, o viešoji biblioteka – skaitytojų).

Duomenų valdytojas - juridinis ar fizinis asmuo, kuris vienas arba drauge su kitais nustato asmens duomenų tvarkymo tikslus ir priemones. Jeigu duomenų tvarkymo tikslus nustato įstatymai ar kiti teisės aktai, tai duomenų valdytojas ir (ar) jo skyrimo tvarka gali būti nustatyti tuose įstatymuose ar kituose teisės aktuose[22].

Pagal Direktyvos 95/46/EB 2 straipsnio d) punktą, asmens duomenų valdytojas reiškia tokį fizinį ar juridinį asmenį, valstybės valdžios instituciją, agentūrą ar bet kurį kitą organą, kuris vienas ar drauge su kitais nustato asmens duomenų tvarkymo tikslus ir būdus. Taigi, apibrėžimas akcentuoja keturis momentus. Pirma, jis numato galimybę, kad vienos asmens duomenų tvarkymo operacijos metu gali dalyvauti daugiau nei vienas asmens duomenų valdytojas. Antra, asmens duomenų valdytojas pats nebūtinai turi turėti, valdyti asmens duomenis. Trečia, kintant duomenų tvarkymo operacijoms, gali kisti pati duomenų valdytojo samprata. Ketvirta, apsprendžiantysis faktorius, tam

[18] Dėl Tipinių duomenų saugos nuostatų patvirtinimo//Valstybės Žinios, 2003, Nr. 76 – 3511.
[19] Dėl Informacijos klasifikavimo pagal duomenų grupes rekomendacijų patvirtinimo//Valstybės Žinios, 2003, Nr. 77-3541.
[20] Dėl Tipinių duomenų saugos nuostatų patvirtinimo//Valstybės Žinios, 2003, Nr. 76-3511.
[21] Dėl Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo//Valstybės Žinios, 2004, Nr. 80-2855.
[22] Asmens duomenų teisinės apsaugos įstatymo 2 straipsnio 7d. Žin., 1996,Nr.63-1479

tiktą subjektą pripažįstant duomenų valdytoju, yra ne formalus duomenų tvarkymo operacijų kontrolės atsakomybės paskirstymas, bet faktinis tos kontrolės vykdymas.

Duomenų **tvarkytojas** - juridinis ar fizinis (kuris nėra duomenų valdytojo darbuotojas) asmuo, duomenų valdytojo įgaliotas tvarkyti asmens duomenis.

Duomenų valdytojas, tvarkydamas asmens duomenis automatiniu būdu arba tvarkydamas susistemintas duomenų rinkmenas, prisiima ir tam tikrus įsipareigojimus. Jis privalo užtikrinti asmens duomenų apsaugą.

Asmens duomenis tvarkyti automatiniu būdu galima tik Vyriausybės nustatyta tvarka pranešus Valstybinei duomenų apsaugos inspekcijai, išskyrus tam tikras išimtis. Vadovaudamiesi ADTAĮ įstatymo[23] 25 straipsniu ir LR Vyriausybės[24] nutarimu asmens duomenų valdytojai privalo pranešti, kad bus tvarkomi asmens duomenis. Duomenų valdytojai neprivalo pranešti Valstybinei duomenų apsaugos inspekcijai apie duomenų tvarkymą automatiniu būdu, kai:

- asmens duomenys tvarkomi vidaus administravimo tikslais, t.y. veikloje, kuria užtikrinamas duomenų valdytojo savarankiškas funkcionavimas (struktūros tvarkymas, personalo valdymas, turimų materialinių ir finansinių išteklių valdymas, raštvedybos tvarkymas);
- politiniais filosofiniais, religiniais ar su profesinėmis sąjungomis susijusiais tikslais, jei asmens duomenis tvarko savo veikloje fondas, asociacija ar kita ne pelno organizacija, kai tvarkomi asmens duomenys yra susiję tiktai su šios organizacijos nariais arba su asmenimis, kurie nuolat kitaip dalyvauja jos veikloje dėl šios organizacijos siekiamų tikslų;
- asmens duomenys tvarkomi visuomenės informavimo priemonėse žurnalistikos, meninės ir literatūrinės raiškos bei kitais tikslais;
- asmens duomenys tvarkomi sveikatos apsaugos tikslais;
- asmens tvarkomi Valstybės ir tarnybos paslapčių įstatymo nustatyta tvarka.

Pranešimą apie asmens duomenų tvarkymą Valstybinei duomenų apsaugos inspekcijai teikia[25]: Duomenų valdytojai LR ADTAĮ nustatytais atvejais; Politinės partijos, rinkimų įstatymo nustatytais atvejais; telekomunikacijų operatoriai ir paslaugų teikėjai , kiti duomenų valdytojai įstatymų nustatytais atvejais.

Valstybės registrui turi būti pateikti duomenys, išvardinti Asmens duomenų valdytojų pranešimo apie duomenų tvarkymą tvarkos 3 punkte[26]:

---

[23] Asmens duomenų teisinės apsaugos įstatymas //Žin., 1996, Nr. 63-1479; 2003, Nr.15-597

[24] LR Vyriausybės 2002 m. vasario 20 d. nutarimas Nr. 262 (Žin., 2002, Nr. 20-768)

[25] LR Vyriausybės 2002 m. vasario 20 d. nutarimu Nr. 262 (Žin., 2002, Nr. 20-768; 2003, Nr. 57-2548) patvirtintos Asmens duomenų valdytojų pranešimo apie duomenų tvarkymą tvarkos 2 punktą

[26] LR Vyriausybės 2002 m. vasario 20 d. nutarimas Nr. 262

- duomenų valdytojo pavadinimas, juridinio asmens kodas ir duomenų tvarkymo vieta;
- asmens duomenų tvarkymo tikslai;
- duomenų subjekto grupė ar grupės, atskiriamos pagal joms būdingą požymį ir su jomis susijusių asmens duomenų sąrašas.
- asmens duomenų šaltiniai;
- gavėjai arba gavėjų grupės, kuriems gali būti teikiami duomenys;
- duomenų teikimas į užsienio valstybes (teikimo tikslas, teikiamų duomenų sąrašas, valstybė);
- duomenų saugojimo terminas;
- asmens, atsakingo už duomenų apsaugą, duomenys;
- duomenų tvarkytojų ir jų atstovų, jeigu tokie yra, sąrašas.

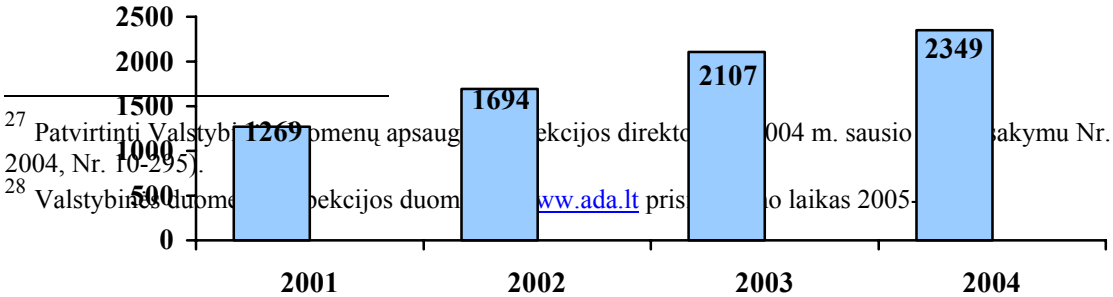
Prie pranešimo pridedami užpildyti duomenų valdytojo ir kiekvieno duomenų tvarkytojo duomenų apsaugos priemonių aprašai pagal VDAI nustatytus reikalavimus[27]. Asmens duomenų valdytojų valstybės registras ir jo informacinė paieškos sistema veikia VDAI interneto svetainėje www.ada.lt ir yra prieinama visiems vartotojams – tiek duomenų subjektams, norintiems sužinoti apie duomenų tvarkymo vietas, tiek duomenų valdytojams, norintiems pranešti apie asmens duomenų tvarkymą ar patikslinti pateiktus registravimo duomenis, tiek kiekvienam norinčiam susipažinti su registru. Šiuo metu Valstybinės duomenų apsaugos inspekcijos asmens duomenų valdytojų registruose yra įrašai apie 2739 duomenų valdytojus.[28]

1.1 lentelė Registruojami duomenų valdytojai Lietuvoje

Duomenų valdytojų registravimo statistika	
Įregistruota	*2439*
Išregistruota	*880*
Patikslinti registravimo duomenys	*302*

Kiekvienais metais Valstybinėje duomenų apsaugos inspekcijoje registruojamų duomenų valdytojų skaičius didėja tai galima pamatyti žemiau pateiktoje antroje lentelėje**.**

1.2 lentelė Įregistruotų duomenų valdytojų dinamika 2001-2004 metais



[27] Patvirtinti Valstybi omenų apsaug ekcijos direkto 004 m. sausio akymu Nr. 1T-7 (Žin., 2004, Nr. 10-295).

[28] Valstybinės duome pekcijos duom ww.ada.lt pris o laikas 2005-

Duomenų valdytojas gali rinkti duomenis tiesiogiai iš duomenų subjekto arba gali rinkti duomenis iš kitų asmenų. Kai duomenys renkami tiesiogiai iš duomenų subjektų, duomenų valdytojas privalo suteikti VDAI šią informaciją (išskyrus atvejus, kai duomenų subjektas tokią informaciją jau turi). Jeigu duomenų valdytojas renka duomenis ne tiesiogiai iš duomenų subjektų, o iš kitų asmenų, jis privalo apie tai informuoti duomenų subjektą pradėdamas tvarkyti asmens duomenis arba, jei ketina duomenis teikti tretiesiems asmenims, privalo apie tai informuoti ne vėliau kaip iki to momento, kai duomenys teikiami pirmą kartą, išskyrus atvejus, kai įstatymai ar kiti teisės aktai apibrėžia tokių duomenų rinkimo ir teikimo tvarką bei duomenų gavėjus. Kai duomenų valdytojas renka ar ketina rinkti asmens duomenis iš duomenų subjektų, ir juos tvarko ar ketina tvarkyti tiesioginės rinkodaros tikslais, prieš teikdamas mūsų duomenis, jis privalo informuoti mus, kam ir kokiais tikslais mūsų asmens duomenys bus teikiami. Duomenų valdytojai mūsų duomenis gali saugoti ne ilgiau, nei to reikalauja duomenų tvarkymo tikslai. Kai asmens duomenys nebereikalingi jų tvarkymo tikslams, jie turi būti sunaikinami, išskyrus tuos, kurie įstatymų nustatytais atvejais turi būti perduoti valstybiniams archyvams.

Dabar apžvelgsim kokius duomenis yra pateikusios policijos įstaigos Valstybinei duomenų apsaugos inspekcijai[29]

1.3 lentelė. Registruoti duomenų valdytojai Lietuvos policijoje

Pavadinimas	Adresas	Kodas	Įregistravimo data
ANYKŠČIŲ RAJONO POLICIJOS KOMISARIATAS	J.Biliūno g. 17, Anykščiai	P3180	2005-03-31
KLAIPĖDOS MIESTO VYRIAUSIASIS POLICIJOS KOMISARIATAS	Jūros g. 1, Klaipėda	P2580	2003-07-10
KUPIŠKIO RAJONO POLICIJOS KOMISARIATAS	Gedimino pr. 54, Kupiškis	P2717	2003-12-10
LIETUVOS RESPUBLIKOS VIDAUS REIKALŲ MINISTERIJA	Šventaragio g. 2, Vilnius	P25	1998-08-18
POLICIJOS DEPARTAMENTAS PRIE LR VIDAUS REIKALŲ MINISTERIJOS	Saltoniškių 19,Vilnius	P2519	2003-06-09
ŠIAULIŲ MIESTO VYRIAUSIASIS POLICIJOS KOMISARIATAS	Aušros al. 19, Šiauliai	P2725	2003-12-17
VALSTYBĖS TARNYBOS DEPARTAMENTAS PRIE VIDAUS REIKALŲ MINISTERIJOS	Šventaragio g. 2, Vilnius	P2556	2003-07-01
VILNIAUS MIESTO VYRIAUSIASIS POLICIJOS KOMISARIATAS	Mindaugo g. 14, LT-2006 Vilnius	P2399	2003-03-31

Iš pateiktos lentelės matoma, kad Valstybinai duomenų apsaugos inspekcijai yra pateikę tik 8 asmens duomenų valdytojai, tačiau kaip žinoma policijos įstaigų Lietuvoje yra žymiai daugiau, todėl šioje srityje policijos įstaigos nepakankamai rimtai atsižvelgia į būtinybę registruoti tvarkomus duomenis.

[29] 2005-11-04 duomenys

Žemiau pateiktos lentelės apie registruotą asmens duomenų valdytoją Vilniaus miesto Vyriausiąjį policijos komisariatą. Matome, kad sostinės policijos įstaiga tvarko asmens duomenis ir yra įregistravusi kaip duomenų valdytoja.

1.4 lentelė. Vilniaus m. policijos pateikti valdytojo duomenys Valstybinei duomenų apsaugos inspekcijai dėl CCTV vaizdo kamerų naudojimo

Tikslas	Viešosios tvarkos apsauga ir nusikaltimų prevencija (vaizdo stebėjimas)
Duomenų gavimo būdas	Duomenys gaunami automatiniu būdu
Gavėjų grupės	Operatyvinės veiklos subjektai
Subjektų grupės	Senamiesčio gyventojai bei praeiviai, patekę į vaizdo stebėjimo kameros aplinką
Asmens duomenų šaltinai	Vaizdo stebėjimo kameros (viso 78)
Saugojimo terminas	14 kalendorinių dienų,

1.5 lentelė. Vilniaus m. policijos pateikti valdytojo duomenys VDAI dėl asmenų identifikavimo užfiksavus juos greičio matuokliais

Tikslas	Transporto priemonių ir jas vairuojančių asmenų, kurie pažeidžia nustatytą tvarką, už kurią įstatymas numato administracinę atsakomybę, identifikavimas. Asmenų, pažeidusių Kelių eismo taisyklių reikalavimus, vairuojant transporto priemones įvykdytus pažeidimus, susisteminimas
Duomenų gavimo būdas	Duomenys gaunami automatiniu būdu
Gavėjų grupės	Operatyvinės veiklos subjektai
Subjektų grupės	Vairuotojai, pažeidę Kelių eismo taisykles (viršiję nustatytą leistiną greitį)
Fiksuojami duomenys	Asmens kodas, gyvenamoji vieta (adresas), pavardė vardas transporto priemonę vairavęs asmuo, vairuotojo nuotrauka, transporto priemonės valstybinis numeris, savininkas
Asmens duomenų šaltinai	Vaizdo stebėjimo kameros (viso 78)
Saugojimo terminas	5 metai
Asmens duomenų šaltiniai	Duomenys gaunami iš juridinio asmens: UAB „VILDOMA“ (duomenų perdavimo įrangos pagalba teikia stacionarias greičio matavimo prietaisais užfiksuotas nuotraukas)
Duomenų valdytojo atstovai	Vilniaus m. Vyriausiojo policijos komisariato Viešosios policijos Eismo priežiūros tarnyba Giraitės g. 3, Vilnius

Išanalizavus kitų policijos įstaigų asmens duomenų tvarkytojus matoma, kad ne visos policijos įstaigos vienodai tieka informaciją VDAI apie tvarkomus asmens duomenis (nesuvienodintas asmens valdytojų registravimas policijos įstaigose), be to dalis duomenų valdytojų pateiktoje paraiškoje[30] vieną iš tvarkymo tikslų įvardinta kaip: Viešosios policijos patrulių rinktinės darbo rezultatų apskaita, viešosios policijos nuovadų darbo apskaita, kitų Šiaulių miesto VPK policijos

[30] Šiaulių miesto Vyriausiojo policijos komisariato duomenys

padalinių darbo apskaita, o tai neprivalomas registruoti asmens duomenų registras, nes jis patenka po išimtimis[31].

Vadovaudamasi Direktyva 95/46/EB bei direktyvos 27 straipsniu[32] Valstybinė asmens duomenų apsaugos inspekcija 2003-05-12 išleido rekomendaciją[33] duomenų valdytojams dėl asmens duomenų tvarkymo etikos kodeksų rengimo kurio tikslas – padėti duomenų valdytojams ir duomenų tvarkytojams tinkamai įgyvendinti ADTAĮ ir kitų teisės aktų, reglamentuojančių duomenų apsaugą, nuostatas. Etikos kodeksai yra rengiami savanoriškai, apsiribojant asmens duomenų tvarkymu konkrečiame sektoriuje ar konkrečiu tikslu. Jie turėtų padėti tvarkantiems asmens duomenis geriau suprasti ir įgyvendinti ADTAĮ nuostatas. Kodeksas taikomas duomenų valdytojui (tvarkytojui), taip pat jų darbuotojams, tvarkantiems asmens duomenis, nepriklausomai nuo jų priėmimo į darbą sąlygų. Duomenų valdytojas privalo nustatyti tinkamas organizacines priemones ir užtikrinti, kad jo duomenų tvarkytojai tvarkydami asmens duomenis pagal duomenų valdytojo suteiktus įgaliojimus, laikytųsi taisyklių ir nuolat kelti duomenų apsaugos lygį. Direktyva taip pat įsakmiai reikalauja, kad duomenų valdytojas įgyvendintų tinkamas technines ir organizacines priemones, skirtas apsaugoti, kad asmens duomenys nebūtų netyčia ar neteisėtai sunaikinti ar netyčia prarasti, pakeisti, neleistinai atskleisti ar palikti prieinami ir apsaugotų nuo bet kokių kitų neteisėtų tvarkymo būdų. Itin svarbu tai, kad atsižvelgus į technologijų lygį ir jų įdiegimo išlaidas, minėtos priemonės turi užtikrinti tokį saugumo lygį, kuris atitiktų duomenų tvarkymo keliamą riziką ir saugotinų duomenų pobūdį.

Vidaus reikalų ministerija kaip informacinių duomenų bazių valdytoja teikia asmens duomenis (sudaro galimybę prisijungti prie centrinio duomenų banko) duomenų gavėjams (vidaus reikalų sistemoje esančioms policijos įstaigoms) Tačiau esti ir nemažai spragų[34]. ADTAĮ nustato pareigą duomenų valdytojui įgyvendinti tinkamas organizacines priemones, skirtas asmens duomenims nuo kokio nors neteisėto tvarkymo apsaugoti. VRM informacinėje sutemoje dažnai nefiksuojamas duomenų naudojimo tikslas ir nėra sukurta tinkama vidinė asmens duomenų naudojimo priežiūros sistema. Vidaus reikalų ministras įsakymu 1999 metais nustatė reikalavimus, kurių privalo laikytis centrinio duomenų banko duomenų naudotojai bei nurodė, kad šių

---

[31] Duomenų valdytojai neprivalo pranešti Valstybinei duomenų apsaugos inspekcijai apie duomenų tvarkymą automatiniu būdu, kai: asmens duomenys tvarkomi vidaus administravimo tikslais, t.y. veikloje, kuria užtikrinamas duomenų valdytojo savarankiškas funkcionavimas (struktūros tvarkymas, personalo valdymas, turimų materialinių ir finansinių išteklių valdymas ir naudojimas, raštvedybos tvarkymas).

[32] Straipsnis kuris numato, kad valstybė skatina duomenų valdytojus rengti etikos kodeksus

[33] Pranešimas spaudai dėl asmens duomenų tvarkymo etikos kodekso 2003-06-19 d. Nr.2R-1830 www.ada.lt prisijungimo laikas 2005-10-15

[34] Duomenų subjektas žino, kad jo gyvenamosios vietos deklaravimo duomenis tvarko VRM. Apie tai, kad VRM informacinėje sistemoje tvarkomi ir kiti asmens duomenys, duomenų subjektas nėra informuojamas, tuo pažeidžiant Asmens duomenų teisinės apsaugos įstatymą.

reikalavimų vykdymą užtikrina vietinių kompiuterių tinklų administratoriai, VRM ir jos struktūrinių padalinių vadovai bei kontroliuoja Informatikos ir ryšių departamentas. Nėra paskirstytos nurodytų reikalavimų vykdymą užtikrinančių ir kontroliuojančių asmenų funkcijos. Be to, už asmens duomenų apsaugą atsakinguoju yra paskirtas ne duomenų valdytojo (VRM), o duomenų tvarkytojo (Informatikos ir ryšių departamento) atstovas. Manytina, kad dėl šių aplinkybių išauga neteisėtos asmens duomenų peržiūros ir kitokio naudojimo tikimybė, netinkamai įgyvendinant organizacines priemones ir pažeidžiant ADTAĮ.

2. ASMENS DUOMENŲ TVARKYMAS IR POLICIJOS INFORMACINĖS SISTEMOS

2.1. Duomenų tvarkymo principai

Direktyvoje 95/46/EB "**asmens duomenų tvarkymas**" reiškia bet kurią operaciją ar operacijų rinkinį, automatiniais arba neautomatiniais būdais atliekamus su asmens duomenimis, kaip: rinkimas, užrašymas, rūšiavimas, saugojimas, adaptavimas ar keitimas, atgaminimas, paieška, naudojimas, atskleidimas perduodant, platinant ar kitu būdu padarant juos prieinamus, išdėstymas reikiama tvarka ar sujungimas derinant, blokavimas, trynimas ar naikinimas.

ADTAĮ numatyta, kad „duomenų tvarkymas – bet kuris su asmens duomenimis atliekamas veiksmas: rinkimas, užrašymas, kaupimas, saugojimas, klasifikavimas, grupavimas, jungimas, keitimas, papildymas ar taisymas, teikimas, paskelbimas, naudojimas, loginės, aritmetinės operacijos, paieška, skleidimas, naikinimas ar kitoks veiksmas arba veiksmų rinkinys.“[35]

Vadovaujantis abiem šiais teisės aktais, matome, kad tai bet kokia su duomenimis atliekama operacija. Ji apima:

- duomenų gavimas, užrašymas ar saugojimas;
- duomenų rinkimas, rūšiavimas, saugojimas, keitimas ar adaptavimas;
- duomenų paieška ar naudojimas;
- duomenų atskleidimas perduodant, skleidžiant, publikuojant ar kitais būdais darant juos prieinamus;
- duomenų išdėstymas reikiama tvarka ar sujungimą derinant, blokavimas, trynimas ar naikinimas.

Taigi sąvoka „**duomenų tvarkymas**“ yra labai plati ir nepriklauso nuo naudojamų metodų. Kiekviena tvarkymo operacija turi būti teisėtai grindžiama arba ADTAĮ, arba kito įstatymo nuostata. Asmens duomenys, surinkti kitais tikslais, gali būti tvarkomi statistikos, istoriniais ar

[35] Įstatymo 2 straipsnio 4 dalis

mokslinio tyrimo tikslais tik įstatymų nustatytais atvejais, kai įstatymuose nustatytos tinkamos duomenų apsaugos priemonės.[36]

Tvarkyti duomenis leidžiama, jei yra išpildytos šios sąlygos:

- duomenų subjektas po to, kai buvo atitinkamai informuotas, nedviprasmiškai pareiškė savo sutikimą;
- duomenų tvarkymas yra būtinas sutarčių, kuriose viena iš šalių yra duomenų subjektas, įgyvendinimui arba sutarčių, kurių iniciatorius buvo duomenų subjektas, pasirašymui;
- duomenų tvarkymas yra privalomas pagal įstatymus;
- duomenų tvarkymas yra būtinas siekiant apginti esminius duomenų subjektų interesus;
- duomenų tvarkymas yra būtinas atliekant visuomenės interesus tenkinančias užduotis, arba kai šias užduotis atlieka valstybinės institucijos (pvz., policija ir pan.);
- duomenys gali būti tvarkomi, jei duomenų valdytojas ar trečioji šalis turi teisėtus interesus tai daryti. Tačiau duomenų valdytojo interesai negali būti aukštesni už duomenų subjekto interesus ar jo pagrindines teises, ypač jei tai susiję su asmens teise į privatumą. Praktikoje ši nuostata reikalauja pagrįsto duomenų valdytojų verslo interesų ir teisės į asmenų privatumą subalansavimo.[37]

Direktyvos 95/46/EB 6 straipsnis įtvirtindamas duomenų kokybės principą, nustato sąlygas, kuriomis esant gali būti tvarkomi asmens duomenys tarp jų ir policijos informacinėse sistemose. Vienas pagrindinių reikalavimų yra tas, kad surinkti duomenys turi būti tvarkomi teisingai ir teisėtai[38].

Teisingas duomenų tvarkymas suponuoja, jog turi būti išlaikytas kuo didesnis atvirumo laipsnis. Asmens duomenys negali būti renkami, kaupiami ar bent kaip tvarkomi užslėptais, slaptais, neatskleistais tikslais. Direktyvos 6 straipsnio 1 dalie (b) punktas aiškiai numato, kad duomenys turi būti surinkti įvardintais, aiškiai apibrėžtais ir teisėtais tikslais, o po to tvarkomi su šiais tikslais suderintais būdais. Direktyvos tikslas – pagrindinių žmogaus teisių ir laisvių apsauga bei gynyba[39], suponuoja, kad tikslas, kuriam yra tvarkomi asmens duomenys, turi būti suderinamas su tokiomis fundamentaliomis žmogaus teisėmis ir laisvėmis, o nuo jų nukrypta gali būti tik išskirtiniais - teisės sankcionuotais atvejais.

ADTAĮ 2 dalies 6 punkte numatyta, kad draudžiama tvarkyti ypatingus asmens duomenis, išskyrus atvejus, kai įstatymų nustatytais atvejais būtina užkirsti kelią nusikalstamoms ar kitoms neteisėtoms veikoms arba būtina jas tirti.[40] Ši nuostata leidžia tvarkyti ypatingus duomenis, kai

---

[36] Direktyva 95/46/EB
[37] Direktyvos 95/46/EB 7 str.
[38] Direktyvos 95/46/EB 6 straipsnio 1 dalies a) punktas
[39] Šis uždavinys įtvirtintas Direktyvos 1 straipsnio 1 dalyje
[40] Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas // Valstybės žinios. 1996, Nr. 63-1479.

įstatymų nustatytais atvejais būtina užkirsti kelią nusikalstamoms ar kitoms neteisėtoms veikoms arba būtina jas tirti. Jos atitikmenį sunku surasti direktyvoje, tačiau ji atitinka direktyvos nuostatas, kurios reglamentuoja valstybės valdžios institucijų atliekamą duomenų tvarkymą teisėsaugos tikslais. Direktyva nereglamentuoja šios srities, kadangi ES nėra kompetentinga priimti direktyvų teisingumo ir vidaus reikalų srityje, kuri apima baudžiamosios teisės pažeidimų prevenciją ir tyrimą. Vis dėlto ADTAĮ apima šią veiklą, nes jai nėra taikoma 1 straipsnio nustatyta išimtis. Dėl šių priežasčių leidimas tvarkyti ypatingus duomenis yra padidintas, nes priešingu atveju teisėsaugos institucijoms ir policijos tikslais[41] būtų sunku imtis atitinkamų veiksmų.

Siekiant suderinti policijos sektoriaus poreikius su direktyvoje numatyta duomenų subjektų teise į privatumą, Prancūzijos duomenų apsaugos įstatymas numato tris ypatingų duomenų tvarkymo draudimo išimtis policijos sektoriui. Ypatingų duomenų rinkimas ir tvarkymas rinkmenose (automatiniu ar rankiniu būdu) policijos sektoriuje yra pateisinamas „visuomenės interesu" siekiant:

- užkirsti kelią nusikaltimams,
- atliekant nusikaltimų tyrimus;
- užtikrinti saugumą.

