Оливер Суботић

БИОМЕТРИЈСКИ СИСТЕМИ ИДЕНТИФИКАЦИЈЕ

критичка студија

Терминологија и технички аспекти
Мултидисциплинарна анализа
Друштвене импликације
Имплементација у земљама света
Имплементација у Републици Србији

Институт за политичке студије
Београд 2007

Оливер Суботић

БИОМЕТРИЈСКИ СИСТЕМИ ИДЕНТИФИКАЦИЈЕ:
КРИТИЧКА СТУДИЈА

Оливер Суботић
БИОМЕТРИЈСКИ СИСТЕМИ ИДЕНТИФИКАЦИЈЕ:
КРИТИЧКА СТУДИЈА

Издавач
Институт за политичке студије,
Савски трг 7а, 11000 Београд, Србија;
e-mail: ipsbgd@eunet.yu
www.ipsbgd.edu.yu
тел: +381 11 2642 042
+381 11 3613 240
факс: +381 11 2645 490

Уредник
Живојин Ђурић

Рецензенти:
Драган Спасић
Никола Марковић
Александар Павић
Драгољуб Ђорђевић
Александар Раковић
Дејан Николић

Дизајн и рачунарска припрема за штампу
Оливер Суботић

Тираж
500

Оливер Суботић

БИОМЕТРИЈСКИ
СИСТЕМИ ИДЕНТИФИКАЦИЈЕ

критичка студија

Институт за политичке студије,
Београд, 2007

Садржај

Уводна реч аутора 9
Abstract: Biometric Systems of Identification: A Critical Study 14
Abstract: Биометрические системы идентификации: критическое рассмотрение 15
Листа скраћеница 16

1. Терминологија, историјат и теоријски концепти биометријских система идентификације 17
1.2 Идентификација, аутентификација и аутентификација идентитета 21
1.3 Начин остваривања биометријских система идентификације у пракси 23
1.4 Фактори безбедности биометријских система идентификације 25
1.5 Однос биометријских и небиометријских електронских карти 26
1.6 Прецизност биометријских система идентификације 27

2. Биометријски системи идентификације: мултидисциплинарна нализа .. 29
2.1 Различите имплементације биометријских система идентификације 30
2.1.1 Имплементација на (над)националном нивоу: некритички и критички приступ 31
2.2 Баријере психолошког, културолошког и верског порекла 33
2.3 Продуктивност и злоупотреба као две стране исте медаље 35
2.4 Тотал(итар)ност концепта централне базе података 38
2.5 Биометријска идентификација без централ(изова)не базе 41
2.6 Биометрија и борба против организованог криминала и тероризма 43
2.7 Биометријски системи идентификације и право на приватност 46
2.8 Утицај на концентрацију моћи државног апарата 50
2.9 E-government, e-commerce, e-banking и биометрија 52
2.10 Поузданост биометријских система идентификације 58
2.11 Закључак 59

3. Имплементација биометријских система идентификације у свету: аналитички преглед 60
3.1 Биометријске личне карте 61
3.1.1 Земље „common law“ система 61
3.1.1.1 Студија случаја – Велика Британија 65
3.1.2 Земље Европе и Европске Уније 68
3.1.2.1 Иницијативе, препоруке и директиве телâ ЕУ 69
3.1.2.2 Земље Европске Уније без личних карата 71

3.1.2.3 Земље Европе и Европске Уније са личним картама на добровољној основи ... 71
3.1.2.4 Земље Европе и Европске Уније са личним картама на обавезујућој основи ... 73
3.1.2.5 Студија случаја: Француска и Немачка ... 76
3.1.3 Стање у европским земљама са већински православним становништвом ... 79
3.1.4 Стање у осталим земљама света ... 81
3.1.4.1 Студија случаја: Јапан и Тајван ... 83
3.1.5 Биометријске личне карте – сумарни закључак ... 84
3.2 Биометријски пасоши ... 84
3.2.1 Настанак и пропозиције ICAO 9303 стандарда ... 85
3.2.2 ЕУ и имплементација биометријских пасоша ... 86
3.2.3 Биометријски пасоши у земљама обичајног права ... 88
3.2.4 Биометријски пасоши у земљама трећег света ... 89
3.2.5 Критички осврт на увођење биометријских пасоша ... 90
3.2.6 Будимпештанска декларација уместо закључка о имплементацији биометријских пасоша ... 94
3.3 Специјална употреба биометријских система идентификације на националном и наднационалном нивоу ... 95
3.4 Сумарни закључак ... 97
4. Република Србија: Биометријски пројекат ... 99
4.1 Куповина рачунарског биометријског система: историјат, планови и (не)законитост ... 100
4.2 Реакције јавности пре доношења Закона о личној карти ... 102
4.2.1 Стручни скупови пре усвајања Закона: Жички симпосион ... 102
4.2.2 Медијски извештаји, публикације, критички текстови и реакције невладиног сектора пре усвајања Закона ... 103
4.3 Владина иницијатива за парламентарну процедуру ... 104
4.3.1 Грешке и некритички ставови у образложењу Предлога закона о личној карти ... 106
4.3.2 Парадокс неадекватног Закона о заштити личних података ... 107
4.4 Стручни скупови и јавне дебате после усвајања Закона о личној карти. 109
4.4.1 Округли сто у галерији САНУ ... 109
4.4.2 Стручни скупови у Краљеву и Вршцу ... 111
4.4.3 Округли сто у Interkontinental-у ... 112
4.5 Званична реакција Српске православне цркве ... 112
4.6 Критичке реакције НВО сектора после усвајања Закона ... 113
4.7 Реакције критички оријентисаних штампаних медија ... 114
4.8 Критички извештаји електронских медија ... 117
4.9 Критичке реакције владиних службеника ... 117

4.10 Реакције пробиометријских интелектуалних кругова 118
4.11 Пробиометријска публикација МУП-а 120
4.12 Уредба владе Србије – опционалност микрочипа на обрасцу 124
4.13 Србија – уместо закључка 126

5. Закључци и препоруке 131

6. Додатак А: Критички гласови из света 135
Роџер Кларк: Електронска идентификациона документа: обећања и опасности (закључно поглавље) 137
Џулијан Ешбурн: Развејавање популарних митова о биометријској технологији (извод) 139
FIDIS: Будимпештанска декларација о машински читљивим путним исправама 141
Кевин Хагерти: Једна генерација је све што им треба 145

7. Додатак Б: Критички гласови из Србије 151
Жички апел 153
Да ли електронска карта угрожава приватност грађана? (закључци и препоруке округлог стола у Галерији САНУ) 155
Декларација стручног скупа у Краљеву 157
Слободан Антонић: У потрази за српским Тороом 159
Родољуб Шабић: Чип за приговор савести 161

8. Библиографија 164
Примарна литература 164
Секундарна литература 173

9. О аутору 183

Свима који су на било који начин били угрожени
због осетљивих података које је (над)државни апарат водио о њима

Уводна реч аутора

Биометријски системи идентификације и њихове друштвене импликације већ неколико година су спорна тема у светској јавности, поготово у земљама западне демократије. Ова тема је у нашој земљи постала актуелна после најаве увођења нових електронских личних карти и централизоване базе биометријских података. Нажалост, по том питању се у нашој јавности појавио велики број дезинформација, пласираних како од стране неких пропонената биометријског система (који су тврдили да је то део наших међународних обавеза, да скоро све земље ЕУ имају биометријске личне карте, да су оне ултимативан услов за успостављање електронске управе итд) тако и кроз реакцију неких недовољно информисаних опонената (који су тврдили да је у питању бесконтактна технологија, да омогућава перманентно праћење, па чак и да је чип радиоактиван итд). С обзиром на чињеницу да је ово озбиљна проблематика, њој се мора приступати темељно и критички, а не површно. Ова студија је формирана управо на критичким постулатима, са циљем да се о биометријским системима идентификације у широј јавности почне расправљати на стручној и научној основи.

Основни нацрт студије формиран је још почетком јула месеца 2006. године, на захтев Светог архијерејског синода Српске православне цркве (документ бр.1102 / зап. 778 од 20. јуна 2006). Свуда у слободном свету прве реакције и стручне студије из ове области су дошле на иницијативу невладиних организација које се боре за очување права на приватност и академских кругова (углавном из области компјутерског права), док је у Србији прва иницијатива за сагледавање тог проблема дошла из Цркве. Наиме, подстакнути захтевима једног броја верника који су ову проблематику пратили на светском нивоу, епископи СПЦ су тражили стручна мишљења о предлогу новог Закона о личној карти Републике Србије. То је био разлог да и ја (у својству стручног сарадника на информационим делатностима Православног богословског факултета у Београду) од стране Светог архијерејског синода званично добијем у задужење израду стручног мишљења по том питању.

С обзиром да је предлог спорног закона већ био у парламентарној процедури, по добијању захтева за стручно мишљење нисам имао на располагању довољно времена за детаљну опсервацију и анализу. Да бих дао релевантан и објективан став, а узимајући у обзир расположиви временски оквир, саставио сам једну концизну студију која је обухватала појам био-

метријских система идентификације, проблематику имплементације електронских биометријских личних карата на националном нивоу, посебан фактографско-аналитички осврт на стање у свету и специфичност случаја Републике Србије. За реализацију тог задатка прикупио сам научне студије реномираних светских академских установа, стручне извештаје парламентарних тела западних земаља, мишљења највећих светских информатичких стручњака, критичке публикације најпознатијих организација које се боре за приватност грађана, чланке познатих рачунарских часописа, медијске извештаје и званична саопштења различитих министарстава. Та првобитна студија је имала нешто више од двадесет страна А4 формата и сумарни закључак на три стране, који се према начелном концепту биометријске идентификације грађана на обавезујућем нивоу односио негативно уз напомену да је цео пројекат у случају Републике Србије додатно оптерећен процедуралним пропустима који имплицирају политички волунтаризам.

Студија која је пред Вама представља значајно проширење тог првобитног материјала, како у погледу обима и детаљности тако и у погледу структуре – обимом и структуром она је петоструко већа и детаљнија. Разлози за то су вишеструки.

Први разлог за њено проширивање лежи у чињеници да је у међувремену (14. јула 2006.) Закон о личној карти изгласан у Парламенту Србије. Према тој легислативи, нова документа су требала да почну да се издају крајем јануара месеца 2007. године, док би постојеће легитимације (којима није истекао рок важења) важиле највише 5 година од тренутка ступања Закона на снагу (осам дана по објављивању у Службеном гласнику Републике Србије бр. 62/2006, што значи највише до половине 2011. године). Иако словом Закона није прецизирано, њиме се фактички уводи и централна база биометријских података, као кључни технолошки супстрат за извођење комплетног пројекта. Управо том кључном аспекту је посвећено мало пажње у нашој јавности, што је разлог да у овој студији буде детаљније обрађен.

Други разлог је потреба за обрађивањем неколико веома битних стручних скупова и округлих столова из ове области који су се у Србији одржали непосредно после доношења Закона. Ови скупови су донели нова запажања и отворили простор за јавну дебату која је изостала пре парламентарне процедуре.

Трећи разлог је доношење Устава (које је уследило неколико месеци после изгласавања поменутог закона), с обзиром да неки чланови истог дају одређени простор за иницијативу за оцену уставности спорних тачака Закона. Нажалост, у тренутку писања ове студије рад Уставног суда Србије још увек је блокиран, због чега иницијатива за проверу уставности закона чека на тренутак његовог поновног фунционисања.

Четврти разлог је одигравање неколико веома битних догађаја на светском нивоу који су потврдили безбедносне закључке и претпоставке наведене у закључку првобитне студије. Уз то, у међувремену се појавило неколи-

ко занимљивих научних студија објављених у западном свету, које додатно откривају битне појединости које до сада нису биле познате и дају додатну потврду ставовима критички оријентисаних академских грађана.

И најзад, на петом месту (иако не по важности) је потреба за што детаљнијим упознавањем не само наше академске јавности, већ и ширих слојева друштва, са проблематиком имплементације биометријских система идентификације превасходно у контексту решења усвојеног у нашој земљи и његових импликација на друштвени живот, поготово уколико је приступ некритички.