Prancūzijos duomenų apsaugos įstatymas garantuoja, kad teismų ir teisėsaugos institucijų (turinčių nusikaltimų tyrimo galią) renkami ir tvarkomi duomenys, siekiant atlikti institucijų teisinę pareigą, yra ribojami. Prancūzijos įstatymų leidėjai, suvokdami ypatingųjų duomenų svarbą, nesuteikė teisės tvarkyti tuos duomenis jokiai kitai institucijai. Todėl Prancūzijos Teisingumo departamentas yra atsakingas už „nacionalinį nuteistų asmenų registrą".

Papildomai be tam tikro tikslo egzistavimo, turo būti įgyvendinta ir kita sąlyga: teisėsaugos institucijų vykdoma veikla turi būti reguliuojama įstatymais. Svarbiausias šaltinis šiuo atveju yra Baudžiamojo proceso kodeksas. Siekiant laikytis teisės principų, kėsinimosi į įtariamų asmenų pagrindines teises ir laisves galimybės turi būti nustatytos šiame ir kituose įstatymuose. Jeigu šie įstatymai suteikia įgaliojimus valstybės valdžios institucijoms imtis prevencinių ar tyrimo veiksmų dėl baudžiamosios teisės pažeidimų, tai ypatingus duomenis leidžiama tvarkyti.[42]

Bendrieji duomenų tvarkymo principai išdėstyti ADTAĮ 3 straipsnyje. Asmens duomenys turi būti:

1. Renkami apibrėžtais ir teisėtais tikslais, nustatytais prieš renkant asmens duomenis, ir paskui tvarkomi su šiais tikslais suderintais būdais. Šis principas yra vienas pagrindinių ADTAĮ

[41] Sąvoka "policijos tikslais" apima visas užduotis, kurias policijos organai privalo atlikti kriminalinių nusikaltimų prevencijos ir stabdymo bei viešosios tvarkos palaikymo tikslais.
[42] Asmens duomenų teisinės apsaugos įstatymo komentaras. Vilnius 2005

ir Direktyvos principų. Tikslai turi būti teisėti. Todėl, tikslai yra ribojami uždavinių, atitinkančių įstatymą. ADTAĮ reikalauja, kad asmens duomenys būtų renkami apibrėžtais ir teisėtais tikslais, nustatytais prieš renkant asmens duomenis, ir paskui tvarkomi su šiais tikslais suderintais būdais. Nors ADTAĮ neminimas vienas Direktyvoje nustatytas tikslo apibūdinimas, t.y. „aiškiai įvardintas“, tai neturi įtakos šio principo teisinei padėčiai, kadangi „aiškiai įvardinto“ principo reikšmė artima „apibrėžto“ principo reikšmei. Tikslai taip pat turi būti apibrėžti (ir „aiškiai įvardinti“, Direktyvos 6 str. 1 d. b) p.). Duomenų valdytojai turi nustatyti tikslą taip, kad nekiltų abejonių dėl tikslo kurio jis nori pasiekti rinkdamas ir tvarkydamas asmens duomenis. Įstatymas, o taip pat ir Direktyva, aiškiai nereikalauja tikslą nustatyti raštu. Kitas svarbus dalykas yra tai, ar visuomet yra reikalingas sutikimas, norint duomenis panaudoti kitam tikslui.

Policijos jos tikslams surinkti ir saugomi asmens duomenys turėtų būti naudojami išimtinai šiems tikslams renkami tik realaus pavojaus prevencijos arba konkretaus kriminalinio nusikaltimo sustabdymo tikslais. Bet kuri šios nuostatos išimtis turi būti taikoma vadovaujantis nacionaliniais teisės aktais. Tais atvejais, kai duomenys apie asmenį buvo surinkti ir saugomi be šio asmens žinios ir jeigu tie duomenys nebuvo ištrinti, toks asmuo, jeigu įmanoma, turėtų būti informuotas, kad apie jį yra turima informacija, iškart, kai grėsmė tik policijos veiklos objektui išnyksta. Duomenų rinkimas techninėmis stebėjimo arba kitomis automatizuotomis priemonėmis turėtų būti numatytas specialiose nuostatose ko Lietuvos teisinėje sistemoje nėra ir ta tema bus nagrinėjama 3 skyriuje.

2.Tvarkomi tiksliai, sąžiningai ir teisėtai; Lietuvos įstatymuose nėra apibrėžta, ką reiškia „sąžiningai“ ar „teisėtai“, todėl šiems žodžiams turėtų būti suteikta jų įprastinė reikšmė. Asmens duomenys, kurie tvarkomi pažeidžiant bet kurį įstatymą, teisės aktą, ar teisiškai įgyvendinamą pareiga ar apribojimą, tvarkomi neteisėtai. „Neteisėtumas“ gali atsirasti, kai veiksmas atliekamas pažeidžiant įstatymą ar sutartį. Sąžiningumas ir teisėtumas turi būti objektyviai įvertinti ir taikomi. Asmens duomenys nebus gauti sąžiningai, jei, prieš gaunant duomenis, asmuo nebuvo informuotas apie bet kokį duomenų valdytojo neakivaizdų tikslą. Nustatant, ar asmens duomenys tvarkomi sąžiningai, reikia atsižvelgti į būdą, kaip jie buvo gauti, ypač ar asmuo, iš kurio jie buvo gauti, nebuvo apgautas ar suklaidintas dėl tikslo, kuriuo jie bus tvarkomi.

3. Tikslūs ir, jei reikia dėl asmens duomenų tvarkymo, nuolat atnaujinami; netikslūs ar neišsamūs duomenys turi būti ištaisyti, papildyti, sunaikinti arba sustabdytas jų tvarkymas. Kai kuriose ES valstybėse narėse ši sąvoka yra apibrėžta. Jungtinėje Karalystėje 1998 m. Duomenų apsaugos įstatyme numatyta, kad „duomenys yra netikslūs, jeigu jie yra neteisingi ar klaidinantys ryšium su fakto klausimu”[43]. Taigi, vien tik nuomonė, kuri nėra fakto teigimas, negali būti

[43] JK Duomenų apsaugos įstatymas, 1998 m., s.70(2). Data Protection Law and Practice 702 (2003).

nuginčijama netikslumo pagrindu. Antroji dalis aiškiai reikalauja, kad duomenų valdytojas turi imtis visų pagrįstų veiksmų, kad užtikrintų, kad netikslūs ar neišsamūs duomenys būtų ištaisyti, papildyti, ištrinti, arba turi būti sustabdytas jų tolesnis tvarkymas.

4. Tapatūs, tinkami ir tik tokios apimties, kuri būtina jiems rinkti ir toliau tvarkyti; Asmens duomenys renkami ir tvarkomi, jei jie tinkami, tapatūs ir nedidesnės apimties, atsižvelgiant į nustatytus tikslus. Todėl duomenys turi būti atrenkami remiantis tikslu rinkti ir tvarkyti kiek įmanoma mažiau duomenų. Labai dažnai duomenų valdytojai surenka daugiau asmens duomenų negu reikia nustatytiems tikslams.

Valstybinė Duomenų apsaugos inspekcija (toliau –VDAI) byloje, prieš C.Zabulėnienę[44], teigė, kad SODRA (Valstybinio socialinio draudimo fondo valdyba) perdavė dalinę SODROS duomenų bazės kopiją, Vidaus reikalų ministerijai ir kitoms įstaigoms neužtikrindama, kad būtų pateiktas tik toks duomenų kiekis, kuris yra reikalingas duomenų tvarkymui, ir tokiu būdu pažeidė ketvirtąjį principą. Teismas pažymėjo, kad pateiktoje medžiagoje nebuvo informacijos, kad minėtos institucijos gavo per daug duomenų, kurie duomenų gavėjams nebuvo reikalingi. Teismas pasisakė, kad ADTAĮ reglamentuoja objektyvias pateiktų duomenų apimtis, tačiau nutyli apie pagrįstai reikalaujamos informacijos apimtį ir dydį. Todėl pats informacijos dydis, pagrįstai pateiktas tokioms institucijoms, negali būti traktuojamas kaip pažeidimas, jei tinkamai vykdomas duomenų valdytojo įsipareigojimas tinkamai įgyvendinti organizacines, techninės kontrolės ir apsaugos funkcijas.

5. Saugomi tokia forma, kad duomenų subjektų tapatybę būtų galima nustatyti ne ilgiau, negu to reikia tiems tikslams, dėl kurių šie duomenys buvo surinkti ir tvarkomi.

„Duomenų saugojimas“ (*data presevation*) turi būti atskirtas nuo „duomenų išsaugojimas" (*data retention*). Saugoti duomenis reiškia laikyti tuos duomenis, kurie jau egzistuoja laikomųjų duomenų pavidale, apsaugoti nuo visko, kas gali sąlygotų jų esamos kokybės ar būklės pasikeitimą arba pablogėjimą. Duomenų išsaugojimas yra duomenų įrašymo į atmintį procesas. Ir priešingai, duomenų saugojimas yra veikla, kuri užtikrina laikomųjų duomenų patikimumą ir saugumą.

Policijos tikslais turėtų būti saugomi tik tikslūs asmens duomenys ir tik tokie duomenys, kurie yra reikalingi policijos tarnyboms vykdyti jų įstatymų nustatytas užduotis, laikantis nacionalinės teisės normų, bei vykdyti savo įsipareigojimus, kylančius iš tarptautinės teisės normų. Policijos įstaigos turėtų imtis priemonių tam, kad asmens duomenys, saugomi policijos reikmėms, būtų ištrinti, jeigu jie daugiau nebėra reikalingi tiems tikslams, kuriems jie buvo saugomi. Šiuo tikslu, būtina itin atsižvelgti į šiuos kriterijus: būtinybę išsaugoti duomenis, atsižvelgiant į konkrečios

[44] Žr. VDAI prieš C.Zabulėnienę, 2003 m. kovo 14 d., Vilniaus m. 1-asis apylinkės teismas.

bylos tardymo išvadas, galutinį teismo sprendimą, ypatingai, išteisinimus, reabilitavimą, netekusius galios nuosprendžius, amnestijas, duomenų subjekto amžių, ypatingas duomenų kategorijas.

2.2. Informacijos poreikis policijoje

Sparčiai plečiantis informacinių sistemų kūrimo galimybėmis keičiasi daugelio žmogaus veiklos sričių darbo aplinka. Technologijų plėtra įtakoja programinės įrangos kūrimo procesams, naujų metodų paieškai, skirtai informacijai ir žinioms kaupti, skleisti, valdyti. Informacijos supratimas siejamas su veiklos kompiuterizavimo procesais, naujomis technikos rūšimis, informacijos apdorojimo saugojimo ir perdavimo technologijomis. Informacija tampa ekonominiu ištekliu.

Informacinę sistemą galime apibrėžti kaip kompleksą komponentų, skirtų įvairių rūšių duomenims ir informacijai rinkti, saugoti, apdoroti, laikyti, bei skleisti, siekiant tam tikrų organizacijos tikslų ir taikant kompiuterines technologijas.[45] Informacinė sistema suprantama, kaip informacinių technologijų ir techninės įrangos visuma.

Policijos informacinės sistemos programinis paketas sudaro galimybę automatizuotam informacijos surinkimui bei analizei, kurios pagrindu priimami teisingi ir operatyvūs valdymo organizavimo sprendimai bei teisingi ir operatyvūs sprendimai kovai su nusikalstamumu. Ši priemonė, informacinių sistemų pagalba įgyvendina racionalų informacijos srautų paskirstymą tarp informacijos šaltinių ir informacijos gavėjų. Kompiuterizuotose darbo vietose policijos pareigūnas turi gauti išsamią, operatyvią informaciją.

Išanalizavus policijos padalinių veiklą, galima išskirti tarnybų poreikį atitinkamiems duomenims:

- Policijos įstaigų vadovybė
    - Personalo duomenys,
    - Baudžiamosios statistikos duomenys,
    - Duomenys apie įvykius,
    - Duomenis apie asmenis
- Personalo tarnyba
    - Duomenys apie dirbančius pareigūnus,
    - Duomenys apie atleistus pareigūnus,
    - Duomenys apie etatus,
- Budėtojų tarnyba
    - Asmens anketiniai duomenys, asmens dokumentai,
    - Duomenys apie ATPK numatytus teisės pažeidėjus,
    - Duomenys apie ieškomus asmenis,
    - Teistumo duomenys,
    - Duomenys apie įvykius,

[45] D.Dzemydienė, R.Naujikienė. Informacinės sistemos – duomenų struktūros ir valdymas. - Vilnius: Lietuvos teisės universitetas 2004. P32.

    - Duomenys apie autotransporto priemones,
    - Duomenys apie ginklus,
- Organizacinis skyrius arba informatikos tarnyba
    - Asmens anketiniai duomenys, asmens dokumentai,
    - Duomenys apie ATPK numatytus teisės pažeidėjus,
    - Duomenys apie ieškomus asmenis,
    - Teistumo duomenys,
    - Duomenys apie įvykius,
    - Duomenys apie autotransporto priemones,
    - Duomenys apie ginklus,
    - Baudžiamųjų bylų duomenys,

  Organizuotų nusikaltimų tyrimo tarnyba

    - Asmens anketiniai duomenys, asmens dokumentai,
    - Duomenys apie ATPK numatytus teisės pažeidėjus,
    - Duomenys apie ieškomus asmenis,
    - Teistumo duomenys,
    - Duomenys apie įvykius,
    - Duomenys apie autotransporto priemones,
    - Duomenys apie ginklus,

  Kriminalinių nusikaltimų tyrimo tarnyba

    - Asmens anketiniai duomenys, asmens dokumentai,
    - Duomenys apie ATPK numatytus teisės pažeidėjus,
    - Duomenys apie ieškomus asmenis,
    - Teistumo duomenys,
    - Duomenys apie įvykius,
    - Duomenys apie autotransporto priemones,
    - Duomenys apie ginklus,

  Ekonominių nusikaltimų tyrimo tarnyba

    - Asmens anketiniai duomenys, asmens dokumentai,
    - Teistumo duomenys,
    - Duomenis apie autotransporto priemones,
    - Duomenys apie ieškomus asmenis,
    - Duomenys apie įmones,
    - Baudžiamųjų bylų duomenys,
- Kriminalinių ekspertizių skyrius
    - Duomenys apie autotransporto priemones,
    - Duomenys apie ginklus,
    - Duomenys apie įvykius,
- Eismo priežiūros padalinai (Kelių policija)
    - Asmens dokumentai,
    - Duomenys apie ATPK pažeidėjus,
    - Duomenys apie ieškomus asmenis,
    - Duomenys apie įvykius,
    - Duomenys apie autotransporto priemones,
- Leidimų skyrius
    - Asmens anketiniai duomenys,
    - Asmens dokumentai,
    - Duomenys apie ATPK pažeidėjus,
    - Teistumo duomenys,

    - Duomenys apie ginklus,
- Finansų tarnyba
    - Duomenys apie dirbančius pareigūnus,
    - Duomenys apie etatus,
    - Duomenys apie atlyginimus
    - Duomenys apie išmokas
- Migracijos tarnyba
    - Asmens anketiniai duomenys,
    - Asmens dokumentai,
    - Duomenys apie ATPK numatytus teisės pažeidėjus,
    - Teistumo duomenys,
    - Nepageidaujami asmenys,
- Nepilnamečių reikalų inspekcija
    - Asmens anketiniai duomenys,
    - Asmens dokumentai,
- Viešoji policija
    - Asmens anketiniai duomenys,
    - Asmens dokumentai,
    - Duomenys apie ATPK numatytus teisės pažeidėjus,
    - Duomenys apie ieškomus asmenis,
    - Teistumo duomenys,
    - Duomenys apie įvykius,
    - Duomenys apie autotransporto priemones,
    - Duomenys apie ginklus.

2.3. Policijos programinis paketas ir jame tvarkomi asmens duomenys

Šiuo metu Vidaus reikalų informacinės sistemos centrinio duomenų banko (toliau -VRIS CDB) informacinėje sistemoje duomenims kaupti ir informacijos paieškai naudojama duomenų bazių valdymo sistema. Ji susideda iš dvylikos integruotų centrinių duomenų bazių kuriose sukaupta per 18 mln. duomenų įrašų. Informacija iš centrinių duomenų teikiama per 4 tūkst. vartotojų policijos bei kitose institucijose. Policijos įstaigos turi galimybę pasijungti prie dviejų duomenų bazių valdymo sistemos kurios sujungtos į vieną centrinę duomenų bazę. Viena iš jų VRIS CDB duomenų saugykla administruojama informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos (toliau – Informatikos ir ryšių departamentas), kita sudaro policijos programinį paketą.

VRIS CDB centralizuotai kaupiami, apdorojami ir saugomi duomenys apie asmenis, daiktus, ir įvykius, registruotus LR vidaus reikalų ministerijos administracijos padaliniams priskirtoms sritims.

Policijos informacinę sistemą sudaro policijos programinis paketas kurio funkcijos: įvykių registracija, asmenų duomenų kartotekos kaupimas, baudžiamųjų bylų statistikos kartotekos kaupimas, personalo apskaita, finansinės ūkinės veiklos apskaita. Paketas sukurtas naudojantis naujomis (ORACLE, PHP) technologijomis. Šiuo metu šis paketas yra vienintelė programinė įranga

apjungianti į vieną paieškos sistemą CDB ir tipinio policijos paketo kaupiamus duomenis. Tai leidžia operatyviai gauti visą norimą informaciją (apie asmenį, transporto priemonę, ginklą ir kt.). Policijos programinio paketo savybė yra integracija su VRM centrinėmis duomenų bazėmis (VRIS CDB), pritaikant ir panaudojant VRM CDB adresų komponenčių sistemos klasifikatorius, asmens dokumentų, transporto priemonių, ieškomų asmenų, teistų asmenų duomenų bazes, bei panaudoti kitas VRIS CDB. Policijos programinis paketas išsiskiria nauju naudotojų teisių ir privilegijų valdymu, naudotojų administravimo sistema, visų naudotojų veiksmų registravimas. Intensyviai besivystančios internetinės technologijos sudarė galimybę į šią aplikacijų sistemą įtraukti informacijos pateikimą naudotojams internetinėmis priemonėmis. Taikant šią technologiją, naudotojui suteikiama galimybė dirbti su įprasta naudotojo sąsaja, taupomi informacinės sistemos resursai. Vienas iš aplikacijos privalumų yra tai, kad aplikacija nereikalauja instaliacijos, nenaudoja personalinio kompiuterio resursų, minimalus naudotojų apmokymo poreikis, žymiai mažesnis CDB tarnybinės stoties apkrovimas nei, aplikacijų sukurtų kitomis programinėmis priemonėmis.

Prieš gaudama leidimą iš Informatikos ir ryšių departamento prie VRM, policijos įstaigos atsakingas pareigūnas, privalo pateikti duomenis apie pareigūną bei jo darbo specifiką, kurie vėliau peržiūrimi ir pagal juos teikiama išvada. Departamento darbuotojams peržiūrėjus pateiktus duomenis iš davus sutikimą, įmonės darbuotojas ketinantis dirbti su centriniu duomenų banku rašo prašymą dėl asmens įrašymo į centrinio duomenų banko naudotojų sąrašą.

Vadovaujantis policijos generalinio komisaro 2002-08-09 įsakymu Nr.451 „Dėl Policijos programinio paketo“ patvirtintos instrukcijos reikalavimais, darbui su policijos programinio paketo duomenimis policijos įstaigos vadovas pildo tarnybinį prašymą dėl įrašymo į policijos programinio paketo naudotojų sąrašą, adresuotą Policijos departamento prie Lietuvos Respublikos vidaus reikalų ministerijos Policijos informacijos valdybai. Kiekvienas Vidaus reikalų ministerijos reguliavimo srities įstaigos tarnautojas arba darbuotojas dirbantis pagal darbo sutartį teisėtai užregistruojamas kaip VRIS CDB duomenų tvarkytojas ar gavėjas, turintis teises tvarkyti arba gauti VRIS CDB duomenis ir naudotis taikomosiomis programinėmis priemonėmis. VRIS CDB vartotoju gali būti kitos valstybės institucijos tarnautojas arba darbuotojas, dirbantis pagal darbo sutartį, šios institucijos ir VRIS CDB duomenų valdytojo duomenų teikimo sutartimi įgijęs teisę gauti VRIS CDB duomenis. Ypatingasis VRIS CDB vartotojas gali būti operatyvinės veiklos subjekto pareigūnas, kurio atliktų asmens duomenų peržiūrimos veiksmų duomenis (vykdytų užklausų ir užklausų rezultatų) be operatyvinės veiklos subjekto leidimo draudžiama atskleisti kitiems asmenims. Leidimą įregistruoti ypatingąjį VRIS CDB vartotoją, atsižvelgdamas į pareigūno vykdomas funkcijas, įsakymu suteikia operatyvinės veiklos subjekto vadovas. VRIS CDB vartotojo vardas žymimas lotyniškomis abėcėlės raidėmis arba skaitmenimis. Sistema yra sudėtinga,

kiekvienas veiksmas, kuris yra atliekamas prisijungiant prie duomenų bazės, yra fiksuojamas, o vartotojas – identifikuojamas. Po vartotojo įregistravimo VRIS CDB vartotojui suteikiamas vardas kuris suteikiamas VRIS CDB vartotojų administravimo sistemoje žr. 2.1 pav.

2.1 pav. Registravimosi į VRIS CDB registravimosi langas



Prisiregistravus atsidaro langas kuriame VRIS CDB administratorius periodiškai keičia pasijungimo prie sistemos slaptažodį.

Duomenų bazę prižiūri sistemos administratorius. Jis mato, ką vartotojas su tais duomenimis darė – juos išsispausdino, peržiūrėjo ar tvarkė.

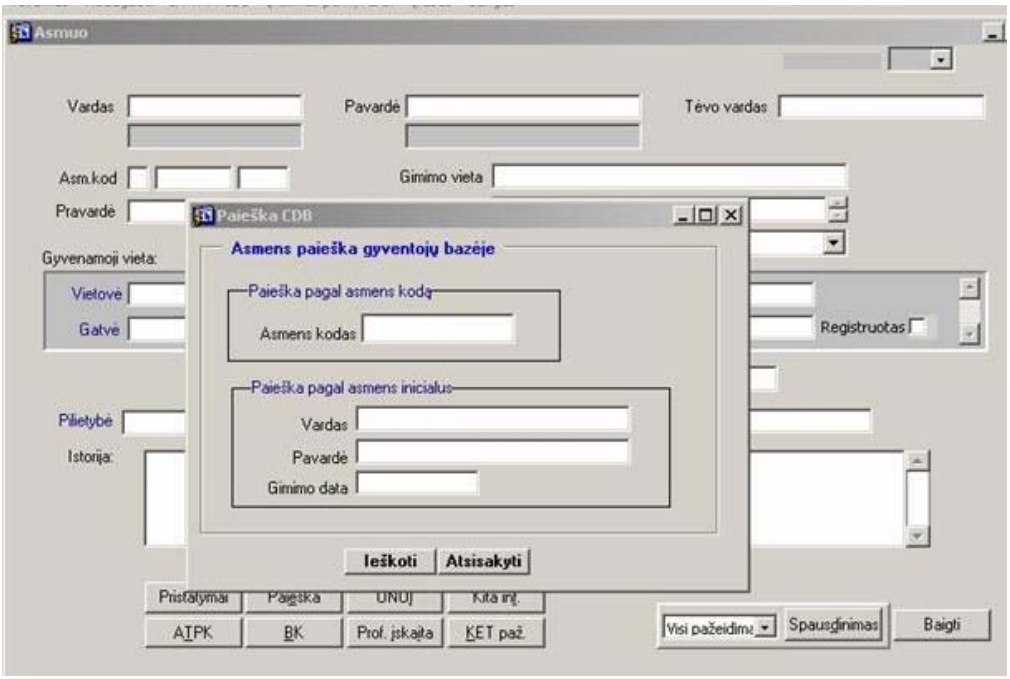
Pabandysime paanalizuoti Informatikos ir ryšių departamento prie VRM tvarkomas pagrindines aplikacijų sistemas bei policijos programinio paketo naršyklėje tvarkomus asmens duomenis.

2.2 pav. Įėjimo į VRIS CDB registravimosi langas



1) "**Lietuvos Respublikos gyventojai**". Tai VRM CDB aplikacijos sistema kurioje kaupiama informacija, gauta iš policijos komisariatų migracijos tarnybų apie fizinius asmenis, kuriems išduodami asmens tapatybę patvirtinantys dokumentai.

2.3 pav. Paieškos VRM CDB LR gyventojai



Informacijos turinys: asmens duomenys (asmens kodas, lytis, gimimo vieta ir data, vardas, pavardė, šeimos padėtis, tėvo, motinos, sutuoktinio ir vaikų asmens kodai, jų vardai ir pavardės), asmens dokumento duomenys, gyvenamosios vietos ir registracijos duomenys, tautybė, mirties data.

Pagrindinės funkcijos: informacijos paieška, statistikos skaičiavimas, duomenų gyventojų registrui teikimas. Duomenų tvarkymo tikslas, paskirtis: Išduodamų asmens dokumentų kontrolė; Duomenų teikimas LR gyventojų registrui. Duomenų šaltiniai: VRM Migracijos tarnybos, pasų poskyriai; duomenys apie asmens mirties faktą. VRM yra gyvenamosios vietos deklaravimo duomenų valdytoja.

2) "**Registruotos Lietuvos Respublikoje autotransporto priemonės**". Informacija gaunama iš Valstybės įmonės „REGITRA“ kuriai pavesta vykdyti kelių transporto priemonių registravimą ir apskaitą bei kitas su šia veiklos sritimi susijusias funkcijas.

2.4 Pav. Policijos informacinės sistema apie transporto priemones

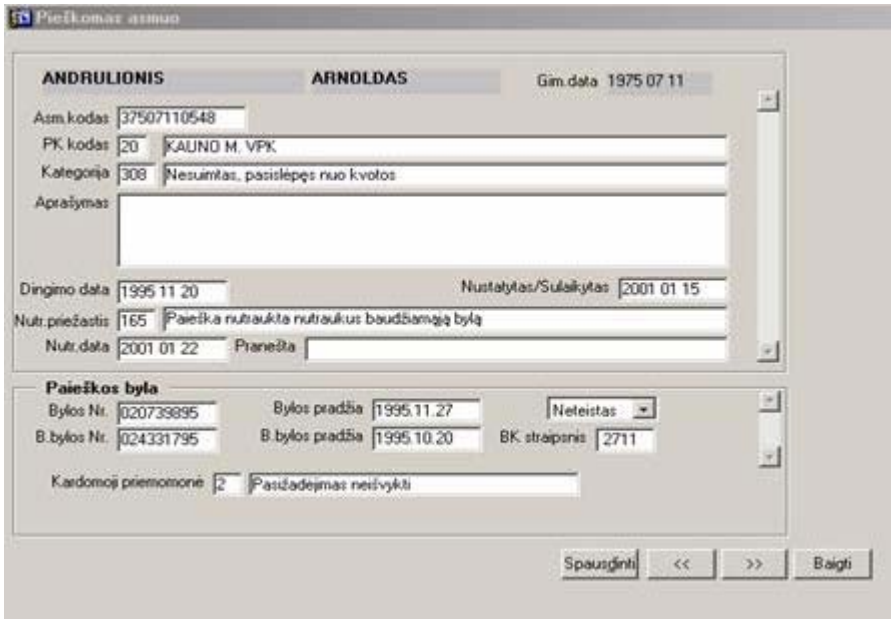


Turinys: informacija apie transporto priemonių savininkus fizinius asmenis (savininko asmens kodas, vardas, pavardė, gimimo data, autotransporto priemones (autotransporto rūšis, markė, gamybos metai, valstybinis numeris, detalių numeriai, spalva ir kt.), apie transporto priemonės įsigijimo būdą, savininko ar transporto priemonės duomenų pasikeitimą, autotransporto registravimo istorija. Pagrindinės funkcijos: informacijos registravimas, paieška, statistikos skaičiavimas, transporto priemonių ir transporto priemonių numerių kontrolė. VĮ „Regitra“ teikia asmens duomenis Valstybės ir teisėsaugos institucijoms, teisės aktų nustatyta tvarka. Asmens duomenų tvarkymas įregistruotas asmens duomenų registre.