Апсолутна је потреба да разговор на ову тему почне да се води у једном академском тону, ван било каквих интересних сфера и површних квалификација. Нажалост, многи интелектуалци постављају питање: зашто се уопште пише и поклања пажња обичном систему идентификације, па макар он био и крајње софистициран? Зашто толико пажње поклањати биометријским личним картама када су оне само технолошки напреднија итерација претходног решења? Није ли то антицивилизацијски и лудистички став? Оваква питања, уколико су добронамерна, настала су или из необавештености или из непрепознавања суштине проблема. Наиме, саме биометријске личне карте као видљива манифестација биометријског система су најмањи проблем, мада не безначајан. Далеко већа проблематика је везана за њихову позадину која је за просечног грађанина „невидљива“, у виду централизоване базе биометријских података. Са друге стране, техничка позадина овог система је *само* пројава проблема концептуалне природе који се тиче односа државе и грађана. Стога горе постављена питања треба да изгледају другачије. Да ли пројекат биометријске идентификације грађана ослоњен на централну базу биометријских података задире у правноцивилизацијске тековине, каква је претпоставка невиности? Да ли се складиштењем биометријских отисака свих грађана у базу података шаље порука да смо сви сумњиви док се не докаже супротно? Да ли је ово први корак ка својеврсном Паноптикону и (над)држави тоталног надзора? Какве су импликације на слободу грађана у будућности, у смислу неговања опортунистичког етоса ка технократским инстанцама, чија се моћ оваквим пројектима повећава? То су права питања на које ова студија тражи одговор, због чега је акценат на друштвеним импликацијама, а не чисто технолошким манама или преимућствима, мада ни оне нису запостављене.

За сагледавање овог проблема у свим његовим димензијама потребно је и мало визионарског духа. Проблем није толико у томе шта овај пројекат јесте данас, већ у ономе у шта он лако може да прерасте сутра. Ово је прави разлог због кога се академски грађани широм света деценијама боре против сличних концепата, знајући да већ сутра можда неће бити у могућности да се изборе за друштво слободних грађана јер ће температура тоталитарног окружења можда бити доведена до тачке кључања, а виталне функције колективног критичког апарата савременог друштва онеспособљене.

Циљ студије је у обрађивању тематике биометријских система идентификације на начин који је примерен научној методологији, с обзиром да тренутно не постоји ни једна нама позната критичка студија ове тематике урађена од стране српског аутора која би имала комплетну критичку апаратуру. У складу са овим циљем је и жеља да се академска јавност укључи у дебату у вези са адекватном имплементацијом идентификационог система у Републици Србији, с обзиром на велики број критика које су упућене владином предлогу. У том контексту, ову студију треба посматрати као позив академским грађанима да покажу своју одговорност по овом питању, али и позив владајућим структурама друштва за заједничко и конструктивно одређивање према овој проблематици.

Студија је конципирана тако да полази од најбитнијих терминолошких одређења везаних за биометријске системе идентификације, систематско излагања теоријских аспеката и њихово довођење у везу са реалним светом. Други део студије се односи на критичку анализу биометријских система идентификације. Трећи део представља фактографско-аналитички преглед имплементације биометријских система идентификације у свету. Четврти део студије представља фактографску, аналитичку и критичку студију стања у Републици Србији, са посебним нагласком на хронологију грађанског отпора. У додацима на крају студије изнети су делови изабраних научних студија, закључци стручних скупова, препоруке стручних тела и релевантни чланци. Финални закључак студије је формиран у таксативном облику. Методолошки гледано, ова студија у себи садржи доста фактографског материјала, али искључиво као подлогу за аналитички и критички приступ који је суштински, пошто суве чињенице без промишљања не дају пуно.

Зарад прегледнијег критичког апарата, изостављене су информације о тачном датуму приступања свакој појединачној интернет адреси, иако према прихваћеним конвенцијама тај податак треба да стоји уз сваку референцу. Уместо конкретног навођења датума приступања, доступност свих наведених линкова у критичком апарату је проверена током децембра месеца 2006. године (а за неколико линкова и током јануара 2007). Уз то, сви коришћени материјали су ускладиштени у архивама аутора студије и издавача.

Надам се да ће, у облику и обиму у коме је написана, ова студија бити од користи не само академској расправи о проблематици биометријских система идентификације, већ да ће њени закључци имати утицаја и на конкретну имплементацију система идентификације у Републици Србији. Такође се надам да ће спорни закон бити поново размотрен, како у Парламенту Србије тако и на Уставном суду, те да ће се одлуке о њему доносити у складу са научним чињеницама и потребама нашег друштва.

Следујући научној лојалности, желим да се захвалим својим рецензентима (по хронолошком реду добијања рецензије) и да појединачно наведем њихов допринос овој студији.

Мр Драган Спасић, стручњак за сертификациона тела и дигиталне (електронске) сертификате, је дао важне сугестије у вези са пожељном терминолошком супституцијом у неколико случаја, две битне корекције и неколико допуна везаних за област e-government-а. У контексту коришћених референци, указао је на неколико веома битних Интернет адреса на којима су се налазиле студије и стручни часописи од великог значаја за овај рад.

Информатички стручњак Никола Марковић, председник *Друштва за информатику Србије*, је указао на потребу консеквентног испуњавања неколико методолошких принципа за израду ове студије. Дао је и предлоге по питању одређених места која захтевају терминолошку разраду и појашњење. Уз то, садржајности студије је допринео допунским информацијама у вези са ставом институције којом председава и тренутном законском подлогом када је реч о заштити података о личности у Републици Србији.

Политиколог Александар Павић, један од оснивача невладине организације *За живот без жита*, је указао на велики број материјала из англосаксонске праксе (са посебим акцентом на Real ID Act), упутио на неке од водећих британских политиколошких часописа и дао важне сугестије из политиколошког аспекта у вези са биометријским пројектом у Републици Србији. Уз то, самоиницијативно је предузео и део рада око коректуре, превео неколико важних докумената са енглеског језика који су инкорпорирани у последњем делу књиге и абстракт студије на енглески језик.

Дејан Николић, директор београдске канцеларије фирме *F-Secure* и стручњак за безбедност информационих система, је дао неколико битних опсервација из његове уже области.

Адвокат Драгољуб Ђорђевић, потпредседник Управног одбора Адвокатске коморе Србије, је указао на две терминолошке допуне и исправке из области правне теорије, као и на тренутно постојећи законски оквир у Републици Србији када је заштита података у питању.

Историчар Александар Раковић, управник Информационо-документационог центра Православног богословског факултета у Београду, је дао више важних сугестија приликом формирања критичког апарата студије.

Др Ксенија Кончаревић, професор руског језика на Православном богословском факултету, је превела абстракт студије на руски језик.

Од посебног значаја за израду овог рада биле су студије и чланци професора Роџера Кларка (Аустралијски национални универзитет) и стручни извештаји Лондонске школе економије и политичких наука (LSE).

Свима које сам навео, али и онима који имају заслуге за ово дело, а које сам можда заборавио, на овај начин се од срца захваљујем.

О Богојављењу, 2007. године,
Оливер Суботић

Biometric Systems of Identification: A Critical Study

ABSTRACT: The topic of biometric systems of identification has been a controversial one in global public opinion for the past several years; in Serbia it gained currency as soon as the government announced the introduction of a new type of identification cards tied to a central database. Technically speaking, the essence of the problem lies precisely in the central database as the invisible foundation of the system. However, the technical background, although important for understanding the problem, is merely a surface manifestation of a conceptual problem dealing with the relationship between the state and its citizens. Does the storing of biometric fingerprints of all the citizens in a central database send the message that we are all under suspicion until proven otherwise? What are the problem areas associated with this concept in the broader sense? Is its introduction a first step toward a total surveillance state? What are the concrete examples of biometric system implementation in other parts of the world, and what are the differences between them? What is the next evolutionary step of these systems if uncritical implementation is allowed today? These are just some of the questions to which an answer may be obtained only through a critical reappraisal of biometric systems of identification from various aspects, before all from the security, informational, ethical and legal aspects.

KEY WORDS: biometrics, identification, authentification, central biometric database, identity theft, security, fight against terrorism, right to privacy, protection of personal data, total surveillance, electronic services, biometric identification cards, biometric passports, social implications.

Биометрические системы идентификации: критическое рассмотрение

ABSTRACT: Биометрические системы идентификации уже неколько лет являются предметом оживленных дискуссий и споров в мировой общественности. В Республике Сербии данная тема стала актуальной сразу же после заявления властей о намерении ввести в обиход новые паспорта с центральной базой биометрических данных. Существенная проблематика в технологическом отношении связывается как раз с центральной базой как с невидимой основой системы. Однако, технический фон, несмотря на всю его важность для понимания данной проблематики, является лишь проявлением проблемы концептуальной природы, касающейся отношения между государством и гражданами. Здесь возникает несколько ключевых вопросов: дает ли накопление биометрических отпечатков пальцев всех граждан в центральной базе данных основание выдвинуть предположение о том, что все мы сомнительны, пока не будет доказано противоположное? Каковы проблематичные точки данного концепта в более широком смысле? Является ли его введение первым шагом на пути к государству тотального контроля? В чем состоят конкретные специфические особенности внедрения биометрических систем в разных странах мира и в каких отношениях наблюдаются дифференциальные черты? Что будет следующей иттерацией данных систем, если сегодня будет позволено их некритическое внедрение? Это лишь часть вопросов, на которые можно ответить лишь критическим перерассмотрением биометрических систем идентификации с разных аспектов, в первую очередь с точки зрения безопасности, а также из информационной, этической и юридической перспективы.

КЛЮЧЕВЫЕ СЛОВА: биометрика, идентификация, автентификация, центральная база биометрических данных, кража идентичности, безопасность, борьба против терроризма, право на приватность, охрана данных о личности, тотальный контроль, электронные сервисы, биометрические паспорта, биометрические заграничные паспорта, общественные импликации.

Листа скраћеница

BETR – Patrice-Emmanuel Schmitz, Roberto Tavano, Juliet Lodge, Ronald Huijgens & al., *Biometrics in Europe - Trend Report 2006*

FIDISD3.2 – FIDIS, *D3.2: A study on PKI and biometrics*

FIDISD3.6 – FIDIS*, D3.6*: *Study on ID Documents*

HCICT – House of Commons Science and Technology Committee, *Identity Card Technologies: Scientific Advice, Risk and Evidence*

LSEIP – London School of Economics and Political Science, *The Identity Project, An assessment of the UK Identity Cards Bill and its implications*

MBID – Damien Dessimoz, Christophe Champod, Jonas Richiardi, Andrzej Drygajlo, *Multimodal Biometrics for Identity Document State-of-the-Art*

NICC – Standing Committee on Citizenship and Immigration, *A national identity card for Canada?*

RSS – Kirstie Ball, David Lyon, David Murakami Wood, Clive Norris, Charles Raab, *A Report on the Surveillance Society*

Терминологија, историјат и теоријски концепти биометријских система идентификације

Уобичајено је да се наметљиве и дехуманизоване технологије (попут генетског тестирања и манипулације, еугенике) прво пробијају у контексту економских добитака и немогућности њиховог одбијања. Популарне метафоре за овај процес су „танки крај клина“ и жаба скувана у води која се постепено загрева.

Roger Clarke, „Chip-Based ID: Promise and Peril“

Да би се проблематика биометријских система идентификације темељно обрадила, потребно је кренути од основне терминологије. Терминологија везана за ову област је широко прихваћена, осим у неколико случајева, који ће бити посебно назначени у критичком апарату. Поред терминологије, потребно је обратити пажњу и на историјат биометријских метода идентификације, јер се тиме стиче права представа о њиховој генези. И на крају, потребно је обрадити теоријске аспекте ове проблематике у техничком смислу, јер је без њиховог познавања немогуће кренути у критичку анализу.

1.1 Појам и историјат биометријских метода идентификације

Појам „биометрија“ може имати различита значења зависно од контекста у коме се користи. Етимологија речи говори да је у питању мерење биолошких особина одређеног организма (од грч. имен. ὁ βίος – живот и гл. μετρέω (поимен. ἡ μέτρησις) – мерити (поимен. мерење)).

Појам идентификација (од лат. identificare – установљење идентичности, истоветности) у савременом друштву одражава повезаност одређеног податка о личности са њом самом. Из наведеног произилази да су биометријске методе идентификације грађана базиране на мерењу одређених својстава организма специфичних за сваког човека, зарад потврђивања његовог идентитета у друштено-институционалном смислу.