3) "**Šaunamieji ginklai**". Informacija įvedama pagal šaunamųjų ginklų apskaitos kortelių duomenis arba gaunama iš policijos komisariatų. Informacijos turinys: duomenys apie ginklo savininką fizinį asmenį, asmeniui priklausantį medžiotojo bilietą, apie ginklo savininką juridinį asmenį, leidimo asmeniui laikyti ginklą duomenys, ginklo duomenys, duomenys apie asmenų padarytus pažeidimus. Pagrindinės funkcijos: šaunamųjų ginklų registracija, informacijos paieška ir statistikos skaičiavimas.

4) "**Ieškomi asmenys**". Informaciją įveda Policijos departamento prie VRM Operatyvaus valdymo tarnyba pagal gautus pranešimus. Lietuvos nacionalinis biuras pagal informacinius pranešimus iš kitų valstybių Interpolo nacionalinių biurų bei Informatikos ir ryšių departamento prie VRM pildo paieškos korteles. Informacijos turinys: duomenys apie ieškomą asmenį, paieškos paskelbimą ir paieškos nutraukimą. Pagrindinės funkcijos: informacijos paieška, statistikos skaičiavimas, nustatymas, ar konkretus asmuo yra ieškomas, kas jo ieško ir kodėl.

2.5 pav. Paieškomi asmenys



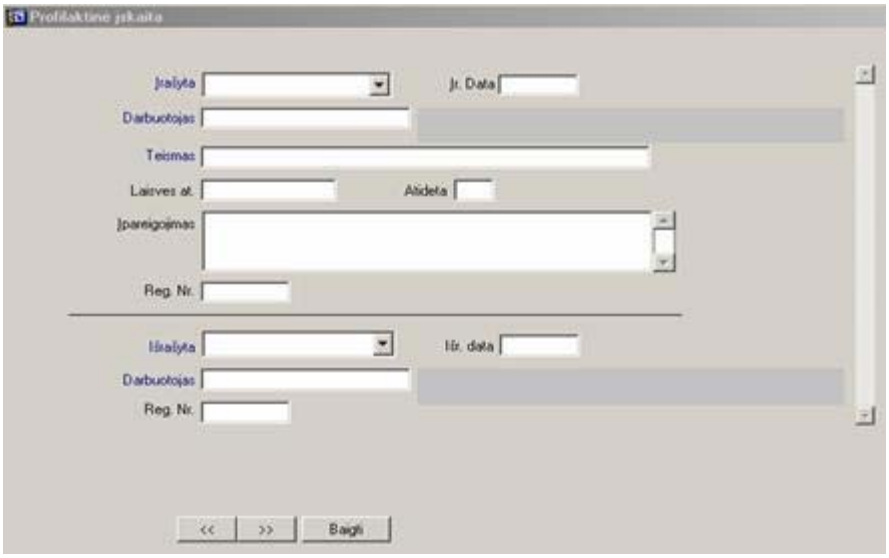
Duomenų tvarkymo tikslas, paskirtis: vykdyti paklausimus, rengti statistinius duomenis. Tvarkomų duomenų grupės: nusikaltėliai, dingę be žinios, skolininkai dėl alimentų išieškojimo, skolininkai dėl lėšų išieškojimo.

5) "**Vogtas autotransportas**". Informacija įvedama pagal duomenis, gautus iš miestų (rajonų) policijos komisariatų, Policijos departamento prie VRM Kriminalinių nusikaltimų tyrimo tarnybos bei Interpolo Lietuvos nacionalinio biuro. Informacijos turinys: duomenys apie vogtų transporto priemonių savininkus, apie vogtas autotransporto priemones, apie nusikaltimą (nusikaltimo aprašymas, data ir vieta, nusikaltimo registravimo duomenys), apie autotransporto suradimą. Pagrindinės funkcijos: informacijos paieška, statistikos skaičiavimas, nustatymas - konkreti transporto priemonė ar jos dalis yra vogta ar ne. Tvarkomų duomenų grupės: vogtos autotransporto priemonės; vogti valstybiniai numeriai ir kitos automobilių dalys.

6) "**Vogti šaunamieji ginklai**". Informacija įvedama pagal informacinę paieškos kortelę daiktui arba gaunama tarnybiniu paštu iš miestų (rajonų) policijos komisariatų, Interpolo Lietuvos nacionalinio biuro. Informacijos turinys: duomenys apie pavogtą, prarastą ar surastą ginklą bei nuosavybę, duomenys apie vagystę, ginklo suradimą ar paėmimą. Pagrindinės funkcijos: padėti nustatyti ryšį su padarytu nusikaltimu, nustatyti savininką, nukentėjusįjį, kaltinamąjį ir kitus duomenis, būtinus nusikaltimo atskleidimui, informacijos paieška, statistikos skaičiavimas. Duomenų tvarkymo tikslas, paskirtis: Programos yra skirtos VRM PD Viešosios policijos padaliniams šaunamųjų ginklų registracijai taip pat nustatyti ginklo priklausomybę. Tvarkomų duomenų grupės: Ginklo: rūšis, šalis - gamintoja, markė, serija, numeris, kalibras, vamzdžių kiekis, paskirtis, nuosavybė, teisė medžioti, leidimas asmeniui, medžiotojo bilietas.

7) "**Policijos profilaktinė įskaita**". Informacija įvedama pagal apskaitos kortelių "Įskaita", gautų iš policijos komisariatų, duomenis. Informacijos turinys: asmens duomenys, įrašymo į profilaktinę įskaitą duomenys (įrašymo į įskaitą pagrindas ir data, įstaigos, užregistravusios administracinį teisės pažeidimą, pavadinimas ir kt.). Pagrindinės funkcijos: informacijos paieška ir statistikos skaičiavimas.

2.6 pav. Policijos profilaktinė įskaita



Tvarkomų duomenų grupės: asmens (asmens kodas, vardas, pavardė, gyvenamoji vieta, ar buvo teistas), apie įrašymo į įskaitą pagrindą ir datą , apie išbraukimo iš ataskaitos pagrindą ir datą.

8) "**Numeruoti daiktai**". Informacija įvedama pagal informacinę paieškos kortelę daiktui. Joje gali būti įrašyta tik ta informacija, kuri užfiksuota baudžiamojoje byloje, tyrimo medžiagoje, dingusio be žinios asmens paieškos ir nežinomo žmogaus lavono asmenybės nustatymo byloje. Informacijos turinys: duomenys apie numeruotą daiktą ir jo nuosavybę, apie vagystę, daikto suradimą ar paėmimą (registravimo priežastis, bylos, medžiagos registracijos numeriai ir data, policijos įstaigos, užregistravusios įvykį, pavadinimas, daikto pavogimo, suradimo ar paėmimo aplinkybės ir kt.), apie asmenį, įstaigą, organizaciją, iš kurios daiktas pavogtas ar paimtas, informacija apie numeruoto daikto detales, jei tokios yra. Pagrindinės funkcijos: padėti nustatyti ryšį su padarytu nusikaltimu, nustatyti savininką, nukentėjusįjį ir kitus duomenis, būtinus nusikaltimo atskleidimui, informacijos paieška, statistikos skaičiavimas. Tvarkomų duomenų grupės: numeruoto daikto: rūšis, markė-modelis, šalis-gamintoja, serija, numeris, fasonas-forma, dydis-kalibras, spalva, ypatumai, vagystės data, inventorinis numeris, atlikimo technika, pagaminimo metai.

9) "**Filtras**". Čia kaupiama informacija apie asmenis, padariusius administracinius teisės pažeidimus, kurių pakartotinas įvykdymas per vienerius metus užtraukia baudžiamąją atsakomybę.

Informacija įvedama pagal administracinio teisės pažeidimo apskaitos korteles, gautas iš policijos komisariatų. Informacijos turinys: duomenys apie asmenį ir jo padarytą administracinį teisės pažeidimą. Pagrindinės funkcijos: informacijos paieška, baudžiamosios atsakomybės neišvengiamumo užtikrinimas - nustatymas, ar konkretus asmuo, kuris padarė administracinį teisės pažeidimą, už kurio pakartotiną įvykdymą per vienerių metų laikotarpį įstatymas numato baudžiamąją atsakomybę, yra padaręs analogišką pažeidimą per vienerius metus.

10) "**Operatyvinė-prevencinė įskaita**". Informacija įvedama pagal pateiktas prevencinio poveikio priemonių taikymo asmenims korteles. Informacijos turinys: duomenys apie asmenį, kuriam paskirta prevencinio poveikio priemonė, apie prevencinio poveikio priemones (oficialus perspėjimas, įrašymas į policijos prevencinę-operatyvinę įskaitą, teismo įpareigojimai), jų taikymo pagrindą ir laikotarpį, apie pritaikytus teismo įpareigojimus, apie išbraukimą iš įskaitos ar įpareigojimo panaikinimo priežastis, apie kortelę užpildžiusią policijos įstaigą. Pagrindinės funkcijos: informacijos paieška ir statistikos skaičiavimas.

11) "**Baudžiamoji statistika**". Duomenys įvedami pagal pateiktas statistines korteles arba iš teritorinių padalinių, atliekančių ikiteisminį nusikaltimų tyrimą. Informacijos turinys: duomenys apie nusikaltimą (baudžiamosios bylos, medžiagos, sumarinio proceso bylos numeris, jos iškėlimo data, kiti procesiniai sprendimai, priimti byloje, subjektai, priėmę šiuos sprendimus, nusikaltimo kvalifikavimas pagal LR Baudžiamąjį kodeksą, kardomosios priemonės, nusikaltimo padarymo vieta, padarymo būdai, įrankiai, priemonės ir motyvai, pasikėsinimo objektai, paimti ginklai, narkotinės priemonės, materialinė žala ir jos atlyginimas, tarnyba, padėjusi nustatyti asmenį, padariusį nusikaltimą, agentūriniai pranešimai, liudytojai) ir duomenys apie asmenį, padariusį nusikaltimą (vardas, pavardė, gimimo data ir vieta, gyvenamoji vieta, asmens kodas, tautybė, išsilavinimas, užsiėmimas nusikaltimo padarymo metu, ankstesnis teistumas, alkoholio ar narkotikų vartojimas). Pagrindinės funkcijos: informacijos paieška ir statistikos skaičiavimas, periodiškas statistinių ataskaitų darymas.

12) "**Teistumo duomenų bazė**". Ją sudaro informacija apie teistus, suimtus ir patrauktus baudžiamojon atsakomybėn asmenis. Turinys: informacija apie teistus asmenis (vardas, pavardė, tėvo vardas, gimimo data, asmens kodas, gimimo vieta, gyvenamoji vieta), apie asmens teistumą, suėmimą, patraukimą baudžiamojon atsakomybėn, bausmės atlikimo vietą ir laiką, paleidimą iš įkalinimo įstaigos. Pagrindinės funkcijos: informacijos centralizuota apskaita, paieška, pažymų apie asmens teistumą išdavimas. Duomenų tvarkymo tikslas, paskirtis: operatyviai ir tiksliai kaupti informaciją, jeigu reikia, išreikalauti ją iš atitinkamų teisėsaugos institucijų, užtikrinti kokybišką informacijos patikrinimą ir pažymų išdavimą laiku pagal policijos komisariatų, kitų teisėsaugos institucijų pateikiamus reikalavimus bei asmeninius piliečių prašymus.

13) "**Nepageidautini asmenys**". Duomenų bazėje kaupiama informacija apie užsieniečius, kurių buvimas Lietuvoje nepageidautinas. Turinys: asmens vardas, pavardė, gimimo data ir vieta, pilietybė, priežastis, dėl kurios asmens informacija įtraukta į šią duomenų bazę. Pagrindinės funkcijos: informacijos paieška, statistikos skaičiavimas.

14) "**Etatai**". Čia kaupiama informacija apie Vidaus reikalų ministerijos sistemos užimtus ir laisvus etatus. Pagrindinės funkcijos: informacijos paieška ir statistikos skaičiavimas.

2.7 pav. CDB personalas



15) "**Personalas**". Čia kaupiama informacija apie Vidaus reikalų ministerijos sistemos personalą. Turinys: dirbančiųjų lytis, amžius, išsilavinimas, darbo stažas ir kt. Pagrindinės funkcijos: personalo apskaita, informacijos paieška ir statistikos skaičiavimas.

Vidaus reikalų ministerijos informacinės sistemos duomenų bazių „Personalas“, „Etatai“ duomenų gavėjai yra policijos struktūriniai padaliniai. Šios duomenų bazės skirtos vidaus administraciniams tikslams, todėl patenka į grupę duomenų apie kurių tvarkymą nereikia pranešti VDAI[46]. ADTAĮ 2 straipsnio 14 dalis, kuri apibrėžia sąvoką „vidaus administravimas“: veikla, kuria užtikrinamas duomenų valdytojo savarankiškas funkcionavimas (struktūros tvarkymas, personalo valdymas, turimų materialinių ir finansinių išteklių valdymas ir naudojimas, raštvedybos tvarkymas). Valstybės ir tarnybos paslaptys taip pat įeina į asmens duomenų grupę kai apie tvarkymą pranešti nereikia[47]. Ši apimtis yra didžiaja dalimi paremta faktu, kad duomenų tvarkymas, kurį numato Valstybės ir tarnybos paslapčių įstatymas, didžiąja dalimi nepatenka į Direktyvos

[46] ADTAĮ 25 str. Asmens duomenys gali būti tvarkomi automatiniu būdu tik kai duomenų valdytojas arba jo atstovas nustatyta tvarka praneša Valstybinei duomenų apsaugos inspekcijai, išskyrus atvejus, kai asmens duomenys tvarkomi vidaus administravimo tikslais.
[47] ADTAĮ 25 str. 5d.

95/46/EB apimtį. Direktyvos 3 straipsnio 2 dalies pirmas punktas nustato, kad Direktyva nėra taikoma, kai yra užsiimama tokia veikla, kuriai netaikomi Bendrijos įstatymai, (…) taip pat kai atliekamos tvarkymo operacijos, susijusios su visuomenės saugumu ir gynyba, su valstybės saugumu (taip pat ir valstybės ekonomine gerove, kai tvarkymo operacija susijusi su valstybės saugumo klausimais) ir su valstybės veiksmais baudžiamosios teisės srityje.

Policijos programinio paketo "Baudžiamoji statistika", "Šaunamieji ginklai", "Vogti šaunamieji ginklai", "Vogtas autotransportas" aplikacijos registruotos VDAI asmens duomenų tvarkymo valdytoju registre. Tačiau informacinėse aplikacijoje "Ieškomi asmenys", "Policijos profilaktinė įskaita", "Numeruoti daiktai", "Filtras", "Operatyvinė-prevencinė įskaita" to nėra padaryta. Deklaruojamas policijos įstaigų abstraktus asmens duomenų tvarkymo tikslas kuris apima nusikalstamų veikų (nusikaltimų ir baudžiamųjų nusižengimų), asmenų, įtariamų (kaltinamų) nusikalstamų veikų padarymu, asmenų, pripažintų nukentėjusiais, duomenų apskaita, statistinių ataskaitų rengimas. Atsakomybė tenka duomenų valdytojui arba jo atstovui (pastarasis reikalingas tam, kad būtų pabrėžta asmeninė atsakomybė tuo atveju, jeigu valdytojas yra juridinis asmuo). Už šio įstatymo pažeidimą atsakomybę numato ADTAĮ 33 straipsnis bei Administracinio teisės pažeidimų kodekso 214-14 straipsnis, kuris taip pat numato pažeidėjui skiriamas baudas.

Duomenų bazėje ,,LR Gyventojai“ yra ir kiti (ne gyvenamosios vietos deklaravimo) asmens duomenys, pvz.: šeiminė padėtis, tėvo asmens kodas, motinos asmens kodas, sutuoktinio asmens kodas, vaikų asmens kodai, jų vardai ir pavardės, asmens dokumento rūšis, dokumento serija ir numeris, tautybė (ypatingas asmens duomuo) ir kt. Nei įstatymai, nei Vyriausybės nutarimai nereglamentuoja teisinio pagrindo, pagal kurį VRM būtų tokių duomenų valdytojas. Duomenų bazėje ,,LR Gyventojai“ yra identiški duomenys Gyventojų registro tarnybos valdomai Gyventojų registro duomenų bazei. VRM sukurta naršyklė, leidžia jungti, grupuoti asmens duomenis, siejant juos su giminaičiais, kaimynais, transporto priemonėmis.

Duomenų subjektas žino, kad jo gyvenamosios vietos deklaravimo duomenis tvarko VRM. Tai, yra užregistruota asmens duomenų valdytojų valstybės registre, nes tvarkomi duomenys patenka į grupę duomenų kai apie tvarkymą būtina pranešti. Bet duomenų subjektas nėra informuojamas, apie tai, kad VRM informacinėje sistemoje tvarkomi ir kiti asmens[48] duomenys tuo pažeidžiant ADTAĮ.

Be to, už asmens duomenų apsaugą atsakinguoju yra paskirtas ne duomenų valdytojo (VRM), o duomenų tvarkytojo (Informatikos ir ryšių departamento) atstovas. Manytina, kad dėl šių

[48] Nėra deklaruojama apie galimybę kaupti ne vietos deklaravimo duomenis, grupuoti asmens duomenis, siejant juos su giminaičiais, kaimynais, transporto priemonėmis.

aplinkybių išauga neteisėtos asmens duomenų peržiūros ir kitokio naudojimo tikimybė, netinkamai įgyvendinant organizacines priemones.

Peržiūrėjus policijos programinio paketo kaupiamus duomenis šalia asmenų (policijos įskaita) pasigendama fotokartotekos duomenų aplikacijoje. Nors VRIS CDB ir gaunama informacija tikrinama, nemažai pasitaiko atvejų, kai atsakomybėn patraukiami asmenys, neturėję nieko bendra su teisės pažeidimu, nes duomenų valdytojui nesuteikta galimybė tikslai nustatyti asmens tapatybės. Netinkamai nustačius asmens tapatybę ne kartą atsakomybės buvo patrauktas nekaltas žmogus kurio asmens duomenimis pasinaudojo kitas asmuo[49], dėl to tikslinga modernizuojant ir vystant programinį paketą sukurti fotokartotekos įskaitos aplikaciją.

Policijos įstaigos be policijos programinio paketo tvarko duomenis automatinu būdu ir iš Vilniaus mieste esančių vaizdo kamerų bei greičio matuoklių apie kuruos bus kalbama šio darbo 3 skyriuje.

2.4. Asmens kodas informaciniuose registruose

Pagal ADTAĮ, asmens duomenimis laikytini ne tik asmens vardas, pavardė, bet ir bet kokia kita informacija, kuria pasinaudojus galima tiesiogiai ar netiesiogiai nustatyti asmens tapatybę. ***Asmens kodas*** – unikali skaitmenų seka, kuri asmeniui suteikiama Gyventojų registro įstatyme nustatyta tvarka.[50] Asmens identifikavimo kodas gali būti panaudotas kaip raktas, atveriantis duris į valstybės ir kitų viešųjų tarnybų siūlomas elektronines paslaugas. Turint omeny duomenų apsaugą, svarbu užtikrinti pagrindinį principą – leisti naudoti asmens duomenis tik tuo tikslu, kuriuo jie buvo surinkti. Vadovaujantis Gyventojų registro įstatymu (toliau-GRĮ) asmens identifikavimo kodas yra suteikiamas kiekvienam LR piliečiui, o taip pat asmenims be pilietybės ir kitiems valstybių piliečiams, deklaruojantiems gyvenamąją vietą Lietuvoje ar registruojantiems asmens civilinės būklės pasikeitimus Lietuvos Respublikos institucijose[51]. GRĮ 8 straipsnio 3 dalis nustato, kad asmens identifikavimo kodas yra įrašomas į asmens dokumentus[52].

Asmens (identifikavimo) kodo kaip bendrojo taikymo žymens reikšmė ir paskirtis yra apibrėžta Gyventojų registro įstatyme 4 straipsnio 9 dalyje. Vadovaujantis šia nuostata, kodas yra skirtas „asmeniui identifikuoti, duomenims apie jį kaupti, valstybės registrų ir informacinių sistemų sąveikai užtikrinti“.

---

[49] Klaipėdos miesto apylinkės teismas nekaltam žmogui skyrė administracinę nuobaudą, apie kurią pastarasis sužinojo tada, kai antstoliai atsiuntė pranešimą apie pradėtą baudos išieškojimą. Žmogaus teisių stebėjimo instituto ataskaita http://www.hrmi.lt/ prisijungimo laikas 2004-12-14

[50] Asmens duomenų apsaugos įstatymas 7 straipsnis

[51] Ta pati formuluotė nurodyta Gyventojų registro nuostatų 3 dalyje.

[52] Nei GRĮ, nei nuostatai nepatikslina, kokie tai dokumentai.

Lietuvoje sukurta sistema atitinka Direktyvos 95/46/EB 8 straipsnio 7 dalyje apibrėžtą sistemą. Asmens identifikavimo kodas 7 straipsnio prasme – **tai nacionalinis žymuo tapatybei nustatyti,** kuris yra bendrai taikomas visoje Lietuvos teisinėje sistemoje. Direktyvos 8 straipsnio 7 dalyje pripažįstama, kad valstybės narės gali turėti bendrojo taikymo žymenų sistemą tapatybei nustatyti. Kadangi 7 straipsnis patenka į Direktyvos 95/46/EB 8 straipsnio 7 dalies kompetencijos sritį (ypatingi duomenys), tai reiškia, kad asmens identifikavimo kodas yra tam tikra prasme ypatingi duomenys, kurių apibrėžimas pateiktas 2003 m. ADTAĮ 2 straipsnio 9 dalyje. Taigi asmens identifikavimo kodas turi būti naudojamas taip, kad būtų atsižvelgta į jo jautrumą. Pagrindinės asmens duomenų perdavimą ES ribose reguliuojančios direktyvos 95/46/EB, 2002/58/EB apie asmens kodus beveik nekalba, apsiribojama tik tokia Direktyvos 95/46/EB 8 str. 7 d. nuostata: "Šalys Narės nustatys sąlygas, kuriomis nacionalinis identifikavimo numeris ar bet koks kitoks bendro taikymo identifikavimo žymuo gali būti naudojamas." 2001 metais nedidelę šios taisyklės išimtį numatė tik Europos Parlamento ir Tarybos reglamentas Nr. 45/2001. Čia teigiama, kad nustatymas tvarkos, pagal kurią nacionaliniai identifikavimo žymenys naudojami ES institucijų, paliekama ES kompetencijai (10 str. 6 d.). Tok į negausų asmens kodų srities reguliavimą ES teisėje sąlygojo gana dideli ES valstybių narių teisės šioje srityje skirtumai.

Yra valstybių, kurios apskritai nenaudoja oficialių, įvairios paskirties identifikavimo kortelių, kartu – asmens kodų, kaip jie suprantami Lietuvoje. Tarp tokių valstybių – Australija, Kanada, Indija, Airija, Naujoji Zelandija, JAV, Skandinavijos šalys, Jungtinė Karalystė. Šiose šalyse vietoje vieno kodo, naudojamo nusakant asmens tapatybę bet kurioje situacijoje, naudojami įvairūs siaurai taikomi žymenys. Kai kuriose šalyse kaip, pavyzdžiui, Vokietija, bendrasis asmens identifikavimo kodo taikymas prieštarauja konstitucijai. Vadovaujantis 1983 m. Vokietijos Federalinio Konstitucinio Teismo sprendimu, kuriame buvo pažymėta, kad „unikalus asmens identifikavimo numeris, skirtas visiems gyventojams, prieštarautų konstitucijai. Teismas nusprendė, kad visų gyventojų registravimas, surašymas į katalogus ir laikymas „kodu" žeidžia žmogaus orumą ir buvo atsisakyta asmens kodo įvedimo ir šiuo metu numerius turi tik gyventojų pasai ir asmens tapatybės kortelės, tačiau šie numeriai keičiasi keičiant nurodytus dokumentus. Todėl Vokietijoje neįmanomas lietuviškasis modelis. Vokietijoje yra su sektoriais susieti asmens identifikavimo kodai: pavyzdžiui, pensininko draudimo ar mokesčio mokėtojo kodas.

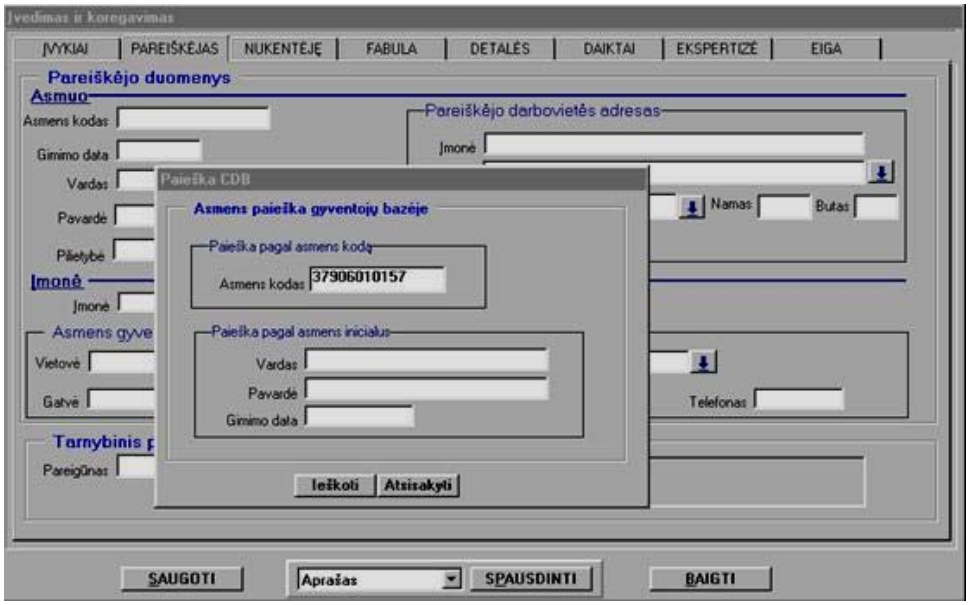
Asmens kodų pirminė paskirtis Belgijoje, Prancūzijoje, kitose minėtose valstybėse (ir Lietuvoje) – *tinkamai identifikuoti* asmenį, nedviprasmiškai apibūdinti jo tapatybę, išvengti dėl vardų/pavardžių vienodumo kylančios painiavos. "Išgryninant" asmens kodų naudojimą, būtent į tokią jų paskirtį ir atsižvelgiama. Būtina imtis priemonių apriboti nepateisinamą šios asmens informacijos platinimą.