Ове методе су у свом рудиментарном облику биле познате и древним народима, какви су Сумерци и Египћани.[1] С тим у вези, у време фараона су узимане физичке карактеристике поданика,[2] док су у Вавилонском царству трагови отисака прстију на глиненој табли коришћени приликом склапања послова.[3] Својеручни потпис, који представља основу за сваку пословну трансакцију и потврду аутентичности документа, такође се користи вековима. Током прошлог века класична дводимензионална слика лица, креирана помоћу фотографског апарата, уводи се у велики број земаља као саставни део најбитнијих докумената. Отисци прстију у криминалистици први пут почињу да се користе у 19. веку,[4] док у 20. веку њихова употреба у оквиру у криминалистичких база података доживљава праву експанзију.[5]

Крајем 20. и почетком 21. века листа биометријских података и начин њихове обраде значајно се проширују, због могућности које су понудиле са-

---

[1] Julian Ashbourn, *The Societal Implications of the Wide Scale Introduction of Biometrics and Identity Management*, Background paper for the Euroscience Open Forum ESOF 2006, Минхен 2006, стр. 4. Студија је преузета са адресе: www.statewatch.org/news/2006/jul/biometrics-and-identity-management.pdf.

[2] Simon G. Davies, „Touching Big Brother: How biometric technology will fuse flesh and machine“, Privacy international, 1996. Чланак је преузет са адресе: http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-61904.

[3] Marie Shroff, „Trans Tasman Standardisation for Biometrics“, ауторизовано излагање комесара за приватност Новог Зеланда у оквиру групне теме, Конвенциони центар, Велингтон, Нови Зеланд, 1. октобар 2004, стр. 1. Документ је преузет са адресе: www.privacy.org.nz/filestore/docfiles/652009.pdf.

[4] Malcolm Crompton, „Biometrics and Privacy: The End of The World as We Know It or The White Knight of Privacy?“, ауторизована и публикована верзија излагања аустралијског комесара за приватност на конференцији Biometrics – Security and Authentication, Сиднеј, 20. март 2002, стр. 4. Документ је преузет са адресе: http://www.privacy.gov.au/news/speeches/sp80notes.pdf. – Аутор наводи да је француски полицајац Алфонс Бертиљон (Alphonse Bertillon) први искористио биометријски отисак за потребе полицијских органа 1879. године. Бертиљон је тада сугерисао да се за прецизну идентификацију људи могу користити мере различитих делова тела.

[5] Tony Bunyan, „While Europe sleeps“, *ECLN Essays no. 11*, 2005, стр. 4. Есеј је преузет са адресе: http://www.statewatch.org/news/2005/oct/ecln/essay-11.pdf . – Највећу базу података отисака прстију данас поседује FBI и она броји око 45 милиона отисака везаних за криминалне досијее или места злочина.

времене информационе технологије. Данашњи комерцијално расположиви биометријски системи идентификације могу имати могућност обраде слике лица из неколико перспектива, дигиталног отиска прстију (са фиксирањем кључних тачака и превоја),[6] облика руке, шаке и прстију, својеручног потписа у дигиталном облику (који поред простог графичког облика може инкорпорирати и специфичну динамику писања)[7] и скена очне рожњаче.[8] Најсавременији биометријски системи идентификације иду корак даље и обухватају могућности генерисања тродимензионалног модела лица, препознавање распореда вена, анализу ДНК структуре, детекцију мириса и специфичних хемијских својстава коже за сваког човека.[9] Иако одређени број аутора тврди да се и гласовна компонента може користити као поуздана биометријска информација,[10] то пракса и многи стручњаци поричу.[11]

Узевши све наведено у обзир, биометријске податке можемо поделити на оне који одређује физиолошку компоненту (тј. пасивну, у коју спадају фиксиране особине организма какве су отисци прстију, скен рожњаче итд) и на оне који одређује компоненту понашања (тј. активну, у коју спадају потпис, динамика тела и сл).[12]

Гранични тип биометрије је тзв. „мека“ (*soft*) биометрија, која даје биолошке информације помоћу којих се не може направити прецизна разлика у односу на друге људе (пол, боја очију и косе, висина итд), али се често

---

[6] Damien Dessimoz, Christophe Champod, Jonas Richiardi, Andrzej Drygajlo, *Multimodal Biometrics for Identity Document State-of-the-Art*, Research Report, PFS 341– 08.05, Version 2.0, 2006, стр. 70. Студија је преузета са адресе: http://www.europeanbiometrics.info/images/resources/90_264_file.pdf. У даљем тексту *MBID*.

[7] Roger Clarke, „Biometrics and Privacy“, верзија од 15. априла 2001. Рад је преузет са адресе: http://www.anu.edu.au/people/Roger.Clarke/DV/Biometrics.html.

[8] Simon G. Davies, нав. дело.

[9] Patrice-Emmanuel Schmitz, Roberto Tavano, Juliet Lodge, Ronald Huijgens & al., *Biometrics in Europe - Trend Report 2006*, Брисел 2006, стр. 23. Студија је преузета са адресе: http://www.europeanbiometrics.info/images/resources/112_165_file.pdf. У даљем тексту *BETR*.

[10] Исто, 22.

[11] У оквиру међународне конференције „Smart e-government 2006, Elektronski identitet i servisi e-Uprave“, одржане 25–26. октобра 2006. у хотелу Interkontinental у Београду, на округлом столу под називом „Elektronski identitet u e-Upravi i zaštita privatnosti“, др Владо Делић, експерт за превођење гласа у рачунарски текст (и обрнуто) са Факултета техничких наука у Новом Саду, поставио је питање да ли је гласовна компонента валидан биометријски податак за идентификацију одређене особе. Представник Белгије, професор Дени де Кок (*Danny De Cock*), један од аутора пројекта BELPIC (*Belgian Electronic ID Card Project*), категорично је одбацио ту могућност, наводећи практичан пример да његов глас и глас његовог оца преко телефона не разликује чак ни његова мајка.
Посебан проблем гласовне компоненте је несталност која зависи од здравственог стања организма (прехладе, промуклости итд.) које често може варирати (*прим. О.С*).

[12] FIDIS, *D3.2: A study on PKI and biometrics,* стр. 21. Студија је преузета са адресе: http://www.fidis.net/fidis-del/period-2-20052006/d32/. У даљем тексту *FIDISD3.2*. – FIDIS (*Future of Identity in the Information Society*) је пројекат ЕУ чији конзорцијум чине престижне европске академске установе, истраживачки центри и информационе компаније.

користе као комплементаран скуп информација.[13] Додатно, треба знати да су неки биометријски подаци више, а неки мање променљиви током времена (фацијални подаци спадају у прву категорију, док скоро непроменљива ДНК структура спада у другу).[14]

Најновији експерименти везани за биометријску идентификацију грађана, који се изводе у неким британским и америчким градовима, интерактивно комбинују сигнал камера високе резолуције које су постављене на јавним местима (тзв. CCTV – *Closed Circuit TV*) са алгоритмима за препознавање лица, специфичних покрета и динамике кретања. Циљ је, према речима владиних службеника, да се једног дана добије систем за интерактивно препознавање сваког пролазника и сузбијање *потенцијалних* криминалних активности.[15]

Поред тога што се могу узимати нови видови података, у спрези са информационим технологијама стари биометријски подаци постају далеко сложенији. Примера ради, слика у дигиталном формату се најчешће узима из неколико перспектива и носи са собом одређени број фацијалних информација (размак између зеница, физичке карактеристике носа, јагодица и слично); својеручни потпис у стандардном облику подразумева само графички облик на неком материјалу, док се у рачунарском биометријском систему често мери и динамика потписа, редослед слова, специфичан притисак; отисак прста у дигиталном формату прецизно фиксира и одређени број карактеристичних тачака и превоја, без којих је немогућа аутоматска обрада итд.[16]

С тим у вези, многи стручњаци биометријске системе идентификације у савременом свету гледају само у ужем смислу, одбацујући њихове „претке“ у рудиментарном облику. Такве савремене системе дефинишу као *аутоматизоване, углавном рачунарске системе, који користе различита физиобиолошка својства и/или мерења понашања људског тела која се могу користити за конкретну идентификацију одређене особе*.[17]

У овој студији ће се надаље о биометријским системима идентификације говорити управо у контексту аутоматизованих рачунарских система, с обзи-

---

[13] Исто, 18.

[14] A. Michael Froomkin, *The Uneasy Case for National ID Cards*, Draft, University of Miami School of Law, март 2004, стр. 6. Студија је преузета са адресе: http://personal.law.miami.edu/~froomkin/articles/ID1.pdf.

[15] Kirstie Ball, David Lyon, David Murakami Wood, Clive Norris, Charles Raab, *A Report on the Surveillance Society,* Full Report, 2006, стр. 24. Извештај је преузет са адресе: http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf. У даљем тексту *RSS*. – У питању је извештај сачињен за британског комесара за информације у септембру 2006. године.

[16] Marc Watkins, „What are biometric systems?“. Чланак је преузет са адресе: http://www.cippic.ca/en/faqs-resources/biometrics/#faq_what-are-bs. – Текст је састављен испред *Canadian Internet Policy and Public Interest Clinic* (CIPIC), установљене у оквиру Правног факултета Универзитета у Отави.

[17] Исто.

ром да је то de facto биометријски систем идентификације који се данас уводи или предлаже за увођење у неким земљама света.[18] Из наведеног разлога, студија неће узимати у обзир методе идентификације који биометрију не меморишу у електронском облику погодном за аутоматску обраду.

1.2 Идентификација, аутентификација и аутентификација идентитета

Пре било какве конкретне анализе, потребно је направити додатне терминолошке дистинкције везане за област идентификације. Сам појам „идентитет“ није лако дефинисати, јер се у томе не слажу ни све доктрине. Информатички стручњаци ширег образовања с правом говоре о томе да је идентитет метафизички појам, те да не може незамршено бити повезан само са физичким својствима.[19] Стога повезивање идентитета у искључивој вези са физичким својствима представља својеврсан редукционизам са материјалистичким предзнаком. Различите философске доктрине имају различит поглед на ово питање, док се теолошки ставови по питању идентитета такође разликују и зависе од религије и деноминације.[20] Ипак, за потребе ове студије, морамо се ограничити на идентитет онако како га гледају државне институције, који као такав мора бити осиромашен свог пуног значења, јер данас у друштвено-правном смислу другачије тешко може бити дефинисан.

У контексту тако одређеног идентитета, информације о личности се често разлажу на три компоненте: *атрибутивну* (име и презиме, датум и место рођења, место пребивалишта...), *биографску* (детаљи везани за запослење, школску спрему, финансијске трансакције...) и *биометријску* (лични биометријски подаци попут слике, потписа, отисака прстију...).[21] По питању наведених података, могла би се увести и другачија класификација, у смислу *података о личности* и *личних података*, која се често користи када се прави разлика између биометрије (која је лична особеност, тј. лични податак) и других типова података (који говоре о личности, али нису физички део ње саме).[22]

---

[18] Конкретне имплементације биометријских система у свету су обрађене у 3. поглављу.

[19] Stephen Mason, „Is there a need for identity cards?“, стр. 3. Чланак је преузет са адресе: http://www.compseconline.com/free_articles/cfs_IDcards.pdf.

[20] Примера ради, Западна и Источна Црква су одувек имале различит поглед на питање идентитета. Прва је (следујући традицији чији је родоначелник био блажени Августин) антрополошку основу идентитета проналазила у индивидуи и њеној самосвести, док је друга (следујући кападокијској богословској традицији, чији је један од утемељивача био свети Василије Велики) то посматрала у контексту заједнице и односа са другим као конститутивног чиниоца за личност. За дубље разматрање ове проблематике погледати предавања Ј. Зизиуласа објављена у оквиру зборника *Догматске теме,* Беседа, Нови Сад, 2001.

[21] Cabinet Office UK, *Identity fraud: A Study*, Лондон 2002, стр. 9. – Ово је одређење које је дато у званичној студији владиног кабинета Велике Британије. Студија је преузета са адресе: http://www.identitycards.gov.uk/downloads/id_fraud-report.pdf.

[22] Roger Clarke, „Biometrics and Privacy“.

У том контексту, *идентификација* представља процес у коме се помоћу одређеног броја мање или више дистинктивних података једнозначно утврђује идентитет одређене особе у конкретном друштву (тј. *ко* је та особа).

Аутентификација (потврда аутентичности) представља процес у коме се успоставља одређени степен сигурности у складу са тврђењем одређене особе зарад постизања различитих циљева.[23] Иако дефиниција делује помало сложено, у пракси процес аутентификације сви користимо. Најбољи пример је провера овлашћења одређене особе за неку радњу, *без* уласка у конкретни идентитет те особе. У контексту пословања, рецимо, то може бити провера да ли је особа овлашћена да продаје одређене производе, да ли може да заступа одређену фирму, да ли има довољан број година да би купила одређени производ (за цигарете или алкохолна пића граница је најчешће 18 година, рецимо). Суштина је, дакле, у ономе *за шта* је одређена особа овлашћена, а не *ко* је та особа. У српском језику није обичај да се за овај процес користи појам „аутентикација", мада се у неким круговима користи.[24] Иако је то граматичко, а не техничко питање, оно ипак може унети забуну приликом упоредног разматрања тог концепта.[25] Уз то, вреди и напоменути разлику између аутентификације и *ауторизације* у контексту коришћења рачунарског система – прва представља својеврсно „пријављивање" на систем, док друга представља ниво овлашћења које корисник има после пријављивања.

Аутентификација идентитета (код аутора који су наклоњени употреби биометријских система наилази се на појам „верификација")[26] је процес провере у коме се успоставља одређени степен сигурности да је конкретна особа управо та за коју тврди да јесте.[27] Дакле, то је идентификовање одређене особе уз помоћ процеса аутентификације, односно процес аутентификације у коме је сама потврда везана за идентитет личности. Ово је могуће

---

[23] Исто.

[24] Погледати о томе у часопису Матице српске *Језик данас*, бр. 17, у чланку под називом „Језичке недоумице", на стр. 29. Часопис је преузет са адресе: http://www.maticasrpska.org.yu/download/danas17.pdf.

[25] Такво погрешно терминолошко решење налази се у брошури урађеној за потребе Министарства унутрашњих послова Републике Србије, представљеној на конференцији YU INFO 2006, ауторâ Sunčica Nešić, Vojkan Nikolić, под називом „Elektronski identitet građana i mogućnosti njegove primene", Београд 2006. Публикација се налази се на листи YU INFO 2006 радова на адреси: http://www.edrustvoscg.org.yu/radovi2006.htm. – У наведеном раду се користи појам „аутентикација" уместо „аутентификација". То, наравно, није нека крупна грешка, с обзиром да не мења суштину ствари и очигледно је настала под утицајем текстова на енглеском језику. Проблем је што може унети забуну приликом поређења различитих стручних студија на српском језику из ове тематике. У наведеном проспекту се такође примећује честа употреба терминологије коју користе компаније које производе биометријске системе идентификације (примера ради: појам „верификација" уместо „аутентификација идентитета").

[26] Roger Clarke, „Biometrics and Privacy".

[27] *MBID,* стр. 10.

учинити помоћу више аутентификатора било да је то преко нечега што особа зна (PIN код, лозинка), нечега што она ради (то је релевантно код процеса где се захтева својеручни потпис), нечега што има (идентификациони документ са одговарајућим подацима) или нечега што је њено лично својство (биометрија, за коју неки критички настројени аутори у овом контексту користе термин „аутентификација ентитета“).[28]

1.3 Начин остваривања биометријских система идентификације у пракси

У биометријским системима идентификације подаци могу бити смештени и обрађивани комбиновањем различитих метода. У мањем броју случајева, они се налазе само у одвојеној бази података, док у предмету коју корисник поседује као лични документ постоји одређени кључ (податак) за приступ делу базе која се једнозначно односи на њега. У случају *smart* карти,[29] на меморију микроконтролера су често смештени и биометријски подаци који могу (а не морају) бити дуплирани и у позадинској бази.[30] Сама позадинска база може бити реализована на локалном нивоу (рецимо, у фирми где запослени ради) или у ширем виду (на нивоу друштвеног сектора, рецимо).[31]

Предмет који користимо приликом идентификације (било ког да је типа) се у стручној литератури зове *token*[32] (тај материјални носилац података је, рецимо, лична карта, возачка дозвола, пасош, било у каквом да су облику). Биометријски систем идентификације уопште не мора бити базиран на token-има, јер се биометријски подаци могу директно узимати на лицу

---

[28] Roger Clarke, „Identification and Authentication Fundamentals“, верзија од 22. августа 2003. Чланак је преузет са адресе: http://www.anu.edu.au/people/Roger.Clarke/DV/clpc030908.html.

[29] Smart карте зависно од сложености могу имати само меморијски чип или пак микропроцесор са меморијом. Ове потоње представљају минијатуран рачунар, због чега и имају име „паметне карте“, док оне које имају само меморију можемо слободно назвати и „глупе“, јер могу само да памте податке, али не и да их обрађују. Нажалост, разлика између ове две технологије се ретко прави у колоквијалном говору. Друга веома битна дистинкција коју треба имати на уму је разлика између контактних и бесконтактних технологија. Технологија бесконтактних чипова се најчешће базира на радио вези којом се подаци шаљу (нема физичког контакта са читачем), док је за читање података са контактних smart чипова потребан физички контакт са читачем. Основне стандарде за smart карте дефинише ISO/IEC (*International Organization for Standardization / International Electrotechnical Commission*). Иако се често може чути да су smart карте практично непробојне, у стручној литератури се редовно наводе три могућа нивоа напада, од којих се напад на логичком нивоу криптоанализе и убацивања „тројанаца“ показао као најопаснији. Међутим, треба навести и да су реакције произвођача опреме углавном брзе и адекватне, у смислу имплементирања великог броја сигурносних мера. Погледати о томе: FIDIS*, D3.6*: *Study on ID Documents*, стр. 44. Студија је преузета са адресе: http://www.fidis.net/fidis-del/period-2-20052006/d36/. У даљем тексту *FIDISD3.6*.

[30] Roger Clarke, „Chip-Based ID: Promise and Peril“, верзија од 27. септембра 1997. Рад је преузет са адресе: http://www.anu.edu.au/people/Roger.Clarke/DV/IDCards97.html.

[31] Roger Clarke, „Biometrics and Privacy“.

[32] A. Michael Froomkin, нав. дело, стр. 3.

места и сравњивати са позадинском базом биометријских података.[33] Такође, може постојати и супротан случај постојања искључиво token-а (документа) без икакве базе биометријских (или других) података ван њега.

У случају када се приликом идентификације претражује позадинска база, користи се метод упоређивања биометрије који се означава као 1:n („*један према више*“). То значи да се идентитет особе проналази тако што претраживачки алгоритам упоређује биометријски узорак особе узет на лицу места са узорцима свих грађана који су претходно снимљени у бази.[34]

Уколико не постоји позадинска база биометријских података, тада имамо случај 1:1 („*један према један*“) идентификације, тачније аутентификације идентитета са коришћењем биометрије као „јаког“ механизма за потврду.[35] У том случају се врши упоређивање између биометријског отиска особе на лицу места и податка агрегираног у token-у (тј. микрочипу на карти).[36] То практично значи да биометријски подаци суштински не одлазе ван електронске карте имаоца података нити постоје на неком другом месту осим на самој карти грађанина, те да је ималац карте и теоријски и практично потпуни и одговорни власник својих биометријских података у електронском облику.

Дакле, у зависности од ова два модела, приликом провере идентитета (рецимо, узимањем отиска прста на скенеру) подаци се могу упоређивати: 1) пролазом кроз комплетну базу података чија величина зависи од броја корисника; 2) само са претходно унетим подацима за одређену особу који се налазе на token-у (микроконтролеру карте, рецимо); 3)комбинованим начином, уколико један од претходно наведених закаже из неког разлога.

Приликом идентификације помоћу биометријских података у неким научним студијама се наводе два регулаторна принципа.

Први је тзв. *позитивна идентификација*. Она се користи када треба спречити појаву да више корисника има један идентитет, јер се подразумева да не постоје две особе са идентичним биометријским подацима. Циљ је, дакле, потврдити ко *јесте* одређена особа.

Негативна идентификација се користи када треба потврдити да одређена особа *није* та са којом се врши поређење, што се користи код спречавања да једна особа има више идентитета под једним биометријским податком.[37]

Системи базирани на првом принципу и теоријски и практично могу бити у оквиру 1:1 идентификације и то на добровољној основи (јер се упо-

---

[33] Исто.

[34] *MBID,* стр. 10.

[35] Roger Clarke, „Authentication: A Sufficiently Rich Model to Enable e-Business“, верзија од 26. децембра 2001. Рад је преузет са адресе: http://www.anu.edu.au/people/Roger.Clarke/EC/AuthModel.html.

[36] *MBID,* стр. 10.

[37] Исто.

редо може користити и алтернативни модел идентификације). Други принцип подразумева позадинску базу података тј. обавезујући пролаз 1:n и најчешће нема алтернативни модел идентификације.[38]

1.4 Фактори безбедности биометријских система идентификације

У случају постојања позадинске базе података (систем 1:n), фактор безбедносног ризика коришћења базе података је одређен комплексношћу система, бројем корисника базе, опсегом осетљивих информација које се чувају у њој, степеном повезаности са осталим рачунарима (понајпре Интернетом), као и примамљивошћу података за спољни упад.[39] Додатно, питање броја људи који су укључени у рад система[40] и квалитета криптографске заштите који се примењује на податке (квалитет система енкрипције/декрипције података)[41] су такође једнако битни параметри.

Готово сви информатички стручњаци се слажу да је најсигурнији систем (по питању безбедности и приватности биометријских података грађана) онај у ком подаци не напуштају карту. Прецизније речено, то је систем у коме не постоји позадинска централна база података и у коме је ималац карте потпуни и одговорни власник биометрије у електронском облику.[42] То би према претходно изложеним пропозицијама био концепт 1:1 „јаке“ аутентификације идентитета.[43]

---

[38] Исто.

[39] London School of Economics and Political Science (LSE), *The Identity Project, An assessment of the UK Identity Cards Bill and its implications*, Version 1.09, Лондон, јун 2005, стр. 188. Студија је преузета са адресе: http://www.csrc.lse.ac.uk/idcard/identityreport.pdf. У даљем тексту *LSEIP*.

[40] Исто, 191.

[41] Roger Clarke, „Message Transmission Security“, верзија од 11. маја 1998. Рад је преузет са адресе: http://www.anu.edu.au/people/Roger.Clarke/II/CryptoSecy.html; додатно погледати и: Branko Nikitović, „Put do sigurnih podataka“, PC, бр. 128, PC Press, Beograd, 2007. – Шифровање (енкрипција) је механизам којим се информација претвара у шифровану форму, док је дешифровање (декрипција) обрнут процес и служи за враћање шифроване у читљиву форму. Ове конверзије се извршавају преко специјалног податка који се зове *кључ*, који може бити различите дужине (зависно од које постоје јаке и слабе шеме шифровања). *Симетрични* алгоритми у криптографији користе исти кључ за шифровање/дешифровање (тзв. *тајни кључ*), док *асиметрични* алгоритми (или понегде у литератури *алгоритми јавног кључа*) користе различите кључеве за шифровање и дешифровање података. Симетрична шема је постојала у свом основном облику још пре 2000 година. Код ње је одувек највећи проблем био то што тајни кључ морају поседовати обе стране, које се претходно морају познавати – уколико тајни кључ дође у посед треће стране, онда су сигурносне мере уништене. Асиметрична шема је пронађена током 70-их година 20. века и базира се на принципу парова кључева, где је један тзв. *приватни* кључ (који зна само власник поруке), а други *јавни* (који могу и треба да знају сви који желе да комуницирају са власником приватног кључа). Власник пара кључева слободно може објавити свој јавни кључ, који ће пошиљаоци порука користити да помоћу њега шифрују поруке. После шифровања поруке јавним кључем једино ће ималац одговарајућег приватног кључа моћи да је прочита.

[42] *MBID*, стр. 29.

[43] Тј. аутентификације идентитета са биометријским механизмом потврде.

1.5 Однос биометријских и небиометријских електронских карти

Биометријске карте не треба мешати са свим врстама електронских карти нити пак са картицама са машински читљивом зоном.[44] Електронске карте које се данас користе за различите сврхе уопште не морају поседовати биометријске податке, што је поготово случај уколико нису идентификациони документ. Оне се најчешће користе за аутоматизовано обављање разних услуга и углавном поседују само *електронски сертификат*, тј. скуп електронских процедура и механизама за потврду аутентичности потписника приликом коришћења карти за потребе електронског пословања.[45] Уз ову проблематику стоји и термин *електронски (дигитални) потпис*, који представља електронску аналогију обичног потписа и кога не треба мешати

---

[44] Ово смо посебно назначили током учешћа на округлом столу „Да ли електронска лична карта угрожава приватност грађана?“, у одржаног у Галерији САНУ 18. јула 2006. године, у организацији *Друштва за информатику Србије*. Терминолошка прецизност је у овом случају веома битна, јер је неправилно и недопустиво поистовећивање свих електронских личних карти и биометријских електронских личних карти (нап. *О.С*).