Asmens identifikavimo kodas gali būti panaudotas kaip raktas, atveriantis duris į valstybės ir kitų viešųjų tarnybų siūlomas elektronines paslaugas. Vieną kodą turėti yra ir gerai, ir pavojinga. Viena vertus, esant vienam unikaliam kodui lengviau užtikrinti sąveiką tarp skirtingų registrų ir duomenų bazių, taip pat surasti paieškomus asmenis. Kita vertus, asmens tapatybė gali bet kas lengvai nustatyti, nepriklausomai nuo kodo naudojimo tikslų ir aplinkybių. Be to, unikalus kodas tam tikra prasme gali padėti užtikrinti įstatymų nustatytą duomenų valdytojo pareigą saugoti tik teisingus duomenis, o tam reikalingas teisingas duomenų subjekto identifikavimo kodas.

Lietuvoje paplito sunkiai pateisinamas asmens kodo naudojimas. Kiekvienas asmuo turi asmens kodą, kuris turi būti nurodomas asmens dokumentuose. Tačiau asmens kodas vis dažniau naudojamas be jokio reikalo, taip viešinami asmens duomenys. Pavyzdžiui, jis naudojamas prisegamuose darbuotojo pažymėjimuose arba sudarant minimaliausius sandorius. Taip bet kuris asmuo gali atsirinkti privačią informaciją, nes asmens kodai parodo asmens lytį ir gimimo datą. Šį kodą galima surasti nacionalinėje asmens tapatybės kortelėje, piliečio pase ir vairuotojo pažymėjime. Kita vertus, kodą gali lengvai pamatyti bet kas, į kurio rankas patenka dokumentai, nepriklausomai nuo, ar jam šie duomenys reikalingi, ar ne.

ADTAĮ 7 straipsnio 2 ir 3 dalyse yra numatytos įvairios sąlygos, kurioms esant duomenų valdytojai gali panaudoti asmens identifikavimo kodą. Iš esmės asmens kodą galima panaudoti tik tada, jei gautas duomenų subjekto sutikimas. Šios išimtys – tai baigtinis ir išimtinis atvejų sąrašas, kai asmens kodas gali būti tvarkomas be duomenų subjekto sutikimo. Vadovaujantis ADTAĮ 3 dalies 3 punktu, asmens identifikavimo kodą galima panaudoti be duomenų subjekto sutikimo valstybės registruose ir informacinėse sistemose, jeigu jie yra įteisinti teisės aktų nustatyta tvarka. Kalbant apie valstybės registrus, tuo pačiu ir apie policijos informacines sistemas akivaizdu, kad juose naudinga tvarkyti asmens kodą. Paprastai tokie registrai yra paremti asmens kodu kaip pagrindiniu žymeniu. žr.2.8 pav.

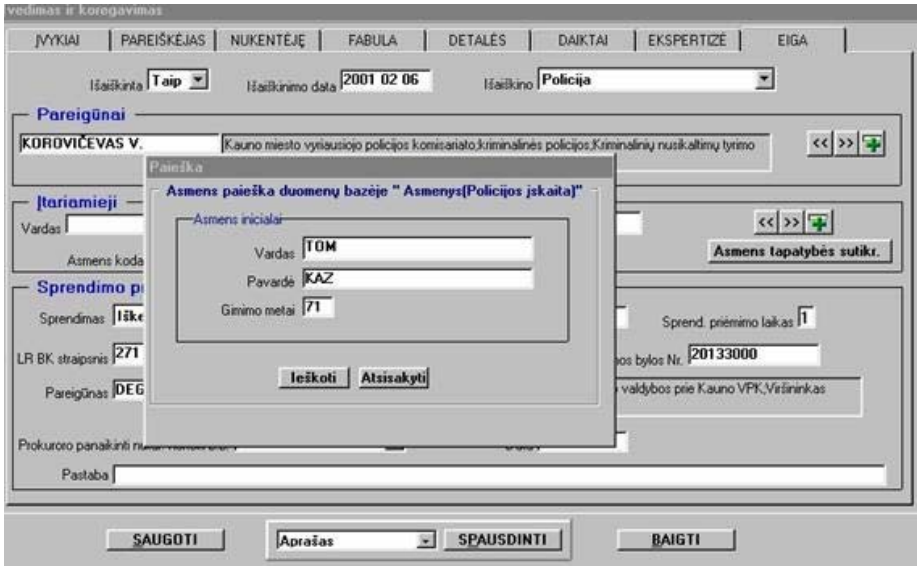
2.8 pav. Informacijos paieška pagal asmens kodą



Tai viena iš priežasčių, dėl kurių buvo sukurtas asmens identifikavimo kodas. Siekiant užtikrinti tinkamas ypatingų duomenų apsaugos priemones, turi būti aiškiai nurodyta atitinkamame registrų įstatyme, ar leidžiama tvarkyti asmens kodą, o jeigu taip – esant kokioms sąlygoms ir kokiais tikslais.

Tarkim policijos informacinėse sistemoje “Gyventojų registras“ atlikti asmens duomenų paiešką galima pagal daug faktorių asmens kodą; vardą pavardę, gimimo data, tačiau žinant paieškomo asmens kodą sužinoti asmens duomenis yra žymai paprasčiau. Kai norima sužinoti, kur jis dabar gyvena, kur registruotas, įeinant į duomenų bazę reikia nurodyti pirmąją vardo raidę ir pavardės šaknį. Kai norima sužinoti, kur jis dabar gyvena, kur registruotas, įeinant į duomenų bazę reikia nurodyti pirmąją vardo raidę ir pavardės šaknį.

2.9 pav. Informacijos paieška pagal pavardę



Alytaus organizuotų nusikaltimų tyrimo tarnybos inspektorės A.G. teigimu[53], Alytaus mieste yra triskart už grotų patekęs Algis Brazauskas. Tikrinant asmenį pagal pavardę „gauni žinių apie penkis ar šešis Brazauskus. Jeigu nenori, kad tarp jų būtų ir premjeras, gali jį apsaugoti nuo tokio „sekimo“. Tereikia užblokuoti jo duomenis“, Tik Vilniuje rasime 2 Algirdus Brazauskus, 6 Artūrus Paulauskus, net 19 Jonų Kazlauskų ir t.t. O per visą šalį tokių žmonių, kurių pavardės ir vardai sutampa, yra dar daugiau.[54] Taigi nustatant už valkatavimą sulaikyto asmens, kurio pavardė tokia pat kaip aukštą postą užimančio asmens, tapatybę duomenų bazė gali pateikti ir aukštą postą užimančio asmens pavardę. Ir tai bus užfiksuota kaip duomenų rinkimas apie tą aukštą asmenį. Panaudojus Informatikos ir ryšių departamento CDB specialistai, atlikę dalinį Vidaus reikalų ministerijos informacinės sistemos vartotojų paklausimų per 2003 metų liepos patikrinimą, nustatė, jog buvo domėtasi duomenimis apie aukščiausius šalies pareigūnus. Nustatyta, kad Prezidento Valdo Adamkaus asmens duomenų paiešką vykdė devyni, o jo žmonos Almos Adamkienės – trys įvairių miestų ir rajonų policijos komisariatų pareigūnai. R.Pakso asmens duomenų paiešką vykdė septyni, premjero A.Brazausko – trylika, Seimo pirmininko Artūro Paulausko – penki policijos pareigūnai. Taip pat buvo domėtasi A.Paulausko žmonos Jolantos, vidaus reikalų ministro, kitų aukštų Vidaus reikalų ministerijos pareigūnų duomenimis.[55]

2.10 pav. Paieška pagal pavardę

[53] Tarp seklių komisaro žmona//Lietuvos rytas, 2003-04-17
[54] Totalinio sekimo skandalas – audra stiklinėje//Lietuvos rytas, 2003-04-12
[55] Mesti baisūs kaltinimai bliūkšta//Lietuvos rytas, 2003-04-15



Kauno m. VPK asmenų DB

Vardas	Pavardė	Tėvo vardas	Asmens kodas
TOMAS	KAZLAUSKAS		3 831029 0499
TOMAS	KAZLAUSKAS		3 830703 0759
TOMAS	KAZILIONIS		3 830921 0429
TOMAS	KAZLAUSKAS		3 810827 0460
TOMAS	KAZLAUSKAS		3 720831 0730
TOMAS	KAZLAUSKAS	ANTANAS	3 760424 0018
TOMAS	KAZLAUSKAS		3 580826 0457
TOMAS	KAZOKAS		3 731127 0313
TOMAS	KAZOČIŪNAS		3 760629 0509
TOMAS	KAZLAUSKAS		3 790319 0095
TOMAS	KAZLAUSKAS		3 830316
TOMAS	KAZLAUSKAS	PETRAS	3 660101
TOMAS	KAZAKEVIČIUS		3 711020 0733
TOMAS	KAZLAUSKAS	ALBERTAS	3 800320 0090

Nors Informatikos ir ryšių departamento informacinės sistemos yra sudėtingos, kiekvienas veiksmas, kuris yra atliekamas prisijungiant prie duomenų bazės, yra fiksuojamas, o vartotojas – identifikuojamas. „Bazę prižiūri sistemos administratorius. Jis mato, ką vartotojas su tais duomenimis darė – juos išsispausdino, peržiūrėjo ar tvarkė. Daugeliu atvejų duomenų bazėje kai kurie pareigūnai tiesiog patenkino savo smalsumą. Kai kam paprasčiausiai rūpėjo pasidomėti, kokio amžiaus yra galimos pirmosios šalies ponios. O viena Molėtų migracijos tarnybos darbuotoja norėjo sužinoti, kada gimęs jai patinkantis simpatingas Policijos departamento pareigūnas. Moteris bandė lyginti savo ir šio vyriškio horoskopus. „Ko gero, daugelis pareigūnų bandė patenkinti savo smalsumą, bet smalsumas – taip pat nusikaltimas, jeigu jis prieštarauja galiojantiems įstatymams“, – „Lietuvos rytui“ teigė V.Ivanauskas[56]. Nors Vidaus reikalų ministerijos duomenų bazėje esanti informacija yra anketinio pobūdžio, svarbu užtikrinti žmogaus teisių laikymąsi ir apsaugoti asmens duomenis tokius kaip asmens kodas nuo bereikalingo ar smalsaus naudojimosi.

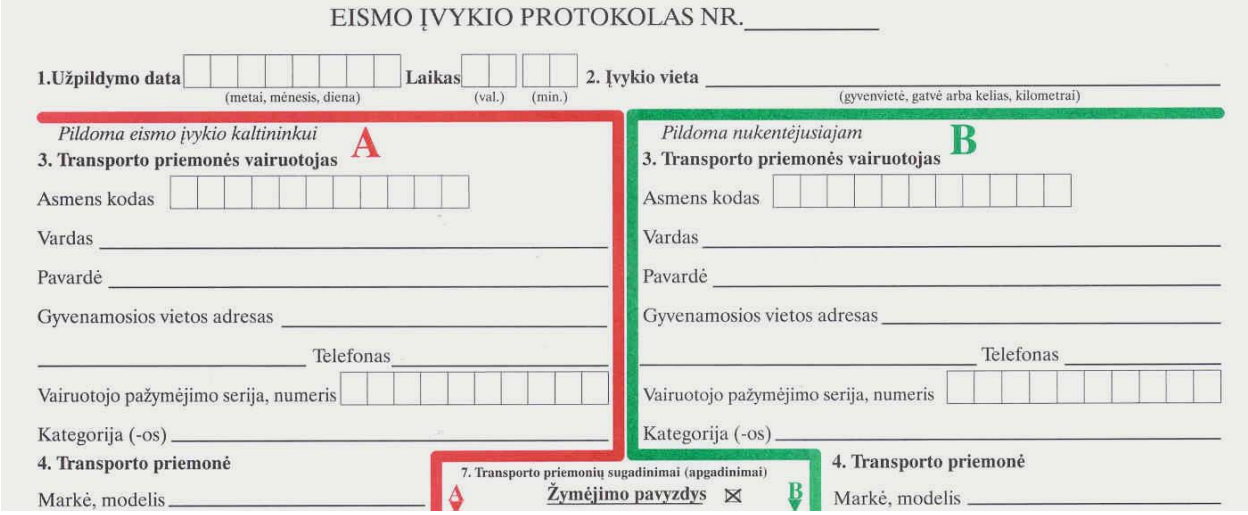
Nerimą kelianti yra Asmens duomenų apsaugos įstatymo numato 7 straipsnio 3 dalies 4 punkto nuostatą, vadovaujantis kuria asmens be duomenų subjekto sutikimo leidžiama tvarkyti **juridiniams asmenims** tokių kaip draudimo bendrovės, kurie vykdo tam tikrą veiklą. Kadangi viena iš tokių veiklų yra betarpiškai surišta su policijos duomenų tvarkymu ir asmens duomenų tvarkymu.

Asmens duomenų inspekcijos asmens duomenų valdytojų registruose radau 39 įrašus apie registruotas draudimo bendroves kurie kaupia asmens duomenis. Bendrovės užsiima asmenų, turto ir transporto priemonių draudimu ir neabejotinai savo informacinėse sistemose naudoja asmens kodą. Draudimo bendrovėms yra įstatymu suteikiama panaudoti asmens kodą, jeigu jis yra reikalingas vartotojo unikalumui nustatyti. Tačiau draudimo bendrovės piniginei išmokai patvirtinti

[56] Mesti baisūs kaltinimai bliūkšta//Lietuvos rytas, 2003-04-15

siunčia užklausią į policijos įstaigas. Eismo įvykių protokoluose žr. 2.11 pav., 2.12 pav. bendrovės gauna informacija apie abiejų eismo įvykių dalyvių bei pareigūno forminusio įvykį asmens kodą bei kitus asmens duomenis. O tai jau pertekliniai duomenys.

2.11 pav. Eismo įvykio protokolo viršutinė dalis


EISMO ĮVYKIO PROTOKOLAS NR._____

1.Užpildymo data _____ (metai, mėnesis, diena) Laikas _____ (val.) _____ (min.) 2. Įvykio vieta _____ (gyvenvietė, gatvė arba kelias, kilometrai)

Pildoma eismo įvykio kaltininkui A

3. Transporto priemonės vairuotojas

Asmens kodas

Vardas _____

Pavardė _____

Gyvenamosios vietos adresas _____

_____ Telefonas _____

Vairuotojo pažymėjimo serija, numeris

Kategorija (-os) _____

4. Transporto priemonė

Markė, modelis _____

Pildoma nukentėjusiajam B

3. Transporto priemonės vairuotojas

Asmens kodas

Vardas _____

Pavardė _____

Gyvenamosios vietos adresas _____

_____ Telefonas _____

Vairuotojo pažymėjimo serija, numeris

Kategorija (-os) _____

4. Transporto priemonė

Markė, modelis _____

7. Transporto priemonių sugadinimai (apgadinimai)

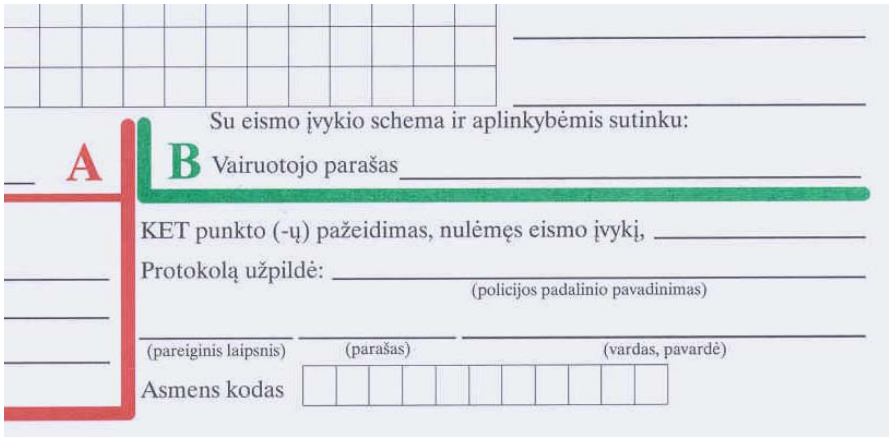
Žymėjimo pavyzdys ⊠

A B

ADTAĮ 5 straipsnio 3 pastraipos 4 dalyje nurodytas juridinis asmuo, prieš pradėdamas naudoti asmens kodą, turi visų pirma gerai išsiaiškinti, ar jam iš tikrųjų reikalingi šie duomenys savo verslo tikslams pasiekti bei užduotims įvykdyti. Renkant asmens duomenis, reikia užtikrinti, kad duomenys būtų tik tokios apimties, kuri būtina jiems rinkti ir toliau tvarkyti. Dažniausiai asmens kodą galima naudoti tik gavus duomenų subjekto sutikimą. Vadovaujantis ADTAĮ, sutikimas – savanoriškas duomenų subjekto valios pareiškimas tvarkyti jo asmens duomenis jam žinomu tikslu. Atitinkamoms institucijoms pateikiamų dokumentų turinys dažniausiai teisės aktuose yra konkrečiai apibrėžtas. Dokumentai, kuriuose reikalaujama (pageidaujama) nurodyti asmens kodus, yra labai įvairūs. Jie skiriasi ne tiktai savo turiniu, bet ir paskirtimi, naudojimo dažnumu, galimybėmis su jais susipažinti (užfiksuoti) kitiems asmenims (prieinamumu), pagal subjektus, kuriems atskleidžiami asmens kodai. Šiuo atveju policijos įstaigos darbuotojai jokiu teisės aktu neįpareigojami to daryti. Nepakanka nuostatos, kad asmens kodo panaudojimas gali praversti siekiant tikslų. Be to, pati policijos įstaiga rengdama eismo įvyko protokolo blanko pavyzdžius nesilaiko pagrindinių Asmens duomenų apsaugos reikalavimų priimdami Lietuvos Respublikos Policijos departamento generalinio komisaro 2002-12-14 d. įsakymą Nr.660 kuriame reglamentuojama policijos pareigūnų veiklos instrukcija bei įteisinamas draudimo bendroves tenkintinas eismo įvykio blankas.

Duomenų subjektas patekęs į eismo įvykį nebegali pareikšti savo valios, kad nebūtų tvarkomi jo ypatingi asmens duomenys (asmens kodas), nes teisės aktai įpareigoja įforminti šį procesą įstatymo nustatyta tvarka, kuri prieštarauja duomenų subjekto teisei pasirinkti duoti sutikimą arba ne tvarkyti savo asmens duomenis, be to, perduoti tuos duomenis kitiems. Pakaktų, kad procesinių dokumentų grafose būtų duomenų subjekto sutikimas tvarkyti jo duomenis (ypač asmens kodą) bei sutikimas juos perduoti trečiosiomis šalims. Kita būtina sąlyga turėtų būti alternatyvus pasiūlymas, asmens kodą pakeičiant vairuotojo pažymėjimo ar kito dokumento numerio fiksavimu. Tokiu būtu galima nesunkiai išspręsti šią susidariusią situaciją.

2.12 pav. Eismo įvykio protokolas kuriame policijos įstaigos darbuotojas pats privalo suteikti tretiems asmenis savo asmens kodą



Direktyvos 95/46/EB 6 straipsnio 1 dalies b) punkte. ADTAĮ reikalauja, kad asmens duomenys būtų renkami apibrėžtais ir teisėtais tikslais, nustatytais prieš renkant asmens duomenis, ir paskui tvarkomi su šiais tikslais suderintais būdais.

Pagal dabar galiojančią tvarką eismo įvaikio protokolas kuriame fiksuojami trijų duomenų subjektų asmens kodai patenka į draudimo bendrovę kuri tvarko gautus duomenis be duomenų subjektų leidimo ir neįvardijusi savęs kaip asmens duomenų valdytoja.

Policijos įstaigos teikdamos asmens duomenis draudimo bendrovėms be duomenų subjekto informavimo bei teikdama perteklinius duomenis pažeidžiant ketvirtąjį bendrą asmens duomenų tvarkymo principą.[57]. Šiuo atveju duomenys turi būti atrenkami remiantis tikslu rinkti ir tvarkyti kiek įmanoma mažiau duomenų, o šiuo atveju duomenų valdytojas surenka daugiau asmens duomenų negu reikia nustatytiems tikslams.

[57] Asmens duomenys renkami ir tvarkomi, jei jie tinkami, tapatūs ir nedidesnės apimties, atsižvelgiant į nustatytus tikslus.

Baigiant temą kurioje keliamas klausymas apie asmens kodo naudojimą policijos procesiniuose dokumentuose manyčiau, kad ADTAĮ įstatyme turėtų būti aiškiai apibrėžta nuostata, kokias atvejais galima viešai tvarkyti duomenis tokius, kaip asmens kodas. Todėl manyčiau, kad:

- Asmens identifikavimo numeris turėtų būti naudotinas tik tada, kai būtent asmens tapatybės patvirtinimas būtinas,
- Tapatybės atskleidimu nederėtų piktnaudžiauti, todėl turėtų būti įvardijama konkreti atsakomybė,
- Valstybė privalo sudaryti sąlygas individui atskleisti minimalų reikalingą kiekį duomenų apie save, kartu – sąlygas neatskleisti savo tapatybės tada, kai tai nereikalinga ir tik tai kiek yra įmanoma. Galima alternatyva būtų kitų asmens dokumentų numerių fiksavimas ir pan.
- Asmens kodo naudojimas neturėtų automatiškai reikšti kitų konkrečiu atveju nebūtinų duomenų apie asmenį atskleidimo. Nustatant asmens tapatybę, turėtų būti nesvarbi kita asmeninė informacija, pavyzdžiui, asmens amžius, gyvenamoji vieta lytis ir panašiai. Valstybė turėtų sudaryti sąlygas tokios nebūtinos informacijos neatskleisti. Tuo tikslu "išgrynintas" ne tik asmens kodo naudojimas, bet taip pat jo sudarymo tvarka. Sudarant asmens kodą, į jį neturi būti įtraukiama jokia papildoma informacija apie privatų asmens gyvenimą.

Panašios taisyklės ginant žmogaus teises laikomasi daugelyje demokratinių valstybių. Vengrijos Konstitucinio Teismo sprendime tiesiogiai nurodoma, kad į asmens kodą nedera įtraukti jokios papildomos asmeninės informacijos, pavyzdžiui, tautybės, religinės priklausomybės, gimimo datos ar vietos. Prancūzijoje 1980 metais ši taisyklė realizuota identifikacinius numerius susiejant su identifikavimo kortelėmis, o ne su asmenimis; nors praktikoje tokie numeriai ir toliau naudojami nusakant asmens tapatybę, jie yra nesunkiai pakeičiami, nesiejami su kitais privačiais duomenimis. Panašios nuostatos laikomasi ir Portugalijoje.

Atsižvelgdami į tai, kad asmens kodas yra itin svarbūs duomenys, duomenų valdytojai, o tuo pačiu ir policijos įstaigos bei draudimo bendrovės savo informaciniuose registruose tvarkydami asmens duomenis, privalėtų atsižvelgti į pagrindinius duomenų tvarkymo principus, kurie yra nustatyti ADTAĮ 3 straipsnyje.

Besiplečiantis asmens kodo naudojimas ir jo pagrįstumas kelia didelį susirūpinimą žmogaus teisių apsaugos požiūriu. Nors asmens kodo paskirtis identifikuoti ir autentifikuoti asmenis, tačiau jame slypi su asmeniu susijusi privati informacija, kurios naudojimas yra, tiksliau – turėtų būti apribotas iki minimumo. Be to, turėti vienintelį identifikantą kiekvienam individui būtų neapsakomai patogu tai paverstų duomenų surinkimą, laikymą ir naudojimą efektyvesniu, tačiau kaip tik toks disponavimo išsamiais įrašais paprastumas išplečia invazijos į privatumą mastą.

Galiausiai kiekvienas duomenų tvarkymo žingsnis turi būti atskirai nuodugniai apsvarstytas. Antra vertus, žmonės turėtų priešintis šiam nepagrįstam asmens duomens paviešinimui.

2.5. Teisė į informaciją tvarkant duomenis viešose duomenų rinkmenose

Policijos institucijose tvarkomos rinkmenos priklauso viešajam sektoriui, todėl diegiant naujausias technologijas valdžios institucijose, o taip pat ir policijos įstaigose atsiranda ir galimybės teikti viešąsias elektronines paslaugas piliečiams. Institucijų viešosios paslaugos – terminas "viešosios paslaugos" yra vartojamas plačiąja prasme ir apima visą gyventojo ar verslo subjekto bendravimą, pavyzdžiui, paklausimą ir atsakymą į paklausimą, įvairių dokumentų užpildymą ir pateikimą, atsiskaitymus ir kita.[58]

Įgyvendinant elektroninės valdžios koncepciją bei siekiant gerinti policijos ir visuomenės bendradarbiavimą, Policijos departamento interneto svetainėje pateikiama visuomenei naudinga informacija, sudarytos galimybės asmenims interneto svetainėje pateikti jiems rūpimus klausimus, atsakymai pateikiami šalia pateikto klausimo.

Deja, dėl lėšų ir kvalifikuotų specialistų, kurie administruotų policijos įstaigų interneto svetaines, trūkumo tokių galimybių šiuo metu nėra daugelyje policijos įstaigų. Nors pastaruoju metu daugelis policijos įstaigų pradėjo kurti savo interneto svetaines, dauguma šių svetainių neatitinka Lietuvos Respublikos Vyriausybės 2003 m. balandžio 18 d. nutarimu Nr. 480 patvirtintų Bendrųjų reikalavimų valstybės institucijų interneto svetainėms nuostatų.[59] Nežiūrint į tai, policijos interneto svetainėse pastaruoju metu yra skelbiama daug informacijos.

Lietuvos Respublikos policijos veiklos įstatymo 6 str. teigiama, kad asmens prašymu Vyriausybės nustatyta tvarka policija privalo pateikti savo informacinėse sistemose turimus neslaptus duomenis apie asmenį. Įstatyme taip pat numatyti ir keli šio principo apribojimai. Pavyzdžiui – pirmas, draudžiama asmenims teikti informaciją apie kitus asmenis, jeigu įstatymai bei kiti teisės aktai nenustato kitaip. Antras – policija neteikia informacijos, kuri pažeistų asmens nekaltumo prezumpcijos principą, policijos etikos normas, asmens, visuomenės ar valstybės saugumo interesus.[60]

Lietuvos Respublikos visuomenės informavimo įstatymo 14 straipsnis[61] numato, kad rengiant ir platinant viešąją informaciją, privaloma užtikrinti žmogaus teisę į tai, kad būtų gerbiamas jo asmeninis ir jo šeimos gyvenimas. Informacija apie privatų gyvenimą gali būti skelbiama be

---

[58] Elektroninės valdžios koncepcija patvirtinta Lietuvos Respublikos Vyriausybės 2002 m.
[59] Lietuvos policijos ryšių su visuomene koncepcija, patvirtinta Lietuvos policijos generalinio komisaro 2005 m. gegužės 17 d. įsakymu Nr.5-V-317 „Dėl Lietuvos policijos ryšių su visuomene koncepcijos patvirtinimo"
[60] Jurisprudencija, 2002, t. 36(28); 13–24 Socialiniai pokyčiai ir policijos subjektiškumas Doc. dr. A. Urmonas
[61] Lietuvos Respublikos visuomenės informavimo įstatymas//Valstybės žinios 1996, Nr. 71-1706

žmogaus sutikimo tais atvejais, kai informacijos paskelbimas nedaro žalos asmeniui arba kai informacija padeda atskleisti įstatymų pažeidimus ar nusikalstamas veikas, taip pat kai informacija yra pateikiama nagrinėjant bylą atvirame teismo procese.