[45] Оно што је обичан потпис у класичном пословању, то је квалификован електронски потпис у електронском пословању, с тим што електронски потпис (*digital signature*) у себи садржи заштитне механизме који штите интегритет поруке. Наиме, приликом трансмисије поруке морају се обезбедити одређени безбедносни параметри. Најбитнији су *интегритет* поруке (она не сме бити промењена током слања), *аутентификација идентитета* пошиљаоца и примаоца (пошиљалац треба да је сигуран да је порука доспела до назначеног примаоца, а прималац да му порука долази од правог пошаљиоца) и *непорецивост* (онемогућава се порицање извршене трансакције) – то су кључне улоге електронског потписа (детаљније на адреси: http://www.cepp.co.yu/ca).
Према директиви Европске Уније 1999/93/ЕС, усвојене 13. 12. 1999, електронски потпис представља податке у електронској форми који су везани или логички повезани са осталим подацима и користе се као метод аутентификације (погледати *FIDISD3.2,* стр. 8). Према истој директиви, *електронски сертификат* представља електронски атест који повезује податке везане за верификацију потписа са одређеном особом и потврђује идентитет конкретне особе. Квалификовани сертификат према наведној директиви представља онај сертификат који испуњава услове из Анекса I истог документа, а који је обезбеђен од стране услужног сервиса који испуњава за то прописане у слове наведене у Анексу II наведеног документа. Наиме, да би постојала сигурност да је то заиста јавни кључ пошиљаоца, морају постојати тзв. *сертификациона тела*, која треба да обезбеде сигурност да одређени јавни кључ припада тачно одређеној особи и да обезбеде „окружење поверења“. Та сертификациона тела у једној државни могу бити различите компаније, државне установе или пак министарства.Закон и подзаконска акта треба да пропишу услове под којим је електронски потпис еквивалентан обичном (када га зовемо *квалификовани* електронски потпис) и услове које треба да испуне сертификациона тела која издају сертификате за верификацију потписа.
Најзначајније употребе електронског потписа су у електронском пословању (*e-Business*), електронској трговини (*e-Commerce*), електронском банкарству (*e-Banking*) и електронској управи (*e-Government*). За дубљи увод у ову проблематику, поред *FIDISD3.2*, погледати студије професора Роџера Кларка на адреси http://www.anu.edu.au/people/Roger.Clarke/EC/RogersBibl.html. Република Србија је однедавно законски регулисала ову област. Поводом проблематике увођења *Закона о електронском потпису* у Србији додатно погледати: Milan Marković, „Elektronski potpis u Srbiji“, на адреси http://www.emagazin.co.yu/clanak.asp?id=453; Nikola Marković, „Konačno! Usvojen zakon“, EBIT бр. 36, на адреси http://www.ekonomist.co.yu/magazin/ebit/36/por/por2.htm; Branko Nikitović, „Digitalni serfitikati“, *PC,* бр. 129. Закон о електронском потпису и придружена подзаконска акта су објављени на Интернет адреси Народне скупштине Србије (http://www.parlament.sr.gov.yu), Министарства науке (http://www.mntr.sr.gov.yu), као и првог сертификационог тела у Републици Србији – Сертификационог тела Поште (http://www.cepp.co.yu/ca/dokumentacija).

са горе наведеним дигитализованим својеручним потписом – намене и облик су им потпуно другачији.[46]

Узевши наведено у обзир, можемо рећи да је биометријска лична карта само онај тип електронских личних карти који агрегира и карактеристичне биометријске податке њеног имаоца. Иако проблематику електронског потписа и проблематику биометријских система идентификације треба посматрати одвојено, ове две области се могу (а не морају) преплитати. Такав је случај, рецимо, уколико се биометријски подаци користе за „откључавање" електронске карте (уместо шифре или PIN кода рецимо) да би се користила приликом електронских трансакција,[47] мада је то у пракси реткост из више разлога. Електронске карте (било да су биометријске или небиометријске) у контексту остваривања тзв. „електронског идентитета" начелно се могу поделити на три највеће групе: 1) које се користе искључиво за идентификацију; 2) које агрегирају и електронски сертификат; 3) које поред свега наведеног имају могућност коришћења у различитим секторима: здравственом, за потребе социјалног осигурања и сл.[48] Наравно, ову поделу треба узети само условно, с обзиром да није ултимативна и да постоје различити гранични случајеви.

1.6 Прецизност биометријских система идентификације

Када је реч о прецизности биометријских система идентификације, процене су различите.[49] Оне у великој мери зависе од опсега и типа информаци-

[46] Својеручни потпис пребачен у дигитални облик (дигитализован) не треба мешати са електронским потписом. Први представља биометријски идентификатор активног типа који се може користити за физичку идентификацију конкретног човека, док други нема никакве везе са графичким обликом и представља електронску аналогију својеручног потписа, а примену има код успостављања тзв. „електронског идентитета". Њиме се постиже сигурност код коришћења докумената у електронској форми. С тим у вези, оно што је обичан потпис на папирним документима у класичном пословању, то је квалификовани електронски потпис у електронском пословању, с том разликом што електронски потпис у себи садржи заштитне механизме који штите интегритет потписане поруке, као што је то детаљније образложено у претходној функцији.

[47] Graham Greenleaf, Roger Clarke, „Privacy Implications of Digital Signatures", верзија од 10. марта 1997. Рад је преузет са адресе: http://www.anu.edu.au/people/Roger.Clarke/DV/DigSig.html. – За остваривање електронских трансакција коришћењем електронског потписа користи се комбинација асиметричних и симетричних криптографских метода (симетричне методе су у том случају додатак асиметричним као главним, зарад добијања на брзини). Да би само пошиљалац могао да користи приватни кључ у склопу електронске карте (тј. да се не би десило да неко неауторизован користи приватни кључ и тиме користи све ингеренције његовог власника), могу се користити различити механизми за откључавање електронске карте, при чему упоређивање биометрије (са оном складиштеном у карти или другде) може бити један од њих, што је у пракси ретко. Најчешћи начин за откључавање карте у досадашњој пракси је употреба PIN кода или лозинке.

[48] *FIDISD3.6.*

[49] Понегде се наилази на оквирне процене да на 1000 случајева 10 бива погрешно идентификовано, мада је то специфично за сваку појединачну имплементацију и биометријски идентификатор. Према досадашњим искуствима, грешке углавном варирају од 10‰ па чак до 7%, што зависи од низа фактора: типа биометријског идентификатора, прецизности хардверско-софверске платформе, броја упоредних биометријских идентификатора који се узимају итд. Пракса показује да је

ја који се узимају, квалитета опреме за анализу биометријских узорака, као и стања улазног биометријског податка. Примера ради, често постоје проблеми приликом узимања отисака са сувише влажних или сувише сувих руку, које отклањају тек најновији уређаји са технологијом дубинског скенирања.[50] Проблем могу представљати и потоња обољења и оштећења коже која спречавају валидну идентификацију (тј. упоређивање са претходно ускладиштеним отисцима у бази или микрочипу),[51] мада по том питању још увек не постоје адекватне научне студије које би одредиле степен одступања. Уз то, за узимање квалитетне биометријске слике лица (код дводимензионалних система) потребни су и погодни спољашњи услови (попут осветљења).

Бројчани показатељи прецизности су *учесталост погрешног поклапања* (*false match rate*) који показује вероватноћу случаја да ће приликом провере биометрија особе бити повезана са неком другом особом из базе, док *учесталост погрешног непоклапања* (*false non-match rate*) јесте вероватноћа случаја да се биометрија одређене особе не поклопи са оном која се у бази на њу односи.[52]

Генерално гледано, прецизност биометријских система се мери преко три основна показатеља, у контексту вероватноће: 1) да се биометријски податак једног човека повеже са биометријским податком другог човека; 2) да се не препозна садашњи биометријски податак узет од човека са податком узетим одраније; 3) да систем не може прецизно да одреди резултат због слабог квалитета улазних података.[53] Сва три показатеља су релевантна у случају идентификације 1:n, док су друга два показатеља релевантни за идентификацију 1:1.

У сваком случају, ниједан биометријски систем идентификације данашњице није стопостотно прецизан, због чега се класификују у корпус *пробабилистичких метода идентификације*.

Постоје још неки мање важни технички аспекти биометријских система идентификације, али су за даља разматрања у оквиру ове студије неважни.

најмањи проценат грешке углавном код отисака прстију, док је највећи проценат грешке код аутоматског препознавања лица. Који год да су проценти у питању, сви стручњаци се слажу да ниједан биометријски систем идентификације није стопостотно поуздан. Погледати о томе: Canadian Internet Policy and Public Interest Clinic, „How reliable are biometric systems?“, на адреси: http://www.cippic.ca/en/faqs-resources/biometrics/#faq_how-reliable-bio-systems; као и *FIDISD3.6*, стр. 10.

[50] *BETR*, стр.19-20.

[51] *LSEIP*, стр. 175.

[52] Stephen Mason, нав. чланак, стр. 9.

[53] House of Commons Science and Technology Committee, *Identity Card Technologies: Scientific Advice, Risk and Evidence*, Sixth Report of Session 2005-06, Лондон 2006, стр. 12. Студија је преузета са званичног сајта британског парламента, из одељка посвећеног публикацијама, на адреси http://www.publications.parliament.uk/pa/cm200506/cmselect/cmsctech/1032/1032.pdf. У даљем тексту *HCICT*.

Биометријски системи идентификације
– мултидисциплинарна анализа –

Садашња фиксација на идентификационом менаџменту и његовој глобализацији је поприлично чудна, несразмерна његовим наводним бенефицијама и очигледно политички инспирисана. Ово је помало узнемиравајуће, поготову унутар земаља-чланица Европске Уније, за које смо се надали да би заузеле становиште које би се више приклонило обзирима друштва. Као резултат, предлози се на брзину гурају кроз институције без одговарајуће дебате, без разумевања о друштвеним последицама и без ослањања на једну претходно договорену дугорочну стратегију. Морамо да препознамо реалност ситуације пре него што можемо да предузмемо кораке да је побољшамо. Проблем лежи у томе што овде имамо посла са синдромом „царевог новог руха“, где је веома мали број људи спреман да се изјасни и погледа ствари на објективан начин, а још мањи број спреман да слуша. Ова ситуација мора да се промени ако желимо да избегнемо оне негативније стране индентификационог менаџмента.

Julian Ashbourn*, The Societal Implications of the Wide Scale Introduction of Biometrics and Identity Management*

Критичка анализа употребе биометријских система идентификације мора бити мултидисциплинарна, с обзиром да су импликације такође вишеструке. Притом се у обзир морају узети ставови како пропонената ових система, тако и њихових критичара. Оквирно, та анализа треба да буде изведена из етичког, правног, информатичког, безбедносног, економског и политиколошког аспекта, мада се они често преклапају, што је разлог да се ова студија не држи ригидно таксативног концепта и да следи нешто флексибилнији приступ.

2.1 Различите имплементације биометријских система идентификације

Шира употреба аутоматизованих биометријских система идентификације прво је нашла своју примену у криминалистици, за потребе брзог претраживања база криминалних досијеа и упоређивање трагова са места злочина.[1] У протеклој деценији, појављује се примена у потврди идентитета учесника у крупним економским трансакцијама.[2] За идентификацију запослених овај концепт данас користи један број компанија и организација, поготово приликом коришћења сервисâ који захтевају строга овлашћења (добар пример су војне институције).[3]

Постојале су иницијативе за увођење биометријских система идентификације у оквиру специфичних локалитета, али оне су углавном показале мали успех – један од пропалих покушаја је увођење на стадионима ради спречавања хулиганства.[4] У последње време постоје иницијативе за увођење биометријских система идентификације на аеродромима, а као разлог се наводи терористичка претња.[5]

Занимљиво је да неки серијски производи на себи имају скенер за биометријску проверу идентитета корисника (најчешће је у питању скен јагодице прста), ради спречавања неовлашћеног коришћења. То је приметно код најновијих модела аутомобила и преносних рачунара, мада не наилази на посебно одобравање купаца, поготово због непријатних искустава из праксе.[6]

Начелно, принцип употребе биометријске идентификације грађана на нивоу било ког институционалног подсистема (пословног, рецимо) не представља проблем уколико је таква примена прецизно регулисана законом и уколико су запослени или остали релевантни субјекти који су укључени у процес претходно: 1) детаљно обавештени о типу и количини информација коју ће односна организација од њих захтевати; 2) детаљно обавештени о начину на који ће се то чинити; 3) ако нису под принудом условљени да дају биометријске податке ван експлицитног пристанка, што треба регулисати Уговором о раду; 4) уколико нису дискриминисани ако из било ког разлога

---

[1] Malcolm Crompton, нав. дело, стр. 5.