Viena iš viešosios paslaugos policijoje galima įžvelgti ir Vilniaus mieto Vyriausiojo policijos komisariato (toliau –VPK) internetinio tinklapio įdiegimą.[62] Sukurtame tinklapyje gausu naujausios informacijos piliečiams rūpimais klausimais: tarnybos funkcijos, policijos struktūra, padaliniai, kontaktai, bei kita aktuali informacija. Tinklalapyje įkurta tam tikra forumo nuoroda, kur visi suinteresuoti asmenys gali viešai uždavinėti klausimus ir gautų į juos viešus atsakymus, kuriuos galėtų matyti ir perskaityti ir kiti besidomintys.

Galima būtų padiskutuoti, ar interneto svetainė yra „visuomenės informavimo priemonė“. Vadovaujantis Visuomenės informavimo įstatymo 2 straipsnio 40 dalimi, visuomenės informavimo priemonės yra „knygos, laikraščiai, žurnalai, biuleteniai ar kiti leidiniai, televizijos, radijo programos, kino ar kita garso ir vaizdo studijų produkcija ir kitos priemonės, kuriomis platinama informacija“. Internetas galėtų būti laikomas tokiomis kitomis priemonėmis. Šio įstatymo kontekste internetas nėra „visuomenės informavimo priemonė“, nors dėl to nėra galutinai apsispręsta. Vėlgi reikia pabrėžti, kad 8 straipsnio privilegija priklauso nuo tikslo, o ne nuo visuomenės informavimo priemonės, kuria yra platinama informacija.

2004 metais sostinės policija savo internetiniame tinklalapyje pradėjo skelbti informaciją apie sulaikytus neblaivius vairuotojus skyrelyje "*Jie vairavo neblaivūs*". Tokios prevencinės priemonės nuspręsta imtis siekiant sudrausminti neblaivius vairuotojus ir išvengti avarijų. Statistika rodo, kad girtų vairuotojų sukeltų sunkių avarijų skaičius pastaruoju metu išaugo 20 proc. 2005 metais iki spalio 25 d. nustatyti 2324 asmenys, kurie vairavo transporto priemones būdami neblaivūs. Spalį vyksiančios akcijos metu (spalio 1 iki 25 d.) nustatyti 147 neblaivūs vairuotojai vien tik Vilniaus mieste.[63] Panaši situacija yra ir kituose miestuose bei visoje šalyje. Kauno eismo priežiūros pareigūnai ligi šiol prisimena kaunietį G.V, kuris per pusantrų metų būdamas neblaivus prie vairo įkliuvo apie 10 kartų ir už įvairius kelių eismo taisyklių pažeidimus vyrui skirta beveik 40 tūkstančių litų baudų, kurių jis ligi šiol nesumokėjo.

Tinklapyje šiuo metu skelbiami asmens duomenys[64] asmenų kurie vairavo automobilius būdami neblaivūs.

„Tikimės, kad viešumas padės sutramdyti girtus vairuotojus“, – sakė Vilniaus miesto eismo priežiūros tarnybos administracinės veiklos skyriaus viršininkas E. Tučis[65] palaikęs idėją panaudoti

[62] http://www.policija.lt/sostine/ prisijungimo laikas: 2005-10.07
[63] Vilniaus m. VPK informacija http://www.policija.lt/sostine/ prisijungimo laikas: 2005-10.28
[64] Skelbiami duomenys: pavardė gimimo metai ir aplinkybės kuriomis piliečiai „įkliuvo“ vairuojantys transporto priemones neblaivūs bei paskirtos administracinės nuobaudos dydis

tokią prevencijos priemonę prieš įstatymus laužančius asmenis[66]. Tai pagrindinė priežastis kuri priverčia sostinės policijos interneto svetainėje skelbti neblaivių vairuotojų pavardes. Policijos interneto svetainėse pateikiama informacija apie asmens padarytą teisės pažeidimą, yra susiejama su žmogaus asmeniu, t.y. nurodant vardą ir pavarde bei gimimo metus. Siekiant pusiausvyros tarp teisės į privatumą ir asmens duomenų apsaugos ir visuomenės teisės gauti viešojo sektoriaus duomenis, susiduriama su teisės normų dviprasmybe.

Asmens duomenų skelbimas interneto tinklapyje be duomenų subjekto sutikimo būtų galima įžvelgti kaip akivaizdų kišimasis į žmogaus asmeninį gyvenimą, tačiau visa tai daroma su tikslu kuriuo siekiama pristabdyti sparčiai plintantį šių pažeidimų skaičių, be to, tokios rūšies prevencija manytina yra svarbus atviros pilietinės visuomenės bei demokratijos valstybės komponentas. Galima būtų suabejoti, ar teisinis reglamentavimas dėl asmens duomenų tvarkymo viešajame sektoriuje ir ypač valstybės informacinėse sistemose, yra tobulas. Tikslo nustatymo principas ADTAĮ reikalauja, kad asmens duomenys būtų renkami konkrečiais, aiškiais bei teisėtais tikslais ir vėliau tvarkomi su šiais tikslais suderintais būdais[67]. Šiuo atveju policijos pareigūnai sulaikę neblaivų teisės normas pažeidusį asmenį patraukia jį atsakomybėn tvarkydama jo asmens duomenis, susijusius su visuomenės saugumu. Tolesnis duomenų tvarkymas, asmens duomenų skelbimas jau visas veiksmas. Ar gali būti duomenys naudojami kitu tikslu, nepaisant pradinio tikslo?

Lietuvos Respublikos administracinių teisės pažeidimų kodekso 6 straipsnis kaip tik ir kalba apie administracinių teisės pažeidimų prevencija į kurią įtraukta ir policija[68]. Policijos įstatymo 9 straipsnio 2 dalyje apibrėžia būtinybę informuoti piliečius apie daromus teisės pažeidimus visuomenės informavimo priemonėse[69].

Lietuvos Respublikos Konstitucinis Teismas, 1995 m. balandžio 20 d. nutarime konstatavo, kad „galimybė kiekvienam žmogui laisvai formuoti savo nuomonę ir pažiūras ir laisvai jas skleisti bei būti informuotam – būtina sąlyga demokratijai sukurti ir išsaugoti[70]. Šiuo atveju ir galimybė teisėtvarkos griežtinimui bei pažeidimų bei nusikaltimų prevencijai.

Saugodama žmonių teises policija pirmiausia turi rūpintis prevencija, užkirsti kelią įvairiems teisės pažeidimams bei nusikaltimams ir socializuoti potencialius teisės pažeidėjus. Neveltui dar

---

[65] Lietuvos rytas „Policija girtuoklius pristatė prie gėdos stulpo“ 2004-12-23

[66] LR ATPK 126 str. numato baudą iki 3000 lt su/arba teisės vairuoti atėmimą.

[67] Smulkiau žr. Direktyvos 95/46/EB 6(1b) straipsnį

[68] LR ATPK 6sr. Valstybiniai organai, visuomeninės organizacijos, darbo kolektyvai rengia ir įgyvendina priemones, kuriomis siekiama užkirsti kelią administraciniams teisės pažeidimams, išaiškinti ir šalinti priežastis bei sąlygas, padedančias juos padaryti, auklėti piliečius, kad jie būtų didžiai sąmoningi ir drausmingi, griežtai laikytųsi įstatymų.

[69] Policijos įstatymo 9 str. 2 dalis. Policija gali steigti visuomenės informavimo priemones, kuriose visuomenei būtų teikiama informacija apie nusikalstamų veikų ir kitų teisės pažeidimų prevencijos priemonių, kitų policijos uždavinių įgyvendinimą bei skelbiama kita su policijos veikla susijusi informacija.

[70] Lietuvos Respublikos Konstitucinio Teismo 1995 m. balandžio 20d. nutarimas //Žin., 1995, Nr. 34-847

1995 m. gruodžio 6 d. Strasbūre vykusiame seminare „Policija ir žmogaus teisės“ buvo pabrėžta, kad profilaktinė teisės pažeidimų veikla yra aukščiausia žmogaus teisių apsaugos forma. Tam pritaria ir prof. A. Pumputis teigdamas, jog profilaktinė veikla labiau nei kokia nors kita policijos funkcija užtikrina žmogaus teises[71]. Ir tai, be abejo, suprantama, nes vykdant policijos prevencinę veiklą kiekvienas užkardytas teisės pažeidimas garantuoja visas žmogaus teises.

Asmuo darydamas nusikalstamas ar kitas priešingas teisei veikas, neturi ir negali tikėtis pilno privatumo. Teisė kildinama iš teisių ir pareigų sintezės, išreikštos teisių ir pareigų vienovės. Tai, jog teisė į privatumą nėra absoliuti, ne kartą yra pasisakęs ir LR Konstitucinis Teismas, priešpastatydamas ją tam tikromis kitoms šalies pareigoms. Žmogaus privataus gyvenimo apsaugos ribos baigiasi tada, kai jis savo veiksmais nusikalstamai ar kitaip neteisėtai pažeidžia teisės saugomus interesus, daro žalą atskiriems asmenims, visuomenei ir valstybei. Policijos įstaigoms, kurios pareiga yra užtikrinti kiekvieno individo teises ir laisves, ne visada pavyksta vienu metu suderinti asmens bei visuomenės interesus. Dėl šios priežasties valstybė, nenorėdama pažeisti pusiausvyros tarp asmeniui garantuotų (laiduotų) teisių ar laisvių bei visuomenės interesų, yra priversta ieškoti būdų, kaip suderinti asmens ir visuomenės interesus. Vienas tokių interesų derinimo būdų ir yra asmens teisių ribojimas vardan viešojo intereso ar teisėto tikslo. Tokių apribojimų leistinas ribas nulemia santykis tarp saugomų vertybių bei tuo metu valstybėje galiojančių teisinių vertybių prioritetų. Aptariamu atveju visų asmenų teisė į saugumą kelyje tiesiogiai susijusi su valstybės pareiga ją užtikrinti, įskaitant efektyvią teisės pažeidimų prevenciją. Todėl teisė į asmens privatumą negali būti suabsoliutinta ir ypač viešuose informaciniuose registruose kai atsikirta nuo šios valstybės pareigos ypač paskutinių pažeidimų didėjimo kontekste. Kitą vertus Direktyvos 12 straipsnio b dalis visada užtikrina duomenų subjekto teisę reikalauti, kad duomenų valdytojas tinkamai ištaisytų, ištrintų duomenis kurie tvarkomi nesilaikant direktyvos nuostatų, o ypač kai jie netikslūs.

2.6. Informacinių sistemų priežiūra

Policijos tikslai - suprantami kaip visuma apimanti visas užduotis, kurias policijos organai privalo atlikti nusikaltimų prevencijos viešosios tvarkos palaikymo tikslais, tuo tarpu „atsakinga institucija” (rinkmenos valdytojas) reiškia instituciją, kuriai nacionaliniai įstatymai suteikia kompetenciją priimti sprendimą dėl asmens duomenų, kurie turi būti saugojami apsaugos bei dėl

[71] Dr. G. Danišauskas. Policijos prevencinė veikla- jos teisinio paslaugavimo visuomenei turinio elementas // Jurisprudencija 2002, t. 31(23); 46–52

operacijų, kurios turi būti su jais atliekamos. Policijos departamentas operatyvinės veiklos tikslu renka, kaupia, apdoroja ir naudoja informaciją, naudodamas specialios paskirties sistemas.

Direktyva 95/46/EB įpareigoja valstybes nares paskirti nepriklausomas institucijas, atsakingas už duomenų apsaugos kontrolę bei numatyti sankcijas už asmens duomenų apsaugos pažeidimą. Kiekviena valstybė turėtų turėti nepriklausomą priežiūros instituciją, kuri būtų atsakinga už nustatytų principų laikymosi užtikrinimą. Priežiūros institucija turėtų būti informuojama apie ilgalaikes automatizuotas rinkmenas. Priežiūros institucijų steigimą nustato ir Konvencijos dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu papildomas protokolas (Nr. 181)[72]. Pagal jo nuostatas taip pat reikalaujama, kad priežiūros institucija būtų visiškai nepriklausoma. Žodis „visiškas“ pabrėžia visuotino nepriklausomumo svarbą.

Duomenų apsaugos priežiūrą, išskyrus asmens duomenų tvarkymą visuomenės informavimo tikslais, Lietuvoje vykdo Valstybinė duomenų apsaugos inspekcija. ADTAĮ 29 straipsnis nustato bendruosius priežiūros institucijos steigimo principus. VDAI veiklos teisinius pagrindus bei principus, funkcijas bei teises nustato ADTAĮ 30-32 straipsniai.

VDAI išleido duomenų apsaugos plėtojimo 2002–2004 m. programą[73], taip pat Informacijos technologijų saugos valstybinę strategiją ir jos įgyvendinimo planus[74]. Jose atkreipiamas dėmesys į tai asmens duomenų apsaugos priežiūra susijusias funkcijas. Pagrindiniai šios programos tikslai yra duomenų apsaugos sistemos Lietuvoje plėtra ir visiška duomenų apsaugos lygio atitiktis Europos reikalavimams.

Svarbiausieji Inspekcijos veiklos tikslai yra prižiūrėti asmens duomenų valdytojų veiklą tvarkant asmens duomenis, kontroliuoti asmens duomenų tvarkymo teisėtumą, kovoti su duomenų tvarkymo pažeidimais bei užtikrinti duomenų subjekto teisių apsaugą. Kiekvienas duomenų subjektas turi teisę kreiptis į priežiūros instituciją, jeigu mano, kad jo duomenis tvarkantis duomenų valdytojas pažeidė jo teises. Priežiūros institucija turi panašias funkcijas kaip kontrolierių įstaiga. Be to, ši institucija turi padėti užtikrinti duomenų subjekto duomenų tvarkymo skaidrumą.

Be VDAI policijos įstaigų kontrolę vykdo Vidaus reikalų ministerija kuri atlieka valstybės institucijų informacijos technologijų saugos įvertinimus. Vidaus reikalų ministras 1999 m. gegužės 25 d. įsakymu Nr. 343 patvirtino reikalavimus „Dėl Vidaus reikalų ministerijos centrinio duomenų banko naudotojų įregistravimo ir išregistravimo tvarkos“, kurių privalo laikytis CDB duomenų naudotojai. Vidaus Reikalų Ministras 2005 m. kovo 9 d. įsakymu Nr. 1V-68 patvirtino VRIS CDB duomenų peržiūrimos kontrolės taisykles.

---

[72] Papildomą protokolą Lietuva ratifikavo 2004 m. liepos 1 d.

[73] patvirtinta Valstybinės duomenų apsaugos inspekcijos direktoriaus 2002 m. vasario 26 d. įsakymu Nr. 01-10-01 (Žin., 2002, Nr. 23-871)

[74] patvirtinti Lietuvos Respublikos Vyriausybės 2001 m. gruodžio 22 d. nutarimu Nr. 1625 (Žin., 2001, Nr. 110-4006)

Pagal vidaus reikalų ministro aukščiau paminėtą įsakymą už policijos pareigūnų VRM CDB naudojimo teisėtumą bei tikslingumą atsakingi policijos komisariatų vadovai bei VRM ir jos struktūrinių padalinių vadovai bei kontrolę vykdo Informatikos ir ryšių departamento Informacinių sistemų administravimo ir priežiūros skyrius. Galima būtų suabejoti ar policijos komisariatų vadovai pakankamai yra pasiruošę ir sugeba interpretuoti plačias bendro ADTAĮ normas bei išmano asmens duomenų apsaugos subtilybes, todėl tokią veiklą riekėtų patikėti informacinės sistemos saugos įgaliotiniams kurie yra šios srities specialistai.

Vidaus reikalų ministras, kurio kompetencijoje yra informacinių technologijų saugos koordinavimas valstybės institucijose ir įstaigose, patvirtino Informacinių technologijų saugos atitikties vertinimo metodiką ir duomenų saugos įgaliotinį įvardijo kaip vertintoją, kuris rengia informacinių sistemų saugos atitikties vertinimo ataskaitą ir teikia ją įstaigos vadovui. Šis organizuoja trūkumų šalinimo priemonių planą, atsako už saugumo politikos įgyvendinimą ir kontrolę. Galime kelti klausimą dėl atsakingojo už duomenų apsaugą ir duomenų saugos įgaliotinio funkcijų derinimo bei atsakomybės teisinio reglamentavimo.

Vidaus reikalų ministerijos ministro įsakyme[75] numatė, kad sistemos tvarkytojo sprendimu saugumo politikai įgyvendinti ir saugumo kontrolei užtikrinti įstaigose gali būti steigiamas atskiras padalinys. Toks padalinys galėtų būti nepriklausomą audito grupė susidedančią iš informacinės sistemos saugos įgaliotinių, o tuo pačiu VRS įstaigų darbuotojų kuri galėtu pastoviai atlikinėti nepriklausomą informacinių sistemų auditą, teikti rekomendacijas policijos įstaigų vadovams informacijos saugumo ir duomenų tvarkymo policijos įstaigose klausymais, bei sudaryti sąlygas saugiai automatizuotu būdu tvarkyti duomenis policijos registruose ar kitose informacinėse sistemose.

Šiuo metu galima būtų suabejoti, ar policijos informacinių sistemų duomenų saugumo ir apsaugos teisinis reglamentavimas yra efektyvus ir tinkamai vykdomas. Informacinės sistemos saugos įgaliotinai tik formaliai vykdo savo funkcijas, o efektyvi sistemų priežiūra nevykdoma. Teisės aktuose nėra įteisinta ir tokia kategorija kaip asmens duomenų saugos įgaliotinio kuris betarpiškai būtų atsakingas už asmens duomenų apsaugą.

Nei pilietis, nei valstybė nebus saugūs kol jų teisės asmens duomenų apsaugos srityje nėra pakankamai neužtikrintos. Įstatymuose ir reglamentuose yra gana daug spragų, o jei tokie įstatymų reglamentai net ir yra, jie yra nevykdomi, o jeigu vykdomi, nepakankamai preciziškai ir iš esmės kontrolės sistemos šioje srityje nėra. Todėl policijos įstaigų kontrolei reiktų vieningos sistemos bei pastoviai atliekamo audito sistemos šioje srityje.

---

[75] Vidaus reikalų ministerijos Ministro 2003 07 16 d. įsakymas Nr. 1V-272 Dėl Tipinių duomenų saugos nuostatų patvirtinimo// Valstybės žinios,2003, Nr. 76-3511

3. ASMENS DUOMENŲ TVARKYMAS VAIZDO STEBĖJIMO PRIEMONĖMIS

3.1. CCTV sistemos ir jų atsiradimo prielaidos

Šiame skyriuje panagrinėsiu vaizdo stebėjimų kamerų (CCTV) panaudojimo viešose vietose atvejus siekiant užtikrinti visuomenės saugumą ir įvertinti jų naudojimo privalumus bei trūkumus asmens duomenų teisinės apsaugos srityje.

Prieš trisdešimt metų Didžiojoje Britanijoje pradėtos steigti viešųjų ir privačių teritorijų vaizdo stebėjimo sistemos pastaraisiais metais paplito visame pasaulyje, neaplenkdamos ir Lietuvos. Pastaruoju metu vis daugiau institucijų, įmonių ir organizacijų tokias sistemas įrengia viešose vietose: gatvėse, visuomeniniuose ir visuomenės lankomuose pastatuose, prekybos vietose, stadionuose. Ši aplinkybė sukėlė gyvus debatus Sąjungos lygyje ir atskirose šalyse, dėl būtinų sąlygų ir apribojimų, taikytinų vaizdo stebėjimo prietaisų įrengimui, ir būtinos duomenų subjektų apsaugos nustatymo.

Per pastaruosius metus sukaupta patirtis ir Direktyvos 95/46/EB perkėlimas į nacionalinį lygmenį parodė, kad labai padaugėjo uždarų sistemų, kamerų ir sudėtingesnių prietaisų, kurie yra naudojami įvairiausiose sferose. Gyvenimas formuluoja pagrindinę problemą: ar panaudojamos visos galimybės ir priemonės ir ar jos yra efektyvios, kad visuomenės saugumo būklė būtų ne blogesnė, nei yra pastaruoju metu ir ar pakankamai užtikrintos duomenų subjektų teisės šioje srityje. Visuomenės saugumo užtikrinimas yra kompleksinė visuomeninio gyvenimo sritis, kurios valdymo efektyvumą lemia valstybės gebėjimas taikyti šiuolaikinius visuomenės poveikio instrumentus. Deja, ne visi visuomenės poveikio instrumentai (pvz., finansiniai, materialiniai, žmogiškieji ištekliai) yra efektyvūs ir gali užtikrinti teigiamą rezultatą. Ieškoma naujų ir novatoriškų žmonių saugumo užtikrinimo priemonių ir būdų, galinčių sumažinti teisės pažeidimų viešose vietose riziką. Vienas tokių būdų – technologinių priemonių, t. y. vaizdo stebėjimų kamerų (CCTV) ir kitų saugumo „produktų“ panaudojimas užtikrinant visuomenės saugumą. Daugelyje Vakarų Europos valstybių (Vokietijoje, Prancūzijoje, Didžiojoje Britanijoje ir kt.) miestuose siekiant sumažinti padaromų nusikaltimų ir kitų teisės pažeidimų skaičių viešose vietose jau keleri metai naudojamos centralizuotos vaizdo stebėjimo kamerų sistemos.

Saugios visuomenės kūrimas glaudžiai siejasi su pilietine visuomene, kurios pagrindinis tikslas – ieškoti, rasti ir aiškiai įvardyti bendras vertybes ir bendrus interesus. Užtikrinant visuomenės saugumą tenkinami atskiro individo saugumo poreikiai. A. Pumputis pripažįsta, kad

saugumo poreikio įgyvendinimas „priklauso nuo visuomenės ekonominės-socialinės aplinkos“[76]. Vadinasi, saugumo poreikis atsispindi socialinėje aplinkoje (šeimoje, gyvenamojoje vietovėje, mokykloje ar kitame bendruomenės junginyje), kurioje pasireiškia pagrindiniai žmonių tarpusavio ryšiai ir kurioje individai nori jausti saugumą bei tvarką.

Visuomenės saugumo problemos laikomos ne vien teisėtvarkos institucijų, bet ir visos bendruomenės rūpesčiu. Vadinasi, gyventojai patys yra įtraukiami aktyviai dalyvauti kuriant saugią gyvenamąją aplinką, ugdomas pilietinės atsakomybės už bendruomenės reikalus jausmas. Teisėtvarką užtikrinančių ir kitų institucijų, atsakingų už viešosios tvarkos ir visuomenės saugumo politikos formavimą, veiklos orientyras turėtų būti ne tik nusikaltimų, bet ir visų teisėtvarkos pažeidimų prevencija. Vadinasi, reikia surasti tinkamų priemonių, kurių dėka būtų sėkmingai užtikrinamas kasdieninis žmonių bei visuomenės saugumas. Viena tokių priemonių galėtų tapti vaizdo stebėjimo kamerų (CCTV) panaudojimas viešosiose ir kitose gyventojų dažniausiai lankomose vietose.

Tiek valstybinių, tiek savivaldybių, tiek privačių institucijų ar net pačios bendruomenės esmine problema tampa siekis sumažinti teisės pažeidimo riziką, t. y. stengiamasi ieškoti tokių saugumo užtikrinimo būdų ir priemonių, kad būtų galima saugiai jaustis gyvenamojoje aplinkoje. Daugelis žino, kad blogai apšviestose gatvėse lengviau daryti smurtinius nusikaltimus, nesant policijos pareigūnų viešose vietose apiplėšiami automobiliai, įstaigos arba organizacijos. Neįrengus vaizdo stebėjimų kamerų sunku įvertinti padarytą teisės pažeidimą ir surasti teisės pažeidėjus. Minėtieji rizikos veiksniai skatina individą dalyvauti užtikrinant savo ir kitų asmenų saugumą, o valstybę – sudaryti palankias sąlygas visuomenės saugumui užtikrinti. Vadinasi, valstybė privalo užtikrinti teisės pažeidimų prevenciją.

Viena dažniausiai naudojamų teisės pažeidimų prevencijos priemonių tampa vaizdo stebėjimo kamerų (CCTV) įrengimas viešose vietose. Reikia pažymėti, kad šios priemonės naudojimas visuomenės saugumo tikslais yra naujas mūsų valstybėje, tačiau gana plačiai taikomas privačioje saugumo užtikrinimo praktikoje. Būtent sparčiausiai saugos paslaugos įsigalėjo privačių asmenų bei jų turto apsaugos techninėmis priemonėmis srityje. Privačios saugos tarnybos, siekdamos kuo efektyviau užtikrinti savo klientų bei jų turto saugumą, kelerius metus naudoja vaizdo stebėjimo kameras ir turi sukaupusios nemažą patirtį šioje srityje. Vaizdo stebėjimo kamerų sistemos yra įrengtos prie didžiausių šalies prekybos ir pramogų centrų, t. y. tose vietose, kur dažniausiai lankosi gyventojai. Pavyzdžiui, šiuo metu viena tobuliausių vaizdo stebėjimo kamerų sistemų, administruojamų privačios saugos tarnybos, yra įrengta prekybos ir pramogų centre „Akropolis“. Ji

[76] Pumputis A. Poreikių ir žmogaus teisių sistemos klausimu // Jurisprudencija: Mokslo darbai. – Vilnius: Lietuvos teisės akademija, 2000. T. 15 (7). 62 psl.

leidžia gyventojams, atvykusiems į šią vietą, jaustis gana patogiai ir saugiai, nebijoti dėl savo fizinio bei turtinio saugumo. Vaizdo stebėjimo kamerų dėka ne kartą buvo sulaikyti nusikaltėliai ir smulkūs teisės pažeidėjai, kurie tiek įstaigos viduje, tiek automobilių stovėjimo aikštelėse iš transporto priemonių vogdavo įvairius daiktus. Kita vertus, vaizdo stebėjimo kameras naudoja ir valstybinės institucijos svarbių objektų apsaugai. Pavyzdžiui, Vadovybės apsaugos departamentas prie LR VRM vaizdo stebėjimo kameras naudoja saugoti Prezidentūros, Seimo ir Vyriausybės pastatus bei aplink juos esančią teritoriją. Pastebėta, kad šiose vietose žymiai rečiau įvyksta įvairių teisės pažeidimų, o jeigu įvykdomi kokie nors teisės pažeidimai, tai greičiau galima nustatyti teisės pažeidėjo asmenybę. Vadinasi, vaizdo stebėjimo kameros (CCTV) tampa puikia prevencijos priemone, nes žinojimas, kad įrengtos vaizdo stebėjimo kameros, sudrausmina žmones bei daro įtaką jų elgesiui.

Vaizdo stebėjimo kamerų (CCTV) panaudojimas užtikrinant visuomenės saugumą – nauja prevencijos priemonė, todėl tikslinga nustatyti teisinius bei organizacinius saugos priemonių taikymo standartus. Priešingu atveju galima susidurti teisės normų pažeidimo, žmogaus teisių ir laisvių suvaržymo problema, taip pat vaizdo stebėjimo kamerų (CCTV) efektyvumo ir ekonominės naudos problema.