[2] Исто.

[3] Simon G. Davies, нав. дело.

[4] *BETR*, стр. 32.

[5] Скандинавска авио-компанија *SAS* је имплементирала биометријски систем идентификације за контролу уласка и изласка путника, са обавезом да податке одмах обрише пошто путник заврши пут. Погледати о томе: Travelbite, „Scandinavian airline first to use fingerprint scans“, 22. септембар 2006. Вест је преузета са адресе:http://www.travelbite.co.uk/newsbrief/flights/scandinavian-airline-first-use-fingerprint-scans-$452572.htm.

[6] *FIDISD3.2*, стр. 23. – У Куала Лумпуру, 28. марта 2005. године, ауто-мафија је прво присилила власника аутомобила са биометријским системом откључавања да својим отиском прста активира аутомобил, а потом му је прст одсекла.

не желе да дају осетљиве биометријске податке, а имали су могућност избора да их дају или не дају. Ови таксативни услови могу бити проширени, зависно од конкретне ситуације.

Уколико изузмемо видео-надзор (који готово никада није повезан са алгоритмом за аутоматско препознавање лица, па самим тим није аутоматски систем за биометријску идентификацију), биометријска идентификација у оквиру пословног окружења није примарна ствар. Фирме које користе биометрију запослених за регулисање пословних процеса углавном то чине за потврду овлашћења пре него ли прецизне идентификације, јер им није битан толико прецизан идентитет колико ингеренције конкретног субјекта.[7]

2.1.1 Имплементација на (над)националном нивоу: некритички и критички приступ

Прави проблем око кога се ломе копља свуда у слободном свету настаје када се биометријски системи идентификације предлажу за увођење на националном или наднационалном нивоу и то у општеобавезујућем виду.[8] Уколико такав систем прати и централна база биометријских (и њима придружених атрибутивних и биографских) података, онда број проблематичних питања расте експоненцијалном брзином.

Нажалост, у пракси неких земаља (пре свега блискоисточних и далекоисточних) у решавању овог питања грађани и академске институције имају миноран удео и решавају га углавном политичке структуре које ове системе спроводе на бази чистог волунтаризма.

Пропоненти биометријског система идентификације у земљама западне демократије га углавном оправдавају новим условима живљења које намеће глобализација и савремени свет, међу којима тероризам игра главну улогу, али и сустизањем далекоисточних земаља у технолошком погледу.[9] У контексту првог разлога, проблематика тоталне идентификације грађана је на Западу посебно актуелизована након великих терористичких напада у Њујорку, Мадриду и Лондону. Поред аргумента борбе против тероризма, обично се наводи да биометријски системи идентификације представљају најбоље средство против покушаја лажирања идентитета, мада чак и пробиометријски кругови делом прихватају ставове стручних организација које тврде да биометријски системи то не могу спречити.[10]

---

[7] Roger Clarke, „Biometrics and Privacy“.

[8] Исто.

[9] *BETR*, стр. 8.

[10] European Biometrics Portal (EBP), „UK’s debate: ID cards biometrics will not stop forgery“, 20. 2. 2006. Текст је преузет са адресе: http://www.europeanbiometrics.info/news/newsdetail.php?Id_news=113.

Међутим, има нешто што не треба никако запоставити када је друштвена пробојност оваквих пројеката у питању, а то је профит транснационалних компанија.[11] Годинама је приметно све веће форсирање технологије плаћања картицом (тј. безготовинског плаћања), док се у последње време тај принцип лагано покушава заменити са тзв. *biopay* концептом, који подразумева директну употребу биометрије (најчешће узимање отиска прста скенером на лицу места), при чему се купци стимулишу мањим ценама.[12] Притисак компанија које производе биометријске системе идентификације у огромној мери утиче и на политичке структуре које одлучују о спровођењу оваквих мера на националном нивоу.[13] Ове компаније у својим прогнозама очекују велики обрт капитала у годинама које долазе,[14] што је повратни импулс политичким структурама које све мере новцем, често не размишљајући о другој страни медаље.

Насупрот некритичком, интересном и политички вођеном приступу, огроман број академских грађана и светски признатих стручњака из области информационих технологија се противи коришћењу биометријских система идентификације у обавезујућој форми (донекле чак и у добровољној) на нивоу држава и унија. Пре нешто више од две деценије, када су биометријске технологије данашњице још увек биле у експерименталној фази, против некритичке употребе тог концепта за идентификацију грађана прво су реаговали стручњаци из области компјутерског права,[15] а потом организације које се боре за очување права на приватност у условима савременог друштва.[16] Они су пре свега указивали на чињеницу да суштински проблем лежи у чињеници да су предлагачи таквих концепата или људи са директним финансијским интересом или политичари који желе да прошире моћ државног апарата над грађанима.

Аргументе које интересне групе користе за форсирано увођење биометријских система чак и неки пробиометријски настројени писци че-

---

[11] Dan Balaban, Don Davis, Thad Rueter, Kevin Woodward, „The future of smart cards – Top 10 trends“, *CardTechnology*, март 2006, стр. 48. Часопис је преузет са адресе: http://www.cardtechnology.com/attachments/200604054yolcsdx-1-ct_march_2006.pdf. – Индустријски аналитичар Џејсон Халверсон (*Jason Halverson*) најављује да ће тржиште електронских личних карти тек доживети огроман раст.

[12] Donald Davis, „Will That Be Cash, Card Or Finger?“, *CardTechnology*, мај 2006, стр. 36. Часопис је преузет са адресе: http://www.cardtechnology.com/attachments/200605319z8l4fwd-1-ct_may_2006.pdf.

[13] *FIDISD3.2*, стр. 30.

[14] CardTechnology, „Analyst Sees Boom In Identity And Biometric Projects“. Вест је преузета са адресе: http://www.cardtechnology.com/article.html?id=20060921gd6l6j83.

[15] Међу њима је један од најпознатијих др Роџер Кларк (Roger Clarke), информатички стручњак и професор на Аустралијском националном универзитету, чија се академска и професионална референца налази на адреси: http://www.anu.edu.au/people/Roger.Clarke/Person.html.

[16] Најпознатије светске организације тог типа су ACLU (*American Civil Liberties Union*), EPIC (*Electronic Privacy Information Center*), Statewatch, Privacy international, EDRI (*European Digital Rights*), APF (*Australian Privacy Foundation*) i CASPIAN (*Consumers Against Supermarket Privacy Invasion and Numbering*).

сто називају митовима који немају никакво утемељење у реалности.[17] Данас се концепту употребе биометријских система идентификације у тоталном виду поред великог броја научних радника из различитих научних области,[18] опире и одређени број јавних личности.[19] Приметно је да и неке познате светске медијске куће не скривају подозрење и резервисаност.[20]

Који су разлози због којих критичари на питање који је основни проблем код биометријских система идентификације (поготово на (над)националном нивоу), прво кажу: „Чему уопште све то?“, а тек онда „На који начин имплементирати?“.[21] Зашто су све гласнији научни апели да се на биометријске методе идентификације стави мораторијум све док се не успоставе потпуно поуздани правно-технички механизми заштите појединца који је њиме обухваћен?[22] Одговор није једноставан и захтева озбиљно промишљање и укључивање у расправу свих слојева друштва. Критички осврт на коришћење биометријских система идентификације грађана насушна је потреба сваког, па и нашег друштва, јер последице некритичке имплементације могу бити катастрофалне. Наведимо стога неке од најпроблематичнијих тачака концепта биометријских система идентификације на (над)националном нивоу, да би могли да извучемо критички закључак по овом сложеном питању.

2.2 Баријере психолошког, културолошког и верског порекла

Први отпор који се јавља код употребе биометријских система идентификације је психолошке природе. Истраживања показују да постоји психоло-

---

[17] Џулијан Ешбурн (*Julian Ashbourn*), председник управног одбора *Међународне биометријске фондације* (*International Biometric Foundation*), у својим познатим „антимитолошким тезама“ обара велики број заблуда везаних за биометријске технологије. Између осталог, Ешбурн наводи да су *нетачне* тврдње: да биометрија доказује да сте особа која кажете да јесте, да је непогрешива, да не може открити личне информације и да складиштени биометријски подаци нису подложни манипулацији. Ове и остале тезе наведене су у студији *The Societal Implications of the Wide Scale Introduction of Biometrics and Identity Management,* под поднасловом „Dispelling popular myths around technology“ („Разбијање популарних митова о технологији“ – *прев.*) и представљене су на конференцији „Euroscience Open Forum ESOF 2006“ у Минхену јула 2006. године.

[18] Такав пример су професори и стручни сарадници познате британске Лондонске школе економије и политичких наука (LSE), Аустралијског националног универзитета (ANU) и Правног факултета Универзитета у Отави (CIPIC).

[19] Погледати BBC-јев прилог „Pet Shop Boys protest at ID cards“, од 01. 03. 2006, на адреси: http://news.bbc.co.uk/1/hi/uk_politics/4763874.stm.

[20] BBC је у више наврата доносио критичке извештаје о теми биометријских личних карти. Један од таквих чланака под називом „ID plan excessive, says watchdog“ налази се на адреси: http://news.bbc.co.uk/1/hi/uk_politics/4627881.stm.

[21] Погледати „Interview with Dr Ted Dunstone, Director, Biometix Consulting“, од 16. септембра 2000, на адреси: http://www.anu.edu.au/people/Roger.Clarke/dv/BiometixIview.html.

[22] Roger Clarke, „Why Biometrics Must Be Banned“, верзија од 25. августа 2003. Чланак је преузет са адресе: http://www.anu.edu.au/people/Roger.Clarke/dv/Biom030908.html.

шки отклон код одређеног броја грађана, који је највећи код узимања скена рожњаче, а најмањи код препознавања гласа.[23] У западној литератури то се означава као „проблем интрузивности“ биометријских технологија (тј. наметљивости, поготово у контексту нарушавања аутономије приватности).

Други аспект психолошког проблема се не пројављује кроз технолошку сферу, већ кроз *теорију моћи* у оквиру политичке социологије. Наиме, просечан грађанин се увек нелагодно осећа знајући да нека инстанца о њему сакупља велики број података, поготово ако су они осетљивог типа. Теоријски радови и практична искуства показују да то итекако може утицати на његово понашање.[24] Што је већи опсег осетљивих информација које одређена инстанца води о конкретној особи, то се та особа осећа рањивијом и мање спремном на било коју врсту конфликта. То у психолошком смислу ствара човека-конформисту, а у социолошком друштво у коме доктрина опортунизма замењује плурализам и слободу мишљења.

Са друге стране, проблем код „идентификационог менаџмента“[25] који укључује биометријске податке јесте што се у неку руку тиме претпоставља да су сви грађани сумњиви уколико се не докаже супротно, што је фактички насртај на основне поставке демократског друштва и ствара климу неповерења.[26] Ствари се по питању рушења таквих принципа у западном свету развијају страховитом брзином. Само пре неколико година у већини западних земаља је било незамисливо узимање биометријских отисака прстију од обичних грађана, јер је у свести грађана то увек повезивано са криминалцима, док се данас о томе увелико размишља и воде жестоке полемике.

Постоје и баријере које се могу свести под проблем приговора савести. У земљама са већинским хришћанским становништвом, биометријски системи идентификације изазивају подозрење одређеног броја верника због конотација са тоталитарним режимом описаним у Јовановом Откровењу, с обзиром да та врста идентификације донекле може бити окарактерисана као својеврсна технолошка претеча једне од полугâ супер-тоталитарног режима у будућности о коме говори наведена књига Светог писма Новог Завета.

Постоје и потенцијалне културолошке баријере. Примера ради, у Јапану се људи не поздрављају руковањем већ наклоном, што може представљати проблем уколико би јапанска влада једног дана предложила увођење биометрије у идентификациони процес – грађани те земље би могли осећати велику нелагоду код узастопног коришћења истог скенера за очитавање би-

---

[23] *BETR*, стр. 15.

[24] На овај аспект проблема српској јавности је посебно указао проф. др Слободан Антонић, у свом излагању на стручном скупу у Краљеву, у Дому владике Николаја, 30. септембра 2006. године.