3.2. Vaizdo apdorojimo sistemos Vilniaus policijoje

Centralizuoto vaizdo stebėjimo kamerų sistemų įdiegimo klausimas Vilniaus mieste yra keliamas jau nuo 1998 metų, kai bendradarbiaujant savivaldybei, policijai ir visuomeninėms organizacijoms buvo pradėtos rengti vietinės prevencijos programos „Saugus senamiestis“, „Saugus Užupis“ ir pan. Būtent vykdant šias prevencijos programas pirmą kartą buvo keliams klausimas dėl vaizdo stebėjimo kamerų naudojimo viešose vietose. Visuomeninių organizacijų pasiūlyta idėja dėl vaizdo stebėjimo kamerų įdiegimo tuo metu nebuvo įgyvendinta būtent dėl finansavimo problemų, nes nei valstybė, nei savivaldybė neskyrė tam pakankamai biudžeto lėšų.

Sekančio etapo metu iniciatyvos ėmėsi privačios saugos tarnybos, pasiūliusios keletą viešojo saugumo problemų sprendimo Vilniaus senamiestyje projektų. 1999 metais vykusiame seminare „Asmens ir turto saugumas Vilniaus senamiestyje“ buvo pabrėžiama, jog privačios saugos tarnybos gali pasireikšti ir nekomercinėje srityje palaikydamos tvarką viešose vietose[77]. Privačios saugos tarnybos siūlė projektą, kurį įgyvendinant į saugos sistemas ir priemones būtų investuojama

[77] Adomaitis J. Saugumo problemos Vilniaus senamiestyje. Galimas saugos tarnybų indėlis // Seminaro „Asmens ir turto saugumas Vilniaus senamiestyje“ pranešimai. - Vilnius, 1999. psl. 52–54

nemažai lėšų. Deja, įgyvendinti idėją vėl sutrukdė finansavimo problemos, nes privačių saugos tarnybų galimybės be savivaldybės finansinės paramos pasirodė menkos.

Vėliau iniciatyvą parodė Vilniaus miesto savivaldybė ir Vyriausiasis policijos komisariatas. Buvo sudaryta bendra šių dviejų institucijų darbo grupė, kurios tikslas – išsiaiškinti, kokiose vietose Vilniaus mieste yra padaroma daugiausiai teisės pažeidimų bei kurios vietos yra nesaugiausios. 2000 – 2002 m. Vilniaus miesto savivaldybė atliko tyrimą, kurio metu nustatyta, jog nesaugiausiomis laikytinos Senamiesčio, Užupio ir Naujamiesčio (šalia stoties) seniūnijų gyvenamosios teritorijos.

Atsižvelgus į tyrimo rezultatus nesaugiausiuose Vilniaus miesto gyvenamuosiuose rajonuose buvo pradėtos rengti vaizdo stebėjimo kameros. 2000 metais Vilniaus savivaldybės ir vyriausiojo policijos komisariato iniciatyva buvo pradėta akcija „saugus miestas“, ir įvairiose miesto vietose imtos diegti vaizdo stebėjimo kameros. Vilniaus miesto VPK duomenimis, šiuo metu Vilniuje veikia 78 vaizdo stebėjimo kameros, kurių vaizdas transliuojamas į VPK būstinę[78]. 30 kamerų yra valdomos, o 48 stebi fiksuotą vaizdą. VPK yra įrengusi vaizdo stebėjimo kameras ir keliuose, kur jos fiksuoja kelių eismo pažeidimus, eismo įvykius, bei padeda išaiškinti iš įvykių pasišalinusius vairuotojus.

3.1 pav. Eismo įvykis užfiksuotas vaizdo stebėjimo sistema

[78]Vilniaus m. VPK duomenys 2005 08 11.



Pirmosios šio projekto dalies metu vilniečiams buvo teikiama informacija apie saugumą miesto seniūnijose ir gatvėse. Antroji jo dalis - vaizdo kamerų įdiegimas Vilniaus mieste. 2002 metų spalio 31 dieną Vilniaus mieste įdiegta 27 vaizdo stebėjimo kamerų sistema.

Nesaugiausios Vilniaus miesto seniūnijos yra Senamiestis, Naujininkai, Šnipiškės ir Naujamiestis, todėl didžioji dalis vaizdo stebėjimo kamerų pirmiausia įrengtos pačios nesaugiausios seniūnijos - Senamiesčio - gatvėse. Kameros sumontuotos Pilies, Aušros vartų, Didžiojoje gatvėse, Rotušės aikštėje ir Geležinkelio stoties aikštėje. Vietos kameroms įrengti pasirinktos atsižvelgiant į daugiametę nusikaltimų, teisės pažeidimų bei labiausiai turistų lankomų vietų analizę. Jau praėjus daugiau kaip dviem mėnesiams po vaizdo kamerų įrengimų, pastebėta, kad tose vietose nusikalstamumas sumažėjo 40 proc.

Nesaugiausios Vilniaus miesto seniūnijos yra Senamiestis, Naujininkai, Šnipiškės ir Naujamiestis, todėl didžioji dalis vaizdo stebėjimo kamerų pirmiausia įrengtos pačios nesaugiausios seniūnijos - Senamiesčio - gatvėse. Kameros sumontuotos Pilies, Aušros vartų, Didžiojoje gatvėse, Rotušės aikštėje ir Geležinkelio stoties aikštėje. Vietos kameroms įrengti pasirinktos atsižvelgiant į daugiametę nusikaltimų, teisės pažeidimų bei labiausiai turistų lankomų vietų analizę. Jau praėjus daugiau kaip dviem mėnesiams po vaizdo kamerų įrengimų, pastebėta, kad tose vietose nusikalstamumas sumažėjo 40 proc.

Kameromis užfiksuotas vaizdas yra perduodamas į Vilniaus m . VPK viešosios policijos operatyvaus valdymo skyriaus įrengtus 12 monitorių, kuriose visą parą stebi įvykius mieste budėtojų poskyrio darbuotojai.

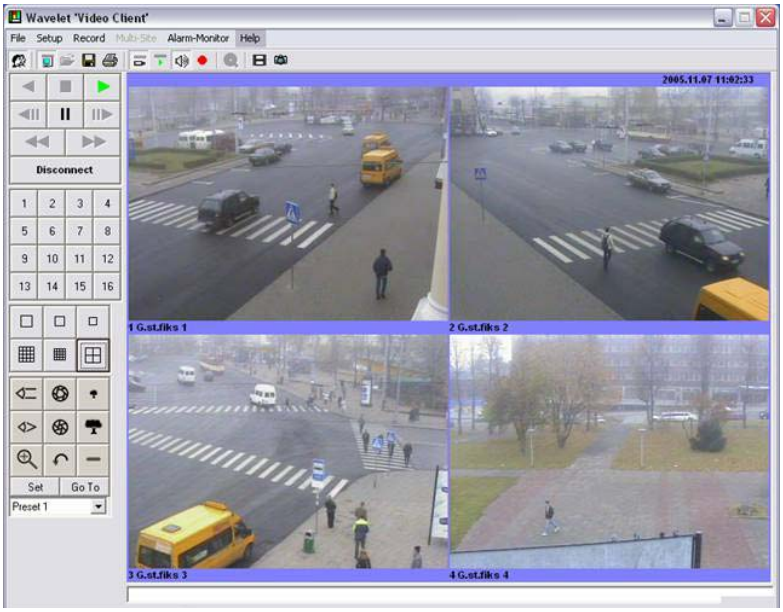
Budėtojo poskyrio darbuotojai, dirbantys prie monitoriaus, bei pastebėję vykdomas ar įvykdytas nusikalstamas veikas, teisės pažeidimus bei kitus įvykius, kurie turi įtakos žmonių gyvybei ir sveikatai ar materialinio turto saugumui, apie tai nedelsdami informuoja atsakingam policijos pareigūnui bei informuoja kompetentingas įstaigas.

3.2 pav. Budėtojų poskyrio patalpa kurioje stebimas vaizdas



Visus pastebėtus įvykius darbuotojas privalo registruoti registracijos žurnale ir, priklausomai nuo įvykio pobūdžio organizuoja reagavimą į pranešimą bei kontroliuoja pranešimo eigą.

3.3 pav. Vaizdas stebimas ir fiksuojamas specialia programa



Vaizdo stebėjimo kameromis užfiksuota informacija yra saugoma Vilniaus m. VPK VP OVS Budėtojų poskyryje skaitmeninėje laikmenoje iki 12 dienų, kad būtų galima panaudoti kaip įrodymą

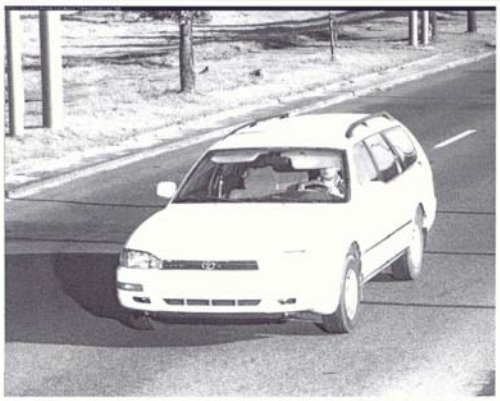
nagrinėjant teisės pažeidimų bylas. Esant būtinumui, asmuo kreipdamasis į Vilniaus m. VPK viršininką, turi teisę susipažinti su jo asmenį liečiančia informacija.

Vaizdo stebėjimo kamerų sistemos viešose vietose efektyvumą, bei veiksmingumą tiek nusikalstamumo prevencijos, tiek nusikalstamų veikų bei kitų teisės pažeidimų išaiškinimo srityje rodo statistinių duomenų analizė: 2003 metais vaizdo stebėjimo kamerų sistemos pagalba buvo užfiksuoti 516 teisės pažeidimai, sulaikyti 676 asmenys, 2004 metais buvo nustatyti 607 teisės pažeidimai ir sulaikyti 753 asmenys. 2005 m. I pusmetį vaizdo stebėjimo kamerų pagalba buvo užfiksuoti 37,8 proc. teisės pažeidimų daugiau negu per 2004 m analizuojamą laikotarpį. Daugiausia buvo nustatyta Kelių eismo taisyklių pažeidimų – 433 (2004 m. – 137). Neginčytina yra tai, kad vaizdo stebėjimo kamerų sistemos viešose vietose įdiegimas bei jos dėka operatyvus informacijos perdavimas didina Vilniaus policijos darbo efektyvumą bei užtikrina galimybę greičiau reaguoti į įstatymų pažeidimus ir juos užkardyti. Taip pat neginčytina ir tai, kad ši sistema turi didelės įtakos nusikaltimų ir kitų teisės pažeidimų išaiškinimui.

Kita asmens duomenų fiksavimo informacinė sistema Vilniaus miesto policijos padalinyje yra automobilių greitį bei vairuotojo atvaizdą bei daromus pažeidimus fiksuojanti sistema.

3.4 pav. Greičio matuoklio „Traffipax SpeedoPho II“ užfiksuotas vaizdas

Greičio matavimo rezultatų protokolas Nr.







Greičio matavimo sistemos gamyklinis Nr.		Pažeidimo vieta	
504-200/60143		Vilniaus m. Laisves pr.	
Pažeidimo data (m. mėn. d.)		**Pažeidimo laikas (val. min. s)**	**Transporto priemonės valstybinis Nr. ženklas**
2004-08-09		083314	AA 32082
Leistinas važiavimo greitis (km/val.)	**Užfiksuotas transporto priemonės važiavimo greitis (km/val.)**	**Matavimo kryptis (artėjanti arba tolstanti transporto priemonė)**	
070	085	Artėjantis transportas	
Kiti pažeidimai			

Pažeidimo medžiagą paruošusio pareigūno pareiginis laipsnis, vardas, pavardė	Parašas
Vilniaus m. VPK VP Eismo priežiūros tarnybos vyresnysis inspektorius	

Transporto priemonės vairuotojo vardas, pavardė, asmens kodas	Parašas

Joje apdorojami asmens duomenys susiję su transporto priemonę vairuojančiu asmeniu. Vilniuje policijos įrengtos greičio kontrolės sistemos fiksuoja ne tik automobilio numerį, bet ir jo vidų, bei keleivių, kurie nenorėtų būti identifikuoti, veidus.

2003 m. rugpjūčio mėnesio UAB „Vildoma“[79] specialistai Vilniaus miesto gatvėse sumontavo stacionarias transporto priemonių greičio matavimo sistemas „TRAFFIPAX Speedo Phot II“ su skaitmeninėmis foto kameromis. Šiuo metu yra įrengtos daugiau nei dešimtyje pagrindinių Vilniaus gatvių, be to, Susisiekimo ministro iniciatyva šių metų spalio mėnesį valstybinės reikšmės magistraliniuose keliuose A1 (Vilnius–Kaunas–Klaipėda) ir A14 (Vilnius–Utena) įrengė stacionarūs greičio matavimo prietaisus, kurie fiksuos leistiną greitį viršijančius vairuotojus ir jų automobilius. Praktikoje yra buvę atvejų, kai kartu su vairuotoju važiavusių asmenų tapatybė buvo atskleista vien dėl to, kad jie sėdėjo šalia kelių eismo taisykles pažeidusio vairuotojo. Kai kuriose Europos valstybėse duomenų apsaugos institucijos griežtai reagavo į tokio pobūdžio pažeidimus nurodydamos policijai, kad sistema, aptinkanti greičio ribojimo pažeidimus, turi filmuoti tik

[79] http://www.vildoma.lt/index.php?page=lt_darbai_radarai_vilnius prisijungimo laikas 2005-07-15.

atitinkamas lenteles, arba automobilį iš galo bet ne transporto priemonės vidų[80]. Vilniaus m. Vyriausiojo policijos komisariato vyriausiojo komisaro 2003 m. spalio 10 d. Įsakyme Nr. 1-V-405 „Dėl stacionaraus automobilių greičio matavimo sistema „Traffipax“ užfiksuotų duomenų apdorojimo taisyklių patvirtinimo“ taisyklėse numatyta, kad užfiksuotas nuotraukas, transporto priemonių keleivių veidai uždengiami, tačiau būdavo atvejų, automobilių vagys ir jų bendrininkai buvo išaiškinti tik vairuotojo ir keleivio atpažinimo dėka.[81]

3.3. Vaizdo stebėjimo sistemų teisinio reguliavimo ir praktikos analizė

Vaizdo stebėjimo veikla, įeina į Konvencijos taikymo sritį. Konvencijos Konsultacinis komitetas konstatavo, kad balsai ir atvaizdai yra laikomi asmens duomenimis, jei jie teikia informaciją apie asmenį, net netiesiogiai sudarantys galimybę nustatyti tapatybę. Garsinių ir vaizdinių duomenų, įeinančių į informaciją apie asmenį, specifinės tvarkymo ypatybės yra išryškintos Direktyvoje 95/46/EB, kurioje apie tai aiškiai kalbama keliuose punktuose. Direktyva užtikrina privatumo ir privataus gyvenimo apsaugą, taip pat ir platesnį asmens duomenų apsaugos diapazoną, atsižvelgdama į fizinio subjekto pagrindines teises ir laisves[82].

Asmens teisė į atvaizdą – viena iš specifinių fizinių asmenų civilinių teisių. Šios teisės įgyvendinimas bei gynimas reglamentuojamas 2001-07-01 įsigaliojusio Civilinio kodekso (toliau - CK) 2 knygos II skyriuje. CK 2.22 str. 1 dalis nurodo pagrindinę šio teisės apsaugos taisyklę: fizinio asmens nuotrauka (jos dalis), portretas ar kitoks atvaizdas gali būti atgaminami, parduodami, demonstruojami, spausdinami, taip pat pats asmuo gali būti fotografuojamas tik jo sutikimu. Reikėtų pažymėti, jog sąvoka „atvaizdas“ apima ne tik asmens nuotraukas, portretus ar kitokius atvaizdus, kuriuose asmuo pavaizduotas, bet ir kūno dalis, iš kurių asmuo gali būti identifikuotas, t.y. atpažintas. Dar daugiau, teisminė praktika parodė, jog asmens teisė į atvaizdą pažeidžiama ir tokiose situacijose, kai asmuo gali būti atpažintas iš nufotografuotų asmens giminaičių ar šeimos narių. Taigi, teisės į atvaizdą apsaugos esmė yra asmens sutikimas, kuris yra būtinas naudojant kito asmens atvaizdą. CK straipsnis nenurodo kokia forma šis asmens sutikimas turi būti gautas. Tad bendruoju atveju tinka visos galimos formos: sutikimas žodžiu, raštu ar konkliudentiniais veiksmais. Asmens neprieštaravimas ir leidimas jį fotografuoti ar kitaip pavaizduoti yra suprantamas kaip sutikimas, išreikštas jo veiksmais.

---

[80] 29 straipsnio – Duomenų apsaugos darbo grupės nuomonė dėl asmens duomenų tvarkymo vaizdo stebėjimo priemonėmis WP 89, 2004 m.
http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2004/wp89_en.pdf; prisijungimas: 2005-08-17

[81] 2003 m. Į Vilniaus m. policiją kreipėsi pilietis su pareiškimu, kad jo automobilis buvo pavogtas. Stacionaraus greičio matuoklio dėka buvo užfiksuotas pavogtas automobilis, o nukentėjusysis atpažino šalia vairuotojo sėdinį savo kaimyną.

[82] Direktyvos 95/46/EB 1str.,1par.

Tačiau vis dėlto reikėtų išskirti du sutikimo tipus: bendrąjį ir specialųjį (arba išimtinį). Bendrasis sutikimas yra toks, kai fotografuojantis asmuo nenurodo tikslo ar neįvardina konkrečių sąlygų, kaip gali būti panaudotas asmens atvaizdas bei to panaudojimo sąlygų. Šiuo atveju galima kalbėti apie modelius, kurių profesija yra tiesiogiai susijusi su jų atvaizdu. Modelis parduoda savo teisę į atvaizdą už sutartą atlygį. Aišku net ir duotas bendrojo pobūdžio sutikimas nesuteikia teisės fotografuojančiam asmeniui panaudoti to asmens atvaizdo asmeniniams ar kitokio pobūdžio neteisėtiems tikslams. Išimtiniame sutikime turi būti asmens sutikimas ir konkrečiai aptartos atvaizdo panaudojimo sąlygos. Dažniausiai šis specialusis sutikimas reikalingas tuo atveju, jei asmens atvaizdas panaudojamas reklamai.

Nė viena subjektinė teisė, taigi ir teisė į atvaizdą, nėra absoliuti. Todėl galimi protingi šios teisės ribojimai. Jeigu asmens fotografavimas ar jo nuotraukų publikavimas yra pateisinamas tam tikru viešuoju interesu, asmens sutikimo nereikia. Pavyzdžiui, teisėti veiksmai, nepažeidžiantys asmens teisės į atvaizdą, yra asmens, darančio nusikaltimą, fotografavimas, dingusio, ieškomo, įtariamo padarius nusikaltimą asmens nuotraukos ar fotoroboto rodymas ir panašiai. Tačiau asmens, kurio, kaip tariamo nusikaltėlio ar įtariamojo, nuotrauka buvo rodoma neturint pakankamo pagrindo jį įtarti, pažeistą teisę į atvaizdą būtina ginti. Pavyzdžiui, motina ir dukra prieš išvykdamos poilsiauti nusifotografavo foto salone. Joms iš jo išėjus darbuotojai pasigedo didelės sumos. Foto salono darbuotojai, manydami, kad pinigus pavogė būtent šios klientės, jų nuotraukas perdavė policijai, o policija, neįsitikinusi kaltinimų pagrįstumu, jas, kaip įtariamųjų vagyste nuotraukas, su atitinkamu prierašu apie nusikaltėlių paiešką išspausdino laikraštyje. Tačiau vėliau paaiškėjo, kad motina ir dukra dėl pinigų dingimo niekuo dėtos. Šiuo atveju pažeista teisė į atvaizdą.[83]

Asmens sutikimo nereikia, jei šie veiksmai yra susiję su visuomenine asmens veikla, jo tarnybine padėtimi, teisėsaugos institucijų reikalavimu arba jeigu fotografuojama viešoje vietoje[84]. Remiantis tarnybine, visuomenine padėtimi be sutikimo gali būti fotografuojami asmenys, pagrįstai sulaukiantys visuomenės domėjimosi – politikai, verslininkai, aktoriai, kiti žymūs žmonės. Tačiau net ir šiais išimtiniais atvejais, tokių nuotraukų ar kitokių atvaizdų negalima naudoti, jei tokiu būdu būtų pažeminta asmens garbė, orumas ar dalykinė reputacija. Minėtos išimtys negali būti laikomos absoliučiomis taisyklėmis. Lietuvos Aukščiausiasis Teismas pabrėžė, kad asmuo, net ir būdamas viešoje vietoje, nepraranda savo privatumo ir individualumo. Todėl būtina atsižvelgti į konkrečią situaciją bei asmens pageidavimą ar sutikimą būti fotografuojamam ar kitaip vaizduojamam. Bet

[83] LAT CBS išplėstinės teisėjų kolegijos 2002 m. vasario 12 d. nutartis c. b. Z.. Karaliūtė v. G. Balionis ir kt., Nr. 3K-7-437/2002, kat. J6.9.
[84] CK 2.22 str. 2 d.

kurioje situacijoje asmuo gali aiškiai ir nedviprasmiškai išreikšti savo nenorą būti fotografuojamam ar filmuojamam.

Jei vis dėlto teisė į atvaizdą buvo pažeista, fizinis asmuo turi teisę teismo tvarka reikalauti nutraukti tokius veiksmus bei atlyginti turtinę ir neturtinę žalą. Po asmens mirties tokį ieškinį turi teisę pareikšti jo sutuoktinis, vaikai ir tėvai[85].

Atskirai reikėtų aptarti neturtinės žalos priteisimą šios teisės pažeidimo atveju. Lietuvos Aukščiausiasis Teismas yra pasisakęs, jog šios teisės pažeidimas nebūtinai reiškia ir neturtinės žalos padarymo faktą. Tam, kad būtų priteista neturtinė žala, asmuo turi įrodyti visas civilinės atsakomybės sąlygas: buvo atlikti neteisėti veiksmai, patirta žala, šiuos veiksmus ir patirtą žalą sieja priežastinis ryšys, kitaip tariant, žala atsirado būtent dėl tų neteisėtų veiksmų, ir, be abejo, turi būti įrodyta neteisėtai atvaizdą panaudojusio asmens kaltė.

Taip pat reikėtų žinoti, jog reikalavimams ginti teisę į fizinio asmens atvaizdą netaikoma ieškinio senatis, t.y. asmens teisės kreiptis į teismą dėl šio pažeidimo neriboja jokie terminai, tačiau dėl patirtos turtinės ir neturtinės žalos atlyginimo asmuo turėtų kreiptis per 3 metus nuo pažeidimo paaiškėjimo dienos.[86]

Reikėtų pažymėti, jog šios teisės apsaugą garantuoja ne tik nacionalinė teisė, bet ir tarptautinė teisė: Lietuva yra ratifikavusi Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvenciją. Šios Konvencijos 8 straipsnio, kuris apima žmogaus teisę į privatų gyvenimą, dalimi yra žmogaus teisė į atvaizdą.

Vilniaus policija informacinėje sistemoje tvarkomiems duomenimis bei vaizdo stebėjimui, vykdomam visuomenės saugumo, gynybos, valstybės saugumo ar valstybinės veiklos kriminalinės teisės sferoje tikslais, vadovaujasi ADTAĮ nuostatomis, bei teisės aktų nustatyta tvarka yra užsiregistravęs[87] kaip asmens duomenų valdytojas, todėl veikla šioje srityje yra teisėta.

Norėčiau paminėti problemą, kurios sprendimas reikalauja nustatyti teisinius vaizdo stebėjimo kamerų (CCTV) naudojimo užtikrinant visuomenės saugumą standartus. Kalbama apie žmogaus teisių pažeidžiamumo problemą. Ne paslaptis, jog įrengus šias kameras viešose vietose galėsime ne tik stebėti daromus teisės pažeidimus ar vykdyti jų prevenciją, bet kartu tarsi „sekti“ kiekvieną pilietį, esantį viešoje vietoje, jam nežinant. Taip pat vaizdo stebėjimo kameras būtų galima nukreipti ne tik į gatves ar kitas viešas vietas, bet ir į piliečių gyvenamuosius būstus ar kitas jų valdas, taip pažeidžiant privatumo ribas. Žmogaus teisių problemos naudojant vaizdo stebėjimo kameras ypač

[85] CK 2.22 str. 3d.
[86] CK 1.125 str. 8 d.

[87] Žr. 1.4 lentelė

aktualios Lenkijos, Vokietijos ir kitose valstybėse, nes riba tarp viešųjų ir privačiųjų interesų šiuo atveju tampa miglota. Valstybei nustačius privalomus teisinius standartus būtų išvengta įvairių teisėtumo pažeidimų, taip pat galėtume pagreitinti vaizdo stebėjimo sistemų įdiegimo viešose vietose procesą bei numatyti subjektų, atsakingų už saugos produktų administravimą bei jų naudojimo kontrolę, kompetencija šioje srityje. Asmens vaizdo duomenų tvarkymui automatiniu būdu ir susistemintų asmens vaizdo duomenų rinkmenų tvarkymui neautomatiniu būdu yra taikomas ADTAĮ, kuriame yra nustatyti bendrieji asmens duomenų tvarkymo principai (3 straipsnis), duomenų subjekto teisės (17–23 straipsniai). Vaizdo stebėjimą atliekantys asmenys (duomenų valdytojai) privalo pranešti Valstybinei duomenų apsaugos inspekcijai apie asmens duomenų tvarkymą (25 straipsnis) ir informuoti duomenų subjektus apie jų asmens duomenų tvarkymą (18 straipsnis). Informuojama galėtų būti matomoje vietoje iškabinant įspėjamuosius ženklus ar informaciją apie vaizdo stebėjimą.

Tvarkymo teisėtumas

Duomenų valdytojas turėtų pasitikslinti, ar stebint laikomasi visų bendrų ir specifinių šitai 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 teisės į atvaizdą arba dėl gyvenamosios vietos apsaugos. Remiantis Direktyvos 95/46/EB nuostatomis, vaizdo stebėjimą atliekantis duomenų valdytojas visų pirma turėtų užtikrinti tvarkymo teisėtumą, taip pat nustatyti aiškius vaizdo duomenų tvarkymo tikslus, kurie turi būti aptarti stebėjimą reglamentuojančiame dokumente. Prieš pradėdamas stebėjimą, valdytojas turėtų įsitikinti, kad numatomi veiksmai atitinka bendrąsias ir specialiąsias šiai sričiai taikomas teisės aktų ir įteisintų elgesio kodeksų nuostatas.

Duomenų valdytojas turėtų atsižvelgti į minėtoje direktyvoje įtvirtintą nuostatą, kad duomenys, susiję su nusikaltimais, asmens teistumais ar valstybės saugumo priemonėmis, gali būti tvarkomi tik tuo atveju, jeigu tai kontroliuoja valdžios institucija arba jeigu užtikrinamos tinkamas saugumo priemones. Duomenų valdytojas vaizdo stebėjimu gali siekti teisėto intereso, tačiau tik su sąlyga, kad duomenų subjekto interesai ar pagrindinės teisės ir laisvės nėra viršesnės. Vaizdo stebėjimo įrangą duomenų valdytojas gali naudoti tik pateisinamais tikslais ir jei kitų apsaugos priemonių aiškiai nepakanka arba jos nepatenkina siekiamų teisėtų duomenų valdytojo tikslų.

Direktyvos 6 straipsnio a) punktas numato, kad duomenų valdytojas turi įsitikinti, kad stebėjimas atitinka bendrąsias ir specifines šiai sričiai taikomas nuostatas – susijusius įstatymus, potvarkius, etikos kodeksus. Reikia imtis visų tinkamų priemonių, užtikrinančių, kad vaizdo stebėjimas atitinka duomenų apsaugos principus ir yra vengiama netinkamo kišimosi į privatų gyvenimą. Šiuo atžvilgiu reikia atkreipti dėmesį, kokie geriausi veiksmai gali būti numatomi, remiantis priežiūros institucijų rekomendacijomis ir kitais savireguliacijos aktais.