[25] Синтагма коју западни социолози користе када је реч о концепту идентификације грађана.

[26] Julian Ashbourn, нав. дело, стр. 13.

ометријских отисака прстију.[27] Сличан отклон постоји у цивилизацијама у којима жене носе вео који не скидају због верских забрана, чиме је онемогућен основни биометријски идентификатор – слика лица.[28]

Посебан отпор се јавља код узимања ДНК као биометријског податка, мада неке земље одавно спроводе репресиван режим по овом питању.[29] Психолошка баријера са ДНК као биометријским идентификатором је у томе што омогућава увид у информације какве су расна и етничка припадност и постојање неких болести (што је мана и код скена рожњаче), док у догледној будућности лако могу искрснути и други проблеми,[30] поготово како истраживања у тој области буду напредовала.[31]

И на крају, последња врста психолошког отклона везана је за стари страх од повреда. Тај страх је приметан код скена рожњаче (јер се неки људи плаше озледе ока при употреби ласерског снопа) или давања отиска прста на скенеру (због страха од кожних болести).[32]

2.3 Продуктивност и злоупотреба као две стране исте медаље

Велика количина биометријских података у електронском облику се може брзо претраживати, копирати, модификовати и укрштати. То и јесте суштинска разлика у односу на њихове претке који нису били складиштени у електронском облику и нису омогућавали узимање специфичних информација за аутоматску обраду. Иако је сасвим јасно да то доводи до великих добитака у брзини обраде и повећању продуктивности рада, критичка анализа брзо показује то може довести и до огромних злоупотреба.[33]

---

[27] *MBID*, стр. 55.

[28] Accenture Technology Labs, „The future of identity: Biometrics solutions to enhance the performance of businesses and governments“, стр. 6. Проспект је преузет са адресе: http://www.accenture.com/xdoc/en/services/technology/vision/future_identity.pdf.

[29] EDRI, „UK DNA Database under scrutiny“, *EDRI-gram 4.21,* 8. 11. 2006. Вест је преузета са адресе: http://www.edri.org/edrigram/number4.21/uk-dan. – Широј јавности је углавном познато да ДНК база података коју британска влада води броји око 3,5 милиона узорака (а постоје прогнозе да би у догледном времену могла да нарасте и на 25% популације), јер полиција узима узорке независно од почињеног незаконитог акта (од вожње у пијаном стању до убиства).

[30] Поред овог проблема, ДНК може посредно служити за прецизно лоцирање трагова сваког грађанина, као и за генетско истраживање ван знања његовог имаоца. Да би се спречила употреба ДНК за потребе генетског истраживања ван знања имаоца, предлаже се да се ДНК узорак уништи пошто је искоришћен за потребе идентификације. Даље се предлаже да базе података ДНК не треба перманентно водити за све грађане (мора постојати одређени рок), већ само за доказане убице и силоватеље. Подразумева се да ова област мора бити прецизно регулисана законом. Погледати памфлет „The police National DNA Database“ организације *Genewatch* на адреси: http://www.genewatch.org/uploads/f03c6d66a9b354535738483c1c3d49e4/leaflet_dna_police_small_1.pdf

[31] A. Michael Froomkin, нав. дело, стр. 9.

[32] Исто.

[33] CIPIC, „Why are biometrics controversial? “. Чланак је преузет са адресе: http://www.cippic.ca/en/faqs-resources/biometrics/#faq_how-reliable-bio-systems.

Здрава логика налаже да готово све око нас може бити злоупотребљено, било да је у питању проста ствар или комплексан систем. Ипак, код биометријских система идентификације ствари су до те мере концептуално сложене да је неумесно поређење са злоупотребом кухињских ножева и аутомобила, што као одговор на овај проблем дају пробиометријски интелектуални кругови.[34] Наведене ствари нису делови институционалног идентитета неке личности већ ствари из спољашњег окружења чији губитак, замена или модификација не доводе до нарушавања интегритета њиховог имаоца, а о поређењу из домена сложености нема ни потребе дискутовати. Замена биометрије у централној бази и укрштање са отисцима са места злочина је нешто што се не може поредити са заменом ствари, па овај аргумент пробиометријских кругова просто разочарава својом наивношћу.

Кључни проблем лежи у чињеници да биометријски подаци (начелно) остају такви какви јесу до краја живота, за разлику од осталих типова података које човек током живота може променити (адреса, број платне картице, запослење...). То практично значи да човек коме је биометрија једном украдена више не може бити заштићен од будуће крађе – покраден је занавек.[35] Једном украдени биометријски податак готово је немогуће изменити или заменити другим, јер он у нормалним околностима остаје скоро идентичан.[36] После крађе овог типа податка немогуће је обезбедити нови и другачији.[37] Додуше, један број података о личности је такође (донекле) неизмењљив, али они су по интегритет личности далеко мање осетљива информација.

Случајеви „крађе идентитета“ могу се драматично завршити по оштећену особу.[38] Постоји више документованих случајева у којима су лојални грађани једног друштва били привођени од полиције или притварани због намерне или ненамерне „замене идентитета“.[39] Неке студије показују да у највећем броју случајева жртва промене електронског идентитета тога није свесна у вишегодишњем интервалу, а када сазна за малициозну или ненамерну

---

[34] *BETR*, стр. 111.

[35] Roger Clarke, „Biometrics and Privacy“.

[36] EPIC, *Annual report 2004–2005*, стр.16 Извештај је преузет са адресе: http://www.epic.org/epic/annual_reports/2004.pdf. – „Лако је заменити број кредитне картице или социјалног осигурања, али како заменити свој отисак прста, глас или рожњачу?“. Непромењивост биометрије треба условно узети – погледати поглавље 1.6 наше студије (*прим. О.С*).

[37] Gerri Peev, „ID cards will lead to ’massive fraud’“, *The Scotsman,* 18. 10. 2005. Чланак је преузет са адресе: http://news.scotsman.com/index.cfm?id=2103982005.

[38] Stephen Mason, нав. чланак, стр.11.

[39] Edgar A. Whitley, Ian R. Hosein, Ian O. Angell, Simon Davies, *Reflections on the academic policy analysis proces and UK Identity Card scheme*, Department of Information Systems LSE, Лондон 2006. – Студија наводи пример Дерека Бонда (*Derek Bond*) из Бристола који је у Дурбану ухапшен фебруара 2003. године за криминална дела која је починио криминалац из Лас Вегаса који је украо његове идентификационе податке. Студија је преузета са адресе: http://is2.lse.ac.uk/wp/pdf/wp147.pdf.

промену, штета је већ учињена.[40] Са друге стране, истина је да је биометрију у принципу прилично лако украсти и ван биометријских база и система идентификације.[41] Међутим, њена крађа у широком обиму, копирање прецизног узорка (уколико у базу нису ускладиштени само шаблони) и директно укрштање у детаљном виду (генерисањем сложеног упита) омогућени су само помоћу њих. Стога аргумент пропонената биометријског система идентификације да је лакше покупити биометрију на други начин осим „хаковања" биометријске базе,[42] тј. пробијања сигурносних механизама који спречавају неауторизовано прикупљање или измену информација – не стоји (бар не у потпуности). Тај аргумент не стоји поготово у контексту преузимање практично неограниченог броја биометријских података (зависно од ширине успешног упита над базом) и преузимања са њима повезаних небиометријских података (атрибутивих и биографских). Стога стручњаци за безбедност наводе да је недопустиво складиштење класичне детаљне биометрије обичних грађана у базу, већ само упрошћене и кодиране шеме у виду тзв. шаблона (*template*),[43] који не могу бити искоришћени за укрштање са базама детаљне биометрије које треба да се воде само у случају криминалних досијеа.

Постоји и могућност злоупотребе биометријских података тако што би се права биометрија заменила лажном (преко контактних сочива у случају скена рожњаче или коришћењем отиска чак и мртвог човека у случају отисака прстију).[44] С обзиром да је могуће нанети туђи биометријски отисак на желатинасту масу, питање је да ли ће пракса показати случајеве издавања вишеструких докумената са замењеним идентитетом, с обзиром да све стоји на савести службеника.[45] Иако се сматра да на читачком пункту није могуће дати лажни биометријски податак, теоријски је то могуће коришћењем гумираног отиска, лажиране рожњаче на сочиву и маске за лице за фацијални скен, зависно од захтеваног идентификатора.[46]

Дакле, зависно од тога где се нападач усмерава (на читачки пункт, централну базу или неки унутрашњи процес обраде података) различите су врсте злоупотребе ради лажирања идентитета.[47] Парадокс целе приче је да је бор-

---

[40] *LSEIP*, стр.110.

[41] *BETR*, стр. 19.

[42] Bori Toth, „Biometric ID Card Debates", Deloitte, 2005, стр. 2. Чланак је преузет са адресе: http://www.deloitte.com/dtt/cda/doc/content/uk_ta_idcarddebates_june05.pdf.

[43] *FIDISD3.6*, стр. 46. – Ово у смислу тога да се не складишти чист биометријски податак који касније може бити компромитован, већ нека врста виртуелног шаблона, упрошћене маске са кључним тачкама која не може бити искоришћена за повреду интегритета особе на коју се односи јер не представља њену биометрију ужем смислу.

[44] *HCICT*, стр 13.

[45] *LSEIP*, стр. 191.

[46] *MBID,* стр. 30.

[47] *FIDISD3.2*, стр.23.

ба против фалсификовања исправа један од кључних аргумената пропонената биометријских система идентификације, иако њиховом употребом може доћи до потпуно нових начина лажирања институционалног идентитета.

Истине ради, треба рећи да крађе идентификационих података могу бити учестале и у небиометријским системима идентификације, поготово у случајевима где постоји један специјални дистинктивни идентификатор који служи као кључ у различитим базама.[48] Примера ради, у Америци тај број је *Social Security Number* (број социјалног осигурања), у Аустралији *Tax File Number* (порески идентификациони број),[49] а у Србији ЈМБГ (јединствени матични број грађана). С тим у вези, забрињава чињеница да су крађе података из дигиталних база података западних држава које су индексиране према тим кључевима реалност потврђена у милионским цифрама.[50] Оно што такође треба навести је да биометријски системи идентификације своје позадинске базе најчешће и индексирају преко сличних идентификатора, због чега у оба случаја императив безбедности налаже строгу и стручно надгледану децентрализацију података.

2.4 Тотал(итар)ност концепта централне базе података

Сви стручњаци за безбедност рачунарских система који се критички односе према биометријским системима идентификације као кључни проблем виде концепт централне (или можда боље рећи „централизоване“) базе биометријских (и осталих) података. Таква база се најчешће налази у позадини биометријског система и за перцепцију просечног грађанина она је „невидљива“.[51] Систем који се ослања на такву базу је рањив како споља (малициозни упад неауторизованог субјекта страног систему) тако и изнутра (малициозна промена података од стране ауторизованог службеника система).[52]

Узевши то у обзир, водећи светски експерти за безбедност података истичу да би овакав тип базе био невероватно примамљив за припаднике оранизо-

---

[48] *Кључ* је податак у пољу базе којим се једнозначно утврђује цео слог у њој. Примера ради, ако неко познаје ЈМБГ (као кључ) он једнозначно може утврдити садржај осталих поља у слогу у којима се налазе атрибутивни подаци конкретне личности (име, презиме, место рођења...), јер су сви кључеви међусобно различити и не могу постојати две особе са истим ЈМБГ податком. Термин кључ код база података не треба мешати са истоименим термином у криптографији, који је објашњен у критичком апарату поглавља 1.4 наше студије (*прим. О.С*).

[49] *LSEIP*, стр. 100.

[50] Hope Yen, „Data on 2.2 Million Active Troops Stolen From VA“, ABC News. Вест је преузета са адресе: http://www.abcnews.go.com/gma/wireStory?id=2047707.

[51] Roger Clarke, „Biometrics and Privacy". – Аустралијска агенција за социјално осигурање (*Australian social welfare agency*) је међу принципима за увођење биометријских докумената навела да они треба да буду уведени једино: а) у случају отвореног прихватања грађана; б) у случају да су документи максимално сигурни и в) ако не постоји централна база података.

[52] *MBID*, стр. 29.