Atlikus Lietuvoje galiojančių teisės aktų analizę pastebėta, jog nėra nė vieno dokumento, reglamentuojančio ar net nustatančio įvairių institucijų ir organizacijų teisę naudoti vaizdo stebėjimo kameras (CCTV) visuomenės saugumui užtikrinti. Galima aptikti tik kai kurių viešojo administravimo institucijų visuomenės saugumo užtikrinimo kompetencijos nuorodų. Pavyzdžiui, Vidaus reikalų ministerija, būdama atsakinga už visuomenės saugumo valstybės politikos įgyvendinimo strategijos formavimą ir jos vykdymo organizavimą, koordinuoja pavaldžių institucijų veiklą rengiant ir įgyvendinant nusikaltimų kontrolės ir prevencijos programas, skirtas visuomenės saugumui užtikrinti. Policija, siekdama užtikrinti asmens ir visuomenės saugumą, turi teisę bendradarbiauti su kitomis valstybės bei savivaldybių institucijomis, bendruomene ar pavieniais asmenimis, įgyvendinant nusikalstamumo kontrolės ir prevencijos programas, o jų finansavimas galimas ir iš savivaldybių biudžeto. Savivaldybėms suteikta savarankiška funkcija – dalyvauti užtikrinant visuomenės saugumą, kuri gali būti įgyvendinama kuriant nusikaltimų kontrolės ir prevencijos vietines programas šioje srityje, pasitelkiant savivaldybių teritoriją aptarnaujančias policijos įstaigas bei įtraukiant į šią veiklą bendruomenę.[88]

Minėtas teisiškai įtvirtintas bendro pobūdžio nuostatas reikia vertinti paviršutiniškai (nors jos išplečia užtikrinant visuomenės saugumą dalyvaujančių institucijų galimybes), nes jos neatspindi konkrečių jų įgyvendinimo priemonių, o anksčiau minėtų institucijų gebėjimai ir galimas poveikis saugumui didinti mažai žinomi. Pastaruoju metu iniciatyvos spręsti visuomenės saugumo problemas viešose vietose imasi teritorinės policijos įstaigos bei savivaldybės.

Tyrinėjant vaizdo stebėjimo kamerų (CCTV) panaudojimo garantuojant visuomenės saugumą problemas remtasi Vilniaus miesto patirtimi, nes saugumo būklė šiame mieste yra bene sudėtingiausia. Didžiojoje Britanijoje vaizdo stebėjimo kameros (CCTV) imtos plačiai naudoti tiek privačiame, tiek viešajame sektoriuose 1990 metais. Tam įtakos turėjo nusikaltimų bei teisės pažeidimų viešose vietose skaičiaus didėjimas bei suvokimas, kad šiomis sistemomis galima žymiai sumažinti nusikalstamumą. Pastarąjį dešimtmetį šis sektorius tapo vienu dinamiškiausių ir greičiausiai besiplečiančių Didžiosios Britanijos saugos produktų rinkoje.[89]

Kita vertus, kai kurios Europos valstybės (Didžioji Britanija, Danija, Norvegija ir t. t.) susiduria su teisinių standartų nustatymo problema vaizdo stebėjimo kameras (CCTV) naudojant viešose vietose. Išanalizavus šių valstybių vaizdo stebėjimo kamerų naudojimo praktiką matyti, jog

[88] R. Kalesnykas, V. Mečkauskas. Vaizdo stebėjimo kamerų (CCTV) panaudojimas užtikrinant visuomenės saugumą: teisiniai ir organizaciniai aspektai. Vilnius, LTU 2002.
[89] R. Kalesnykas, V. Mečkauskas. Vaizdo stebėjimo kamerų (CCTV) panaudojimas užtikrinant visuomenės saugumą: teisiniai ir organizaciniai aspektai. Vilnius, LTU 2002.

yra nustatyti tik techniniai standartai, už kuriuos atsakingos privačios įmonės arba asociacijos, veikiančios privačių saugos paslaugų rinkoje.[90]

Vaizdo stebėjimo naudojimo proporcingumas

Vaizdo stebėjimo sistemų panaudojimas turi būti proporcingas siekiamiems tikslams, t.y. jos turėtų būti naudojamos tik tada, kai kitos priemonės nėra pakankamos. Vaizdo stebėjimo sistemos paprastai yra diegiamos teisės pažeidimų prevencijos, apsaugos arba saugumo tikslais. Jeigu šių ar kitų teisėtų tikslų galima pasiekti priemonėmis, kurios nereikalauja vaizdo atkūrimo – pavyzdžiui, jei pakanka įrengti šarvuotas duris ar automatinius vartus, įdiegti jungtinę aliarmo sistemą ar geresnį apšvietimą gatvėse – vaizdo stebėjimo sistemos nenaudotinos. Toks principas yra įtvirtintas ir darbo grupės dokumentuose ir 2003 m Europos Tarybos ekspertų ataskaitoje apie vaizdo stebėjimo kamerų panaudojimą[91]. Todėl Lietuvoje, specialiame teisės akte turėtų būti įtvirtinta nuostata, jog vaizdo stebėjimo sistemas galima diegti tiktai tada, kai kitų, mažiau privatumą ribojančių, priemonių nepakanka. Taip būtų sumažinta piktnaudžiavimų galimybė ir vaizdo stebėjimo sistemos nebūtų diegiamos nežymių pažeidimų kontrolės ir prevencijos tikslais, tokių kaip, pavyzdžiui, rūkymo mokyklose. Didžiojoje Britanijoje prieš įdiegiant vaizdo stebėjimo sistemą, yra privaloma išsiaiškinti ar nėra mažiau privatumą ribojančių priemonių[92]

Verta pabrėžti ir tai, jog teisės akte būtina įtvirtinti nuostatą, įpareigojančią periodiškai įvertinti vaizdo stebėjimo efektyvumą ir taip išsiaiškinti ar tebėra būtinybė naudoti vaizdo stebėjimo įrangą, konkrečioje erdvėje, nes situacija gali keistis. Pavyzdžiui, Olandijoje yra siūloma sugriežtinti teisės aktus dėl vaizdo stebėjimo panaudojimo ir įtvirtinti reikalavimą periodiškai vertinti vaizdo stebėjimo būtinumą ir efektyvumą[93].

2005 m. Didžiosios Britanijos vidaus reikalų ministerijos atliktas tyrimas atskleidė, kad vaizdo stebėjimo kamerų nusikaltimų prevencinė reikšmė toli gražu neatitiko iki tol skelbiamos optimistinės statistikos. 14 skirtingų vietovių atliktas tyrimas parodė, kad vaizdo stebėjimo kameros dažnai neturėjo jokios įtakos nusikaltimų prevencijai, arba nusikaltimų skaičius įdiegus tokias

---

[90] Ten pat.

[91] 2str. „naudoti vaizdo stebėjimo sistemas, jei, priklausomai nuo aplinkybių, tikslas negali būti pasiekiamas priemonėmis, kurios mažiau riboja privatumą <...>“, Europos Tarybos Konvencijos dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108) konsultacinio komiteto dokumentas “Report containing guiding principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance (2003). http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/Documents/Reports/Q-Report%20guiding%20principles%20video.asp prisijungimo laikas 2005-08-15

[92] Viešųjų erdvių vaizdo stebėjimas Europos žmogaus teisių konvencijos kontekste http://www.crimereduction.gov.uk/cctv13.htm prisijungimo laikas 2005-10-01

[93] 29 straipsnio – Duomenų apsaugos darbo grupės nuomonė dėl asmens duomenų tvarkymo vaizdo stebėjimo priemonėmis WP 89, 2004 m. http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2004/wp89_en.pdf; 8-9 psl

kameras netgi padidėjo.[94] Dažniausiai vaizdo stebėjimo kameros turi įtakos tik nereikšmingiems nusižengimams - tokiems kaip šiukšlinimui viešose vietose ir panašiai. Lietuvoje taip pat reikėtų atlikti nepriklausomą išsamų vaizdo stebėjimo kamerų efektyvumo – kaštų tyrimą, kad būtų galima įvertinti ar verta toliau didinti vaizdo stebėjimo kamerų skaičių.

Kamerų išdėstymas

ADTAĮ yra įtvirtinta nuostata, jog asmens duomenys turi būti tik tokios apimties, kuri būtina jiems rinkti ir toliau tvarkyti[95]. Šios, gana abstrakčios sąvokos išsamesnį paaiškinimą galima rasti VDAI direktorės Rekomendacijose duomenų valdytojams dėl etikos kodeksų rengimo, kur teigiama, kad video stebėjimas ir su tuo susijęs duomenų tvarkymas turi būti organizuotas taip, kad į stebėjimo lauką nepakliūtų didesnė nei būtinai reikalinga teritorija (patalpa, ar jos dalis) ar daugiau nei būtinai reikia asmenų[96]. Kitose valstybėse, pavyzdžiui Didžiojoje Britanijoje tai yra imperatyvi nuostata[97], CCTV Praktikos kodekse yra sakoma, kad jei kameros gali būti reguliuojamos operatorių, jos turi būti įrengtos ir pritaikytos taip, kad operatoriai negalėtų jų nukreipti į erdves, kurių stebėjimas nenumatytas, o jei neįmanoma to padaryti, yra reikalaujama, kad operatoriams būtų pravesti apmokymai, kuriuose jie būtų supažindinami su privatumo principais ir jų pažeidimo pasekmėmis. Taip pat yra reikalaujama vaizdo stebėjimo operatorius aiškiai informuoti, jog įrangą galima naudoti tik tiems tikslams, kurie buvo nurodyti ją įdiegiant – pavyzdžiui, jei yra stebimas bankomatas- negalima kameros nukreipti, arba priartinti vaizdą taip, kad būtų galima matyti kortelių „pin“ kodus. Didžiojoje Britanijoje yra nustatomas ir vaizdo kamerų steigėjų ir operatorių santykis su privačių valdų savininkais - pavyzdžiui yra reikalaujama, jog kamerų naudotojas turi pranešti ir pasitarti su privačios zonos savininku, jei pastarojo teritorija ribojasi su stebima zona ir gali patekti į kadrą. Kad konkretus teisinis reguliavimas šioje srityje yra būtinas rodo įvairūs galimi privatumo pažeidimai. Tarkim, kai vaizdo stebėjimo kamerų operatoriai piktnaudžiauja technikos galimybėmis ir nukreipia kameras bei priartina vaizdą taip, kad nesunkiai nustato asmens mobiliųjų telefonu renkamus numerius. O tai yra grubūs teisės į privatų gyvenimą pažeidimai, todėl VDAI turėtų inicijuoti poįstatyminio teisės akto, numatančio konkrečius principus, rengimą, kad tokių pažeidimų nebūtų.

Vaizdų tvarkymas (saugojimas, naudojimas, naikinimas).

---

[94] The impact of CCTV: fourteen case studies. Home Office 2005 http://www.homeoffice.gov.uk/rds/pdfs05/rdsolr1505.pdf prisijungimo laikas 2005-09-07

[95] ADTAĮ 3 str 4 d.

[96] Rekomendacijos duomenų valdytojams dėl asmens duomenų tvarkymo etikos kodeksų rengimo str 18.

[97] CCTV Code of Practice http://www.informationcommissioner.gov.uk/cms/DocumentUploads/cctvcop1.pdf

Remiantis ADTAĮ, duomenų valdytojas yra atsakingas už duomenų saugumą. Jis privalo imtis organizacinių ir techninių priemonių tai padaryti ir jos privalo būti išdėstytos rašytiniame ar jam prilygintos formos dokumente.[98] Duomenų valdytojai, duomenų tvarkytojai ir darbuotojai, kurie tvarko asmens duomenis, privalo saugoti asmens duomenų paslaptį, jei šie asmens duomenys neskirti skelbti viešai. Šios įstatymo sąvokos yra šiek tiek išsamiau paaiškintos VDAI direktorės rekomendacijose dėl etikos kodeksų rengimo, kur teigiama, kad asmens duomenys turi būti laikomi tokia forma, kad duomenų subjektų tapatybę būtų galima nustatyti, kai to reikia tiems tikslams, dėl kurių šie duomenys buvo surinkti ir tvarkomi<...>. Vis dėlto ši, išsamesnė, rekomendacinio pobūdžio nuostata nėra pakankama vaizdo stebėjimo sistemų pagalba gautų duomenų tvarkymo srityje. Konkretus teisės aktas turėtų būti reguliuoti konkrečius būdus dėl vaizdo laikmenose esančios informacijos apie asmenį apsaugojimo. Pavyzdžiui, jei yra teisėtas tikslas paviešinti vaizdo informaciją, ar pakanka juodos juostelės uždengiančios įraše esančio pašalinio žmogaus akis, ar reikėtų padaryti neaiškų/užtemdyti visą žmogaus siluetą. Šios srities reguliavimas ypač svarbus, nes 2003m. byloje *Peck prieš Didžiąją Britaniją* Europos žmogaus teisių teismas nusprendė, kad vaizdo stebėjimo priemonėmis gautos video medžiagos paviešinimas pažeidė asmens privatumo teises, nors ieškovo akys ir buvo uždengtos juoda juostele. Pasak Teismo, nepaisant šios priemonės jis vis tiek buvo atpažintas daugelio žmonių.

Pagal VDAI direktorės rekomendacijas dėl etikos kodeksų rengimo, duomenų valdytojas pats nusistato ilgiausią asmens duomenų laikymo trukmę, tačiau asmens duomenys turi būti saugomi ne ilgiau, nei to reikalauja duomenų tvarkymo tikslai, o leistina asmens duomenų laikymo trukmė vertinama pagal (teisėtą) tvarkymo tikslą.[99] Toks neapibrėžtumas sudaro sąlygas asmens privatumo pažeidimams. Aiškumo dėlei, VDAI turėtų išleisti duomenų saugojimo trukmės gaires vaizdo stebėjimo sistemomis surinktų duomenų valdytojams. Pavyzdžiui Danijos Duomenų apsaugos inspekcija yra nustačiusi, bendrą taisyklę, kad vaizdo stebėjimo įrašai turi būti saugomi ne ilgiau kaip 30 dienų. Didžiojoje Britanijoje CCTV praktikos kodekse maksimali tokių duomenų saugojimo riba nėra nustatyta, tačiau duomenų valdytojų patogumui yra pateikiamos rekomendacijos ir paaiškinimai kiek laiko turėtų būti saugomi skirtingais tikslais surinkti vaizdo stebėjimo duomenys. Pavyzdžiui, rekomenduojama, kad maksimali vaizdų, nufilmuotų miestų centruose ir gatvėse saugojimo trukme neviršytų 28 dienų, išskyrus tuos atvejus, kai jie naudojami kaip įrodymas teisiniame procese[100]. Bankomatų stebėjimo įrašai turėtų būti saugomi ne ilgiau kaip

---

[98] ADTAĮ 24.1 str.
[99] Rekomendacijos duomenų valdytojams dėl asmens duomenų tvarkymo etikos kodeksų rengimo str.12.5, 12.6.
[100] CCTV Code of Practice http://www.informationcommissioner.gov.uk/cms/DocumentUploads/cctvcop1.pdf
28 psl. prisijungimo laikas: 2005-07-18

tris mėnesius, nes tokiu periodu Didžiojoje Britanijoje asmenys gauna sąskaitų išrašus. Taigi, VDAI turėtų imtis iniciatyvos ir nurodyti konkretiems duomenų valdytojams maksimalias duomenų saugojimo ribas, arba inicijuoti bendrą poįstatyminį teisės aktą kuriame tokios duomenų saugojimo ribos būtų nustatytos.

Lietuvoje nėra reglamentuota ir vaizdo duomenų saugojimo forma. Pavyzdžiui, nėra numatyta kas turi teisę patekti į patalpą, kurioje yra monitoriai, transliuojantys vaizdo kamerų filmuojamus vaizdus, arba į patalpą kurioje yra saugomi vaizdo įrašai, kas turi teisę tuos įrašus žiūrėti, o taip pat ir kitos procedūros. Nesant šios srities reguliavimo bei paliekant šiuos klausimus kiekvieno duomenų valdytojo nuožiūrai, pažeidimai neišvengiami. Pavyzdžiui, Didžiojoje Britanijoje yra reikalaujama, jog monitoriai transliuojantys vaizdus iš erdvių, kuriose asmenys tikisi privatumo, turėtų būti stebimi tik tam įgaliotojo asmens, teisė pamatyti įrašus yra apribota iki vadovo ar specialiai paskirto asmens. Reguliuojama ir įrašų peržiūrėjimo tvarka- reikalaujama, kad įrašų peržiūrėjimas vyktų tik uždaroje patalpoje, pavyzdžiui, vadovo ar specialiai paskirto vaizdą stebinčios įstaigos ar organizacijos darbuotojo kabinete, į kurią pateikti neturi teisės niekas kitas.

Informacija duomenų subjektams

ADTAĮ yra teigiama, kad duomenų subjektas turi teisę būti informuotas apie savo asmens duomenų tvarkymą[101]. VDAI direktorės rekomendacijose duomenų valdytojams dėl etikos kodeksų rengimo šis principas yra paaiškintas išsamiau - pagal jį teritorijoje, kurioje vykdomas video stebėjimas, turi būti matomose vietose iškabinta informacija apie tai, kad teritorija yra stebima (pvz. parduotuvėse tokia informacija turi būti aiškiai matoma įeinant į parduotuvę, degalinėse – įvažiuojant į degalinę, o jei tai neįmanoma, prieš pilantis degalus). Pagal Direktyvos 95/46/EB 10 ir 11 straipsnių nuostatas duomenų subjektams turi būti teikiama informacija apie vykdomą vaizdo stebėjimą. Informacija turi būti gerai matoma, išdėstyta tinkamu nuo stebėjimo vietos atstumu ir efektyvi, pvz., tai gali būti simboliai, panašūs į „nerūkoma“. Vaizdo stebėjimo tikslai ir valdytojas visais atvejais turi būti tiksliai apibūdinti. Duomenų subjektai gali naudotis visomis savo teisėmis, taip pat teise nesutikti su tvarkymu, jei tam yra teisinis pagrindas. Bet koks duomenų subjekto teisių ribojimas galimas išimtinai tik įstatymų numatytais atvejais. Duomenų subjektai turi būti informuojami ir turi žinoti, kad vykdomas vaizdo stebėjimas, ir net jei jis susijęs su visuomeniniais įvykiais, renginiais ar reklama. Nėra būtina tikslai nurodyti, kur išdėstyta stebėjimo įranga, tačiau stebėjimo turinys turi būti paaiškintas nedviprasmiškai.

2003 metais VDAI buvo davusi nurodymus Vilniaus miesto VPK policijos vadovams kaip duomenų valdytojams iškabinti informacines lenteles įspėjančias apie asmenų viešą stebėjimą

[101] ADTAĮ 17st.

vaizdo priemonėmis ir informuoti asmenis apie vykdomą stebėjimą. Po minėto rašto lentelės ties įvažiavimu į miestą buvo iškabintos, nuolat pranešama per žiniasklaidą ir asmenys žino kad yra stebimi. Respondentai patvirtino žinantys apie vaizdo kameromis vykdomą stebėjimą. Todėl informavimas (pavyzdžiui, pagal analogiją teismo pranešimams laikraščiuose, prilyginamas tinkamu informavimu), laikytinas tinkamu.

Riedutininkų atlikta apklausa[102] 2005 m. rudenį tai patvirtina. Apklausus daugiau kaip 240 žmonių, išaiškėjo, kad, nors apie viešas vietas stebinčias kameras žino 83 proc. apklaustųjų, tik 31 proc. jaučiasi saugiau. Tuo tarpu dėl vaizdo kamerų nesaugiau jaučiasi apie 13 proc. apklaustųjų. Daugiau kaip pusė respondentų (54 proc.) mano, kad policija, pasitelkusi modernias stebėjimo technologijas, gali pažeisti žmogaus teisę į privatumą, o 60 procentų norėtų, kad vaizdo kamerų stebimose gatvėse būtu iškabinti atitinkami perspėjimai.

3.5 pav. Informacinė lentelė Vilniaus gatvėje



Atkreiptinas dėmesys, į tai, jog ADTAĮ nenumato konkrečių informavimo pareigos būdų ar priemonių. Tokiu būdu VDAI reikalavimas informuoti būtent iškabinant lenteles ir nurodant vietas negali būti laikomas pakankamai teisiškai pagrįstu, kadangi nėra pagrįstas konkrečiomis teisės normomis (kitaip tariant, kaip ir pastebėta įstatymas nėra įvardines informavimo būdų ir priemonių, bei atitinkamai VDAI nėra suteikęs tokių būdų pasirinkimo teisės). Be to, dėl visų asmenų informavimo įstatymo nuostata turi šiek tiek deklaratyvumo, kadangi yra bendro pobūdžio, be to taip ir lieka nešališku, o faktiškai ir itin sunkiai įvykdomu, nes neaišku kokiu būdu turėtų būti informuojamas kiekvienas neregys, turistas iš pakankamai egzotiškų šalių, nesuprantantis lietuvių bei pagrindinių kalbų , vaikai ir pan.

[102] http://www.inlineskating.lt/?m=2#bbwy prisijungimo laikas 2005-10-28

Didžiojoje Britanijoje CCTV praktikos kodekse yra reikalaujama ne tik informuoti asmenis apie vykdomą stebėjimą, bet ir tiksliai nurodoma kokio dydžio turi būti ženklai ir kokia informacija turi būti juose pateikiama. Pavyzdžiui, ženklų dydis gali skirtis priklausomai nuo aplinkybių - ženklas prie įėjimo durų į pastatą gali būti ir A4 formato, jei yra žmogaus akių lygyje, tačiau automobilių stovėjimo aikštelėje esantis ženklas turi būti didesnis- nes į jį bus žvelgiama iš toliau. Taip pat reikalaujama ant ženklų nurodyti asmens ar organizacijos, atsakingos už sistemos įsteigimą tapatybę, stebėjimo tikslą, bei kontaktinę informaciją-kad asmenys žinotų pas ką kreiptis dėl šios sistemos[103]. Taip pat yra svarbu poįstatyminiame teisės akte užtikrinti asmenų teisę gauti su juo susijusią informaciją. Nors ADTAĮ yra teigiama, kad asmuo turi teisę gauti su juo susijusią renkamą informaciją, ši sąvoka yra gana abstrakti. Reikėtų pasirūpinti, jog duomenų valdytojai nesudarytų nepagrįstų kliūčių duomenų subjektams tokią informaciją (pavyzdžiui nenustatytų neracionaliai didelio mokesčio už informacijos suradimą ar pan.). Taip pat yra svarbu užtikrinti ir trečiųjų asmenų, esančių vaizdo įraše kartu su duomenų subjektu, teises. Todėl specialiame teisės akte reikėtų nurodyti aiškų maksimalų mokestį už informacijos paiešką, kurios duomenų valdytojas negalėtų viršyti, o taip pat ir nustatyti trečiųjų asmenų maskavimo taisykles, suteikiant vaizdo medžiagą duomenų subjektui.

Operatorių švietimas

Svarbu, kad tiesiogiai vaizdo stebėjimą vykdantys operatoriai būtų tinkamai apmokyti ir žinotų, ką reikia daryti, kad jų veikla būtų visiškai suderinta su atitinkamais reikalavimais.

Vilniaus miesto Vyriausiojo policijos komisariato pateiktais duomenimis[104], pasirašyta vaizdo stebėjimo kamerų transliuojamo vaizdo stebėjimo sutartis tarp Vilniaus m. VPK, ir Vilniaus m. savivaldybės „Susisiekimo paslaugos“. Šios sutarties tikslas gerinti viešosios tvarkos užtikrinimą sostinėje, kuo efektyviau panaudojant Vilniaus mieste įrengtą vaizdo stebėjimo sistemą. Remdamiesi sutartimi, Vilniaus m. VPK įsipareigojo sudaryti darbo sąlygas ir priėmė 10 laisvai samdomų darbuotojų dirbti prie vaizdo stebėjimo sistemos monitorių ir užtikrinti, kad visą parą nepertraukiamai būtų stebimas vaizdo stebėjimo sistemos transliuojamas vaizdas.

Kadangi Vilniaus m. VPK VP OVS budėtojų poskyrio padalinys vadovaujasi darbo organizavimo instrukcija,[105] kurioje įteisintos darbuotojų teisės ir pareigos, Vilniaus m. VPK VP OVS nuostatais[106] bei budėtojų poskyrio vidaus instrukcija[107], kyla pagrįsta abejonė ar laisvai priimti asmenys (ne pareigūnai) yra tinkamai susipažinę su asmens duomenų apsaugos įstatymo

[103] CCTV Code of Practice http://www.informationcommissioner.gov.uk/cms/DocumentUploads/cctvcop1.pdf 7-8 psl. prisijungimo laikas 2005-09-18
[104] VPK duomenys 2005-08-11
[105] Lietuvos Policijos generalinio komisaro 2001 m. birželio 25 d. įsakymas Nr. 278
[106] Vilniaus m. VPK viršininko 2003m. gegužės 13 d. įsakymas Nr. 1-V-142
[107] Vilniaus m. VPK viršininko 2002 m. lapkričio 4 d. įsakymas Nr. 287

pagrindais. Pabrėžtina, kad laisvai samdomiems asmenims neprivalomi policijos įstaigų instrukcijos skirtos pareigūnams, kuriose visai nereglamentuoja vaizdo sistemų panaudojimas, todėl nesant šios srities reguliavimo, bei paliekant šiuos klausimus kiekvieno duomenų valdytojo nuožiūrai, pažeidimai neišvengiami.

4. IŠVADOS IR PASIŪLYMAI

Apibendrinant šį magistro baigiamąjį darbą reiktų pastebėti, kad asmens duomenų teisinės apsaugos reguliavimas policijos sektoriuje nėra pakankamas. Lietuvoje formuojasi valstybinis požiūris apie tai, kad asmens duomenų saugumas yra ne tik duomenų subjekto ar duomenų valdytojo problema. Asmens duomenų apsaugos esmė - apsaugoti žmonių teises. Pagrindinis jos tikslas yra užtikrinti, kad asmens duomenys būtų apdorojami taip, kad būtų užtikrinamas žmogaus privatumas ir kitos su tuo susijusios žmogaus teisės. Šiuo metu Lietuvoje galiojantys teisės aktai tik dalinai ir paviršutiniškai garantuoja asmens duomenų saugumą, be to daugelis policijos informacinių sistemų dar tik kuriamos, todėl nėra pakankamos teisinės apsaugos, tvarkant asmens duomenis.

Renkant asmens duomenis, nepakankamai užtikrinama, kad duomenys būtų tik tokios apimties, kuri būtina jiems rinkti ir toliau tvarkyti.

Besiplečiantis asmens kodo naudojimas ir jo pagrįstumas policijos įstaigose kelia didelį susirūpinimą žmogaus teisių apsaugos požiūriu. Asmens kodo naudojimas dažnai pripažįstamas kaip nepagrįstas kai asmens tapatybė gali būti nustatyta remiantis asmens tapatybę, tam tikrą teisinį statusą patvirtinančio dokumento rekvizitais. O asmens kodo tvarkymą policijos įstaigose ypač tose srityse kai jis patikimas bet kuriam kitam fiziniui asmeniui vertintinas kritiškai ir sukelia pažeidžiamumo jausmą.

Nesant Lietuvoje tiesioginio teisinio reguliavimo abejotina ar vaizdo stebėjimo sistemų pagalba renkamų duomenų valdytojai bei operatoriai yra pasiruošę, ir nesugeba interpretuoti plačias ir bendras ADTAĮ normas, kad pritaikytų jas savo vykdomai veiklai ir būtų tikri, kad nepažeidžia asmenų teisės į privatumą.

Apibendrinus visą turimą informaciją, galima pateikti šiuos pasiūlymus:

1. Vidaus reikalų ministerija, kaip duomenų bei informacinių sistemų valdytoja turėtų aiškiai nustatyti asmens duomenų keitimosi tarp valstybės ir savivaldybių institucijų tvarką, detaliai ir aiškiai reglamentuoti asmens duomenų apsikėtimo atvejus konkretizuojant teisių ribojimo sąlygas bei duomenų apsikeitimo atvejus. Įvesti VRM informacinių duomenų bazių peržiūros priežasties lauką su tikslu fiksuoti asmens duomenų naudojimo tikslą, bei kontroliuoti užklausas tam sukuriant

tinkamą vidinę asmens duomenų naudojimo priežiūros sistemą. Griežta naudojimo priežiūra ir naudojimo istorijos kūrimas – tai būtinos priemonės užtikrinant žmogaus teisę į privatumą.

2. Policijos departamentui ir Vidaus reikalų ministerijai parengti teisės aktą policijos įstaigoms kuriame būtų suvienodinama duomenų valdytojų, registravimo tvarka ir aptarti asmens valdytojų registravimo Valstybinėje duomenų apsaugos inspekcijoje atvejai bei metodika.

3. Pakeisti Lietuvos policijos generalinio komisaro 2002 m. gruodžio 24 d. įsakymą Nr. 660 „Dėl policijos patrulių veiklos instrukcijos patvirtinimo“. Jame išsamiai detalizuoti asmens duomenų tvarkymo tikslus, aiškiai apibrėžiant atvejus ir tvarką, kokia remiantis policijos tvarkomose dokumentuose bei pažymose būti tvarkomi duomenys tokie kaip asmens kodas. Taip pat numatyti tvarką ir atvejus šių svarbių asmens duomenų perdavimo trečiosiomis šalims bei fiziniams asmenims nustatant veiksmingas garantijas šių duomenų apsaugai. Apriboti asmens kodo naudojimą, vadovaujantis proporcingumo principu. Teisės aktuose sumažinti prašomus pateikti asmens duomenis, kad toks reikalavimas būtų adekvatus norimam tikslui pasiekti.

4. Policijos programiniame pakete duomenų (policijos įskaita) sukurti fotokartotekos duomenų aplikaciją, kuri padėtų apsaugoti subjektų teises, užkertant kelią piktnaudžiauti svetimais asmens duomenimis.

5. Lietuvoje vaizdo stebėjimo sistemų panaudojimui yra taikomas ADTAĮ, tačiau jame nėra tiesioginio ir konkretaus reguliavimo skirto šių sistemų panaudojimui. Įstatymo nuostatos yra bendro pobūdžio, be to nėra ir jokio kito teisės akto, kuris reglamentuotų tik vaizdo stebėjimo sistemų naudojimą, todėl siūlyčiau: Valstybinei duomenų apsaugos inspekcijai inicijuoti vaizdo stebėjimų sistemų sąvoką, kuri turėtų būti inkorporuota į Lietuvos Respublikos Asmens duomenų apsaugos įstatymą kuriame papildytų bent jau pagrindines nuostatas, kurios:

- apibrėžtų ir patikslintų vaizdo kamerų CCTV priemonių sąvoką;
- reglamentuotų specialius reikalavimus šiuo atveju,
- ateityje nustatyti valstybės instituciją, kuri būtų atsakinga už tokių vaizdo stebėjimo sistemomis tvarkomų duomenų priežiūrą.

Tuo tikslu siūlyčiau papildyti ADTAĮ 2 straipsnį 16 dalimi:

„16. Vaizdo stebėjimas (CCTV) – asmenų stebėjimas ir jų vaizdo duomenų fiksavimas naudojant nuotolinio ar automatinio valdymo vaizdo arba foto kameras ar panašius prietaisus.“

Papildyti ADTAĮ $16^{(1)}$ straipsnį įrašant:

„$16^{(1)}$ straipsnis. Asmens duomenų tvarkymas vaizdo stebėjimo priemonėmis

1. Siekiant užtikrinti visuomenės saugumą, viešąją tvarką, apginti asmenų teises ir laisves, kai kitų, mažiau asmens privatumą ribojančių priemonių nepakanka.

2. Asmenys turi būti tinkamu būdu informuojami apie tai, kad jų asmens duomenys yra tvarkomi panaudojant vaizdo arba foto kameras, nurodant duomenų valdytojo, tvarkančio asmens duomenis, tapatybę, rekvizitus ir buveinę.

3. Duomenys, surinkti konkrečiu iš anksto nustatytu tikslu panaudojant vaizdo ir foto kameras gali būti naudojami kitiems tikslams tik tais atvejais arba kai įstatymų nustatytais atvejais būtina užkirsti kelią nusikalstamoms ar kitoms neteisėtoms veikoms arba šias veikas tirti.

4. Asmens duomenys, surinkti panaudojant vaizdo ir foto kameras, turi būti nedelsiant sunaikinti, kai jie nebereikalingi tikslui, dėl kurio buvo surinkti, arba kai tolimesnis jų saugojimas prieštarautų teisėtiems duomenų subjekto interesams.

5. Tvarkydamas asmens duomenis panaudojant vaizdo ir foto kameras, duomenų valdytojas privalo vadovautis šiuo Įstatymu, taip pat kitais įstatymais bei teisės aktais, reglamentuojančiais privataus gyvenimo apsaugą ir asmens duomenų tvarkymą.

6. Įvertinus galimus pakeitimus ADTAĮ Asmens duomenų apsaugos inspekcija turėtų inicijuoti poįstatyminį akto leidimą, kuriame:

- Apibrėžti vaizdo stebėjimo sistemų įrengimo tikslus, institucijas, asmenys kuriems leidžiama naudoti vaizdo stebėjimą, prievolė išsiaiškinti ar nėra kitų privatumo teisės mažiau ribojančių priemonių;
- Konkretūs apribojimai naudojamai vaizdo technikai, operatorių darbui, taisyklės kuriomis vadovaujantis nebūtų renkami pertekliniai duomenys;
- Numatyta konkreti prievolė duomenų valdytojui informuoti apie vykdomus vaizdo stebėjimus;
- Prievolė apie vaizdo sistemų operatorių mokymus, bei asmens duomenų tvarkymo procedūras;

Jame duomenų valdytojai turėtų tikslai žinoti, kaip derinti savo, visuomenės ir privačių asmenų teises šioje sferoje. Efektyvumo dėlei, šalia duomenų valdytojams privalomų principų, teisės akte turėtų būti numatytos geros praktikos - rekomendacinio pobūdžio normos, tokios kaip „Vaizdo stebėjimo sistemų praktikos kodeksas“ (*CCTV Code of Practice)*, išleistas Didžiosios Britanijos Informacijos Komisaro 2000 metais[108], nes šiuo metu nesant adekvataus vaizdo stebėjimo sistemų panaudojimo teisinio reguliavimo Lietuvoje, sudaromos prielaidos žmogaus teisių pažeidimams.

7. Policijos įstaigų vadovams, padalinių veikloje naudojantiems vaizdo stebėjimo sistemas (CCTV) parengti taisykles bei metodinius nurodymus, pateikiant (techninius ir organizacinius) nurodymus.

---

[108] CCTV Code of Practice http://www.informationcommissioner.gov.uk/cms/DocumentUploads/cctvcop1.pdf prisijungimo laikas 2005-07-15

Tinkamai apmokyti operatorius dirbančius su asmens duomenimis juos supažindinant su vaizdo duomenų gavimo, saugojimo naikinimo procedūromis, duomenų subjektų bei trečiųjų asmenų teisėmis bei savo atsakomybe. Policijos įstaiga turėtų atsižvelgti į Direktyvos 95/46/EB įtvirtintą nuostatą, kad duomenys, susiję su nusikaltimais, asmens teistumais ar valstybės saugumo priemonėmis, gali būti tvarkomi tik tuo atveju, jeigu tai kontroliuoja valdžios institucija arba jeigu užtikrinamos tinkamos saugumo priemonės.

Pagal Europos Žmogaus Teisių ir Pagrindinių Laisvių Konvenciją valstybė ne tik privalo pasirūpinti, jog asmenų teisės nebūtų neteisėtai ribojamos, bet ir turi imtis priemonių, kad tos teisės būtų užtikrintos.

Tikiu, kad kasmet didėjantis žmonių aktyvumas ir rūpinimasis savo asmens duomenimis labiau pakels duomenų apsaugos lygį mūsų šalyje, pagerins duomenų apsaugos principų taikymą ir privers duomenų valdytojus sukurti institucijose, įmonėse, įstaigose ar organizacijose tokią aplinką, kurioje žmogus jaustųsi saugus ir pasitikėtų savo duomenų valdytojais.

LITERATŪROS SĄRAŠAS

Įstatymai

1. Lietuvos Respublikos Konstitucija// Valstybės žinios. 1992, Nr. 33-1014.
2. Lietuvos Respublikos valstybės registrų įstatymas// Valstybės žinios. 1996, Nr. 86-2043.
3. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas//Valstybės žinios, 1996, Nr. 63-1479.
4. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo pakeitimo įstatymas. 2003 m. sausio 21 d. Nr. IX-1296, Vilnius.
5. Lietuvos Respublikos viešojo administravimo įstatymas//Valstybės Žinios. 1999, Nr. 60–1945.
6. Lietuvos Respublikos visuomenės informavimo įstatymas//Valstybės žinios. 1996, Nr. 71-1706.
7. Lietuvos Respublikos administracinių teisės pažeidimų kodeksas//Valstybės žinios. 1985, Nr. 1-1.
8. Lietuvos Respublikos civilinis kodeksas//Valstybės žinios. 2000, Nr. 74-2262.
9. Lietuvos Respublikos operatyvinės veiklos įstatymas //Valstybės žinios. 2002, Nr. 65-2633.
10. Lietuvos Respublikos Baudžiamojo proceso kodeksas//Valstybės Žinios. 2002, Nr. 37-1341
11. Lietuvos Respublikos gyventojų registro įstatymas//Valstybės Žinios. 1999, Nr. 28-793
12. Lietuvos Respublikos policijos veiklos įstatymas//Valstybės Žinios. 2000, Nr. 90-2777

Tarptautiniai dokumentai

13. Visuotinė žmogaus teisių deklaracija//Žmogaus teisės. Jungtinių Tautų dokumentai. 2000;
14. 1980 m. rugsėjo 23 d. EBPO Rekomendacija dėl asmens privatumo apsaugos ir asmens duomenų judėjimo tarp valstybių narių gairių.

15. Konvencijos dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu papildomas protokolas dėl priežiūros institucijų ir valstybės sienas kertančių duomenų srautų // Valstybės žinios. 2004, Nr.36-1187.
16. Konvencija „Dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108)“ // Valstybės žinios. 2001. Nr. 32–1059.
17. Pagrindinės Europos Tarybos sutartys - Vilnius: Europos Tarybos informacijos ir dokumentacijos centras, 2000.
18. Europos policijos etikos kodeksas priimtas Europos Tarybos Ministrų Komiteto 2001 m. rugsėjo 19 d.
19. Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija // Valstybės žinios. 1995, Nr. 40-987.
20. Direktyva 95/46/EB ”Dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo“.
21. Direktyva 2002/58/EB „Dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje“.
22. Direktyva 90/313/EB ”Dėl laisvo prieinamumo prie informacijos apie aplinką“.
23. Direktyva 2002/58/EB „Dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje“.

Kita literatūra

24. Lietuvos Respublikos Vyriausybės 2002 m. gruodžio 31 d. nutarimas Nr.2105 Dėl duomenų saugos valstybės ir savivaldybių informacinėse sistemose//Valstybės žinios, 2003, Nr. 2-45
25. Vidaus reikalų ministerijos Ministro 2003 07 16 d. įsakymas Nr. 1V-272 Dėl Tipinių duomenų saugos nuostatų patvirtinimo// Valstybės žinios,2003, Nr. 76-3511
26. Konvencijos dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu papildomas protokolas dėl priežiūros institucijų ir valstybės sienas kertančių duomenų srautų // Valstybės žinios. 2004, Nr.36-1187.
27. Aiškinamasis raštas dėl Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo pakeitimo įstatymo projekto Nr. IXP-2037.
28. Dėl duomenų saugos valstybės ir vietos savivaldos informacinėse sistemose//Valstybės Žinios. 1997, Nr. 83-2075; Valstybės Žinios. 2003, Nr. 2-45.
29. Dėl Valstybės informacinių sistemų steigimo ir įteisinimo patvirtinimo//Valstybės žinios. 2004, Nr. 58-2061.
30. Dėl saugaus valstybinio duomenų perdavimo tinklo nuostatų ir Saugaus valstybinio perdavimo tinklo paslaugų teikimo taisyklių patvirtinimo//Valstybės žinios. 2004, Nr. 83-3025.
31. Lietuvos Respublikos valstybinės duomenų apsaugos inspekcijos 2003 m. liepos 22 d. Rekomendacijos dėl privatumą stiprinančių technologijų.
32. Informacinės visuomenės plėtros komiteto prie Lietuvos Respublikos Vyriausybės direktoriaus 2004 m. spalio 15 d. įsakymas Nr. T-131 „Dėl valstybės informacinių sistemų kūrimo metodinių dokumentų patvirtinimo“//Valstybės žinios, 2004, Nr. 155-5679.
33. Statistikos departamento prie Lietuvos Respublikos Vyriausybės generalinio direktoriaus ir Valstybės tarnybos departamento prie Vidaus reikalų ministerijos direktoriaus 2005 m. birželio 9 d. įsakymas Nr. DĮ-148/27V-41 „Dėl valstybės tarnautojų duomenų teikimo“ //Valstybės žinios. 2005, Nr. 74-2700.
34. Lietuvos Respublikos Vyriausybės 2003 m. lapkričio 18 d. nutarimas Nr. 1426 „Dėl Vidaus reikalų pareigūnų registro įsteigimo ir Vidaus reikalų pareigūnų registro nuostatų patvirtinimo“//Valstybės žinios 2003. Nr. 109-4883.
35. Lietuvos policijos generalinio komisaro 2003 m. gegužės 15 d. įsakymas Nr. V-271 „Dėl informacijos apie nusikalstamą veiką, kitus teisės pažeidimus ir įvykius registravimo bei tikrinimo“//Valstybės žinios 2003. Nr. 49-2192.

36. Lietuvos policijos generalinio komisaro 2002 m. rugpjūčio 9 d. įsakymas Nr. 451 „Dėl policijos programinio paketo“.
37. Lietuvos policijos ryšių su visuomene koncepcija, patvirtinta Lietuvos policijos generalinio komisaro 2005 m. gegužės 17 d. įsakymu Nr.5-V-317 „Dėl Lietuvos policijos ryšių su visuomene koncepcijos patvirtinimo“.
38. Žmogaus teisės. Europos Tarybos ir Europos Sąjungos dokumentai. – Vilnius: Lietuvos žmogaus teisių centras, 2000.
39. Elektroninės valdžios koncepcija//Valstybės žinios. 2003, Nr.: 2-54.
40. Dėl Informacijos technologijų saugos valstybinės strategijos ir jos įgyvendinimo plano patvirtinimo//Valstybės Žinios. 2001, Nr. 110-4006.
41. Lietuvos Respublikos Vyriausybės 1997 m. rugsėjo 4d. nutarimas „Dėl duomenų saugos valstybės ir savivaldybių informacinėse sistemose“ // Valstybės Žinos.1997, Nr83-2075; 2003, Nr2-45.
42. Vidaus Reikalų Ministro 2005 m. kovo 9 d. įsakymas Nr. 1V-68 „Dėl Vidaus Reikalų informacinėse sistemose centrinio duomenų banko duomenų peržiūrimos kontrolės taisyklių patvirtinimo“
43. Lietuvos Respublikos Vyriausybės 2004-2008 metų programa//Valstybės žinios. 2004, Nr. 181-6703.
44. Dėl duomenų saugos valstybės ir vietos savivaldos informacinėse sistemose//Valstybės Žinios. 1997, Nr. 83-2075; Valstybės Žinios, 2003, Nr. 2-45.
45. Lietuvos Respublikos valstybinės duomenų apsaugos inspekcijos 2003 m. liepos 22 d. Rekomendacijos dėl privatumą stiprinančių technologijų
46. Prancūzijos Duomenų apsaugos įstatymas 1978 m. sausio 6 d.
47. Informacinės visuomenės plėtros komiteto prie Lietuvos Respublikos Vyriausybės direktoriaus 2004 m. spalio 15 d. įsakymas Nr. T-131 „Dėl valstybės informacinių sistemų kūrimo metodinių dokumentų patvirtinimo“//Valstybės žinios 2004. Nr. 155-5679.
48. Lietuvos policijos generalinio komisaro 2002m. gruodžio 24 d. įsakymas Nr. 660 „Dėl policijos patrulių veiklos instrukcijos patvirtinimo“//Valstybės žinios 2003. Nr. 23-985.
49. Lietuvos Respublikos Seimo 2003 m. birželio 26 d. nutarimas Nr. IX-1655 „Dėl asmens duomenų apsaugos valstybės institucijose užtikrinimo“ //// Valstybės žinios, 2003, Nr. 65-2938.
50. Informacijos technologijų saugos valstybinė strategija ir jos įgyvendinimo planas, patvirtintas Lietuvos Respublikos Vyriausybės 2001 m. gruodžio 22 d. nutarimu Nr. 1625 // Valstybės žinios, 2001, Nr. 110-4006.
51. Adomaitis J. Saugumo problemos Vilniaus senamiestyje. Galimas saugos tarnybų indėlis // Seminaro „Asmens ir turto saugumas Vilniaus senamiestyje“ pranešimai. - Vilnius, 1999.
52. Pumputis A. Poreikių ir žmogaus teisių sistemos klausimu // Jurisprudencija: Mokslo darbai. – Vilnius: Lietuvos teisės akademija, 2000. T. 15 (7).
53. Šakočius A. Kova su netvarka įgyvendinant bendruomenės teisėtvarką. – Vilnius: LTA Leidybos centras, 2000.
54. Kurakovas L.P., Smirnovas S.N. Informacija, kaip teisinės apsaugos objektas. – M. :Helios, 1998.
55. T. Birmontienė. Žmogaus teisės Lietuvos Respublikos Konstitucijoje. Konstitucija, žmogus, teisinė valstybė. Konferencija, skirta Lietuvos Respublikos Konstitucijos penkerių metų sukakčiai. Vilnius, 1997 m. spalio 24-25 d.
56. D.Dzemydienė, R.Naujikienė. Informacinės sistemos – duomenų struktūros ir valdymas. Vilnius: Lietuvos teisės universitetas 2004.
57. T. Birmontienė. Žmogaus teisių raida ir perspektyvos Lietuvoje.//Teisinės valstybės link. Teisės akademijos mokslo darbai, Nr. 15. Vilnius, 2000 m.

58. E. Jarašiūnas. Informacijos laisvės apsaugos problemos Konstitucinio Teismo praktikoje. //Jurisprudencija, 1998 m. T. 9 (1).
59. R. Kalesnykas, V. Mečkauskas. Vaizdo stebėjimo kamerų (CCTV) panaudojimas užtikrinant visuomenės saugumą: teisiniai ir organizaciniai aspektai. Vilnius, LTU 2002.
60. Panomariovas A. Viešai neskelbiama informacija – paslaptis kaip socialinis teisinis reiškinys//Jurisprudencija, 2002, T. 32 (24).
61. Žmogaus teisių stebėjimo institutas - analitinė apžvalga „Vaizdo stebėjimo kamerų panaudojimas ir žmogaus teisės“ 2005 m.
62. Lietuvos ryto straipsnis „Audra stiklinėje“ 2003-04-12
63. Švietimo informacinių technologijų centro projektas „Švietimas internetui – internetas švietimui“.
64. Informatikos ir ryšių departamento prie VRM direktoriaus pranešimas simpoziume - „Informacijos saugos naujienos“ 2005-03-07
65. Dabartinės lietuvių kalbos žodynas. Vilnius, 2000.
66. Informatikos ir ryšių departamento prie VRM direktoriaus pranešimas simpoziume - „Informacijos saugos naujienos“ 2005-03-07
67. Projekto „Privatumo ir saugumo lietuviškame internete tyrimas (pirmas etapas)“ dalykinė ataskaita. Vilnius. Atviros Lietuvos fondas. 2002.
68. Keras A., Kurapka E., Petrauskas R. Informacinės visuomenės kūrimo, informacinių technologijų taikymo ir informacinių technologijų teisės plėtros tendencijos Europos Sąjungoje. Vilnius 2001.
69. Ministrų komiteto rekomendacija Nr. R (87) 15 1987-09-17 d. Valstybėms narėms dėl asmens duomenų naudojimo policijos sektoriuje.
70. Кураков Л. П., Смирнов С.Н . Информация как объект правовой защиты. – М.:Гелиос, 1998.
71. Человек и информация. – М.: Прогресс, 1972.

Interneto tinklapių adresai

72. Internetinis žurnalas „Sociumas“ – http//www.sociumas.lt/
73. Lietuvos Aukščiausiasis Teismas – http://www.lat.litlex.lt
74. Informatikos teisės centras - http://www.itc.tf.vu.lt/
75. Lietuvos Respublikos Seimas – http://www.lrs.lt
76. Valstybinės duomenų apsaugos inspekcija - http://www.ada.lt
77. Teisinės informacijos centras – http://www.infolex.lt/portal/
78. Žmogaus teisių stebėjimo institutas - http://www.hrmi.lt/
79. Vilniaus miesto VPK - http://www.policija.lt/sostine/
80. Policijos departamentas prieVRM - http://www.policija.lt/
81. Lietuvos Eismo priežiūros tarnyba prie PD - http://viesoji.policija.lt/ept/
82. Lietuvos Viešoji policija http://www.policija.lt/viesoji/
83. UAB „Vildoma“ http://www.vildoma.lt/
84. Valstybės įminė „Regitra“ http://www.regitra.lt/
85. Vidaus reikalų ministerija - http://www.vrm.lt/
86. Informatikos ir ryšių departamentas prie VRM http://www.vrm.lt/
87. Ryšių reguliavimo tarnyba http://www.rrt.lt/
88. Vilniaus miesto savivaldybė http://www.vilnius.lt/
89. Laikraštis Lietuvos rytas www.lrtas.lt
90. M. Civilka. Asmens duomenų apsaugos teisinis reguliavimas interneto kontekste. http://www.itc.tf.vu.lt/mokslas/mokslas.html

91. M. Civilka. Mokymo apie asmens duomenų apsaugą koncepcija. http://www.itc.tf.vu.lt/mokslas/adak.doc
92. Riedutininkų klubas „Ketvirtadienio nakties karštis“ http://www.riedek.lt/
93. Viešųjų erdvių vaizdo stebėjimas Europos žmogaus teisių konvencijos kontekste http://www.crimereduction.gov.uk/cctv13.htm
94. Asmens duomenų valdytojų Valstybės registras http://db.ada.lt/

SANTRAUKA

Vykstant intensyviam informacijos tarp subjektų keitimosi procesui, iškyla nemažai praktinių problemų, susijusių su asmens duomenų tvarkymo teisėtumu ir pagrįstumu, asmens duomenų apsaugos ir informacijos privatumo užtikrinimu. Atsižvelgiant į tai, jog neteisėti asmens duomenų tvarkymo veiksmai gali turėti ypatingai skaudžių, neigiamų pasekmių asmens, kurio duomenys yra tvarkomi, privatumui, nepažeidžiamumui, šios problemos yra dar aktualesnės.

Didžiausias asmens privatumo pažeidžiamumas yra informacinių technologijų srityje. Informacijos privatumas ir asmens duomenų apsauga užtikrinama teisinės bazės naudojimu ir tobulinimu, saugumo priežiūros stiprinimu, visuomenės informavimu ir mokymu, savireguliacija, technologinių priemonių naudojimu.

Asmens privataus gyvenimo apsaugos užtikrinimas yra įtvirtintas daugelyje teisės aktų. Tačiau Lietuvos teisinė bazė, reglamentuojanti asmens privatumo užtikrinimą, pilna teisinių spragų bei trūkumų, dėl kurių kyla nemažai problemų, sukeliančių skaudžias pasekmes asmens privatumui.

Labai svarbi nepakankamo asmens duomenų apsaugos ir informacijos privatumo užtikrinimo policijos įstaigose priežastis – menkas žmonių suvokimas apie šias problemas. Reikia šviesti informacijos valdytojus apie asmens duomenų apsaugos ir informacijos privatumo užtikrinimo problemas, apie priemones, kuriomis turėtų būti užtikrinama ar užtikrinamas duomenų saugumą, privatumą.

Pažymima pozityvi vaizdo stebėjimo kamerų (CCTV) sistemų naudojimo įtaka užtikrinant visuomenės saugumą, nes jos gali būti naudingos atskleidžiant ir aiškinant teisės pažeidimus, kaip įrodymas teisme, kaip prevencijos priemonė. Vaizdo stebėjimo kamerų (CCTV) naudojimo efektyvumą ir naudingumą (ekonominiu požiūriu) galima vertinti tik praėjus tam tikram laikotarpiui bei atlikus saugios aplinkos būklės tyrimus.

Ir tol, kol nebus įnešta tam tikro aiškumo, konkretumo, tikslumo į Lietuvos įstatyminėje bazėje, kol visuomenė bus menkai informuojama apie privatumą ir savo teisių bei asmens duomenų apsaugos ir informacijos privatumo užtikrinimo problemos išliks.

SUMMARY

PERSONAL DATA PROTECTION IN POLICE INFORMATION SYSTEMS

Considering the fact, that unlawful administration of personal record may entail particularly severe results for the privacy, invulnerability of the individual, whose record is being administrated, these problems are even more relevant.

The highest vulnerability of privacy exists in the sphere of IT. The privy of information and security of personal data is safeguarded by laws implementation and refining of the legal basis, related to this issue, by amplification of security supervision, by information to and lecturing of the society, by the usage of technologic devices.

Security of privacy is entrenched in many laws. However, the Lithuanian legal basis, regulating the security of privacy, is full of juridical vacancies and deficiencies, which cause lots of problems, resulting in severe outcomes to the privacy.

A very important reason of insufficient security of privacy and personal data on the is the low perception by the society about the existence of these problems.

The article analyses the prospects of using CCTV in public places which, authors regard, could have a certain influence on the improvement of public security in the territory of coverage. Installation and usage of security measures which curbs criminal activity or acts as a deterrent, manifests in situational prevention against offences. CCTV in public security is a new preventive measure, therefore it is worth identifying and determining legal and organizational standards for the usage of cameras. Otherwise legal norms might be violated, human rights and freedoms constrained. The effectiveness and economic efficiency of CCTV usage are also touched upon.

As long as there will insufficient transparency and accuracy in Lithuanian legal basis, until the society will be little informed about the privacy and personal data security problems on the police, these problems will prevail.

Magistro baigiamasis darbas baigtas 2005 m. lapkričio mėn. 17 d.

Magistrantas

Žilvinas Jucius