ваног криминала.[53] Иако би имплементацијом доброг алгоритма за енкрипцију података тај посао био знатно отежан, он ипак не би био онемогућен, поготово у случају корумпираних службеника који би били у поседу енкрипционих кључева.[54] Такав ризик од нелојалног коришћења информација од стране овлашћених службеника се у стручној литератури често наводи као Хуверов проблем (према *J. Edgar Hoover*-у).[55] Да би се ова злоупотреба смањила на најмању могућу меру, поред заштите система мора се водити рачуна о строгом увиду у место и време када је конкретан службеник приступао одређеном делу базе података.[56] Уз све наведено, за очување интегритета грађана неопходан је робустан систем за корекцију грешака и ажурирање исправки.[57]

Проблем спољашњег упада је можда и већи. Бивши шефови познатих обавештајних служби истичу да би централизоване базе биометријских података биле поклон за криминалце, који би продором у њих добили податке којим би могли да угрозе интегритет личности који су њима обухваћене.[58] Извештаји експерата показују да погрешни подаци у централној бази података могу носити велики безбедносни ризик по грађане,[59] што може довести до озбиљног проблема малициозне замене идентитета криминалаца и обичних грађана.[60] Концепт централне базе података по питању сигурности и безбедности оспоравају и многе стручне установе,[61] а на могућност масовне крађе података у биометријским базама упозорили су и званичници највећих информатичких компанија на свету.[62]

---

[53] О томе говори водећи британски стручњак за безбедност Питер Дорингтон (*Peter Dorrington)* у интервјуу под називом „Biometric ID cards 'dangerously flawed'", Silicon.com-Law&Policy, 23. 05. 2003. Интервју је преузет са адресе: http://management.silicon.com/government/0,39024677,10004326,00.htm.

[54] Ово нарочито добија на тежини у у друштвима са опресивним апаратом попут нашег, где су криминал и разне „службе" испреплетане историјом и интересима. У друштву где један директор долази до службених података о „делатностима" директора друге компаније, где неколико таблоидних новина добијају извештаје о медицинским третманима политичких опонената својих „опција" и где је корупција на нивоу већине афричких земаља, централна база података *било кої типа* (биометријских, здравствених, финансијских) представља велики проблем.

[55] A. Michael Froomkin, нав. дело, стр. 44.

[56] Исто, 46.

[57] Исто, 47.

[58] Ово наглашава бивша шефица британске тајне службе MI6, Дафни Парк (*Daphne Park*), у интервјуу под називом: „Identity cards a 'present' to terrorists and criminals", *The Scotsman– Scotland`a National Newspaper,* 21. 03. 2006. Интервју је преузет са адресе: http://thescotsman.scotsman.com/uk.cfm?id=441172006.

[59] Andrew Clement, Felix Stalder, Jeff Johnson, Robert Guerra, „National Identification Schemes (NIDS) and the Fight against Terrorism: Frequently Asked Questions", v1.2, 27. 11. 2001. Чланак је преузет са адресе: http://www.cpsr.org/issues/privacy/natidfaq.

[60] Julian Ashbourn, нав. дело, стр. 13.

[61] *HCICT*, стр. 54. – Концепт централне базе биометријских података је критиковао и *Комитет за рачунарска истраживања Велике Британије* (UKCRC).

[62] Могућност масовне крађе података из централне базе је део шире изјаве против биометријског система идентификације коју је дао званичник *Microsoft*-а Џери Фишенден (*Jerry Fishenden)*

Следећа слаба тачка концепта централне базе биометријских података је комуникациони канал између пункта за очитавање биометријских података и ње,[63] поготово уколико се подаци преносе неком врстом модемске везе. Убацивањем малициозног софтвера (тзв. „тројанаца“) омогућена је ситуација аутоматског лажирања идентитета приликом очитавања биометријских података конкретне особе.[64] Сама биометријска апликација (у смислу њеног функционисања), додатно може бити предмет напада кроз промену функционалности.[65] Мањи проблем представља случај „пада система“ (мада га многи наводе као критичан) јер у том случају се може прибећи 1:1 идентификацији (али само у случају тзв. „позитивне идентификације“, када треба потврдити да је особа та која је назначена на документу).

Суштина проблема је у чињеници да пракса показује да не постоји стопроцентно заштићен електронски систем који би заштитио податке од неауторизованог коришћења. То је поготово случај код централизованог система у коме постоји само једна база на коју криминалци треба да се усмере.

Са друге стране, студије независних стручних органа који имају подршку ЕУ[66] показују да формирање централне базе биометријских података јесте први корак ка друштву надзора, мада има стручних институција које тврде да је друштво тоталног надзора већ постало реалност.[67] Западне организације које се боре за очување права на приватност за тако нешто користе појам *Database State* (*држава-база*),[68] а у ширем контексту *Surveilance society* (*друштво надзора*), где је централна база података основни супстрат на коме се систем надзора гради. Занимљиво је да међу европским државама, концепт централног регистра (који је правна основа за развијање централне базе) познају углавном земље које су некада припадале комунистичком блоку, што итекако говори о тоталитарним премисама таквог приступа.[69]

Нуспродукти оваквог централизованог система би лако могли постати крађа идентитета, размена података између различитих неауторизованих инстанци и томе слично.[70] У смислу будућих токова, такав приступ иде ка

у интервјуу „*ID* cards will lead to ’massive fraud’“, *The Scotsman*, 18. 10. 2005. Интервју је преузет са адресе: http://thescotsman.scotsman.com/index.cfm?id=2103982005.

[63] *MBID*, стр. 29.

[64] Исто, 30.

[65] Исто, 31.

[66] Попут конзорцијума FIDIS.

[67] *RSS*, стр. 1. – „Ми живимо у друштву сталног надзора. Беспредметно је говорити о таквом друштву у смислу будућег времена“.

[68] Према организацији NO2ID (*No to Id*) овај појам одређује тенденцију да се рачунарске мреже користе да би се друштвом управљало преко непрестаног надзора грађана. За детаљнији увид погледати сајт поменуте организације на адреси: http://www.no2id.net/.

[69] *FIDISD3.6*, стр. 16.

[70] *FIDISD3.2*, стр. 25.

својевресном Паноптикону, у контексту „свевидеће“ државе константног и сталног надзора,[71] у којој су многобројне укрштене базе у рачунарским мрежама (у спрези са једном централном) темељ система. Стога и не чуди чињеница да многи мислећи информатичари све чешће шаљу отворена упозорења да морамо константно имати у виду пре свега стварање света у коме ће живети наша деца и водити рачуна како о очувању традиционалних вредности тако и о унапређењу живота и коришћењу савремених технологија.[72] Они се питају шта ће се десити сутра уколико се већ данас успостављају темељи за такав механизам праћења и контроле. [73]

2.5 Биометријска идентификација без централ(изова)не базе

У стручним круговима преовладава мишљење да је уместо централне базе података далеко безбедније и по приватност појединаца боље решење 1:1 („*један према један*“) идентификације, где су биометријски подаци смештени само на smart карти, не напуштају је приликом аутентификације идентитета и где ималац биометријских података има неупоредиво већу контролу над њима. У оквиру таквог концепта биометријски подаци су практично у рукама власника карте – приликом провере утврђује се искључиво да ли његов биометријски отисак, рецимо, одговара оном који је у карти кодиран (и заштићен од неовлашћеног приступа).[74]

За такве потребе smart технологија сматра се за једну од технички најпоузданијих, мада је теоријски и практично неоснована тврдња да је стопостотно сигурна,[75] јер напад на такве карте може бити изведен на неколико начина.[76] Други проблем код ње је у чињеници да уколико би лажирање та-

[71] Исто, 30.

[72] Julian Ashbourn, нав. дело, стр. 21. –*У* закључку своје студије о биометријским системима идентификације (одељак „Conclusions and recommendations“, стр. 20) Ешбурн таксативно даје више препорука, између осталог да се: постави мораторијум на међународним и националним биометријским пројектима и учини њихово преиспитивање (*тачка 1*), развије међународна свест која би штитила интересе грађана (*тачка 3*), осигура отворена јавна расправа о овим питањима (*тачка 5*), обезбеди да биометријски подаци буду под контролом корисника где год се биометријски системи идентификације користе (*тачка 6*), забрани учешће трећих лица (поготово из приватног сектора) у руковођењу јавним пројектима идентификационог менаџмента (*тачка 11*), установи чврст механизам по коме би грађани могли у сваком тренутку да провере које се информације о њима скупљају од стране било које владине агенције (*тачка 13*) и установе саветодавни центри за идентификациони менаџмент који би могли да истраже пријављене злоупотребе (*тачка 21*).

[73] Исто, стр. 18.

[74] Ronald Küster, Wolfgang P. Schulz, *Biometric Identity - Privacy, Risks and Law*, Work paper, Пекинг, 2nd Biennial congress on the law of the world, 4-10. септембар 2005, стр. 3. Ауторизовано излагање је преузето са адресе: http://www.europeanbiometrics.info/images/news/24_857_file.pdf.

[75] Andrew Clement и остали, нав. дело.

[76] Душан Булатовић, *Smart картице и сигурност података у њима.* – Аутор разлаже напад на ове картице на активни (у којима се чип практично извлачи са картице, испитује, премерава, моди-

кве карте било успешно изведено, превара би била готово савршена и веома тешко уочљива.[77] Уз то, немогуће је бити потпуно сигуран да додатни подаци коришћењем smart карти не „цуре“ тј. не одлазе на неко неауторизовано место, ван знања имаоца, макар се радило и о ван Ековом (*van Eck*) ефекту.[78] Чак је и проналазач прве генерације smart карти, Роланд Морено (*Roland Moreno*), током седамдесетих рекао да оне имају потенцијал да постану „мали помагач Великог Брата“.[79]

Проблем код концепта 1:1 реализованог помоћу smart карти (који је, да поновимо, далеко безбеднији и неинвазивнији од 1:n концепта са централном базом) може представљати и случај неисправности микроконтролера на самој карти, у ком случају грађанин може бити изложен тортури уколико је сумњив по неком критеријуму. Од тог проблем нису имуна ни изразито демократска друштва, а у случају тзв. „полицијских држава“ то може постати ноћна мора за грађане.

У сигурносне механизме које овај систем мора да поседује спада и захтев за обостраном аутентификацијом, у смислу да чипови на картама морају имати могућност провере уређаја са којим ступају у трансакцију (полицијских читача, рецимо).[80] Тиме би се спречило да лажни органи власти на лажни читачима ишчитају податке ради њихове касније (зло)употребе. Уз све наведено, дизајн карте мора да буде транспарентан за јавност.[81]

Према нашем мишљењу, највећи проблем код чип-карти лежи у тенденцији интеграције (тј. коришћења вишенаменских карти погубних по приватност) и конвергенцији неких будућих итерација ка биочип-имплантат решењима (следујући концепту минијатуризације) који би били неодвојиви од тела, и који би били неприхватљиви из антрополошког, етичког и верског аспекта. Не сме се стога дозволити укидање концепта једнонаменских smart карти и анонимности односно псеудонимности новчаних и осталих трансакција.

фикује, за шта је потребно време, велика количина ресурса и познавање физичког дизајна чипа) и пасивни тип (у којима је рад картице посматран за време њене нормалне употребе са читачем). Поред анализе методологије напада (директни напад на криптографски алгоритам, напад мерењем времена енкрипције и хардверски напад), аутор и анализира различите групе нападача, зависно од знања и расположивих ресурса.

[77] Исто.

[78] S. Brands, *Rethinking Public Key Infrastructures and Digital Certificates; Building in Privacy*, MIT Press, 2000, стр. 24 – Микропроцесори, тастатуре, рачунарски монитори, серијски каблови, штампачи и остали периферали емитују електромагнетну радијацију која пролази преко одређене дистанце, чак и кроз зидове и може бити даљински ухваћена и прегледана.

[79] Исто.

[80] Roger Clarke, „Biometrics and Privacy“.

[81] Roger Clarke, „Chip-Based ID: Promise and Peril“.

2.6 Биометрија и борба против организованог криминала и тероризма

Аргумент да биометријски системи идентификације представљају одлично средство против тероризма првобитно је пласиран од стране западних политичких елита, које их предлажу за увођење ради наводног повећања безбедности грађана. Са друге стране, организације које се боре за очување приватности грађана тврде нешто друго: да политичари борбу против тероризма користе само као изговор за увођење таквог система идентификације, желећи пре свега да уведу већу контролу над становништвом са једне стране и да прикрију неспособност надлежних антитерористичких служби са друге.[82] Критичари тог концепта указују да он у великој мери представља тоталну дислокацију принципа из прошлости на којима су западна друштва устројена.[83] Индикативно је да се биометријски методи идентификације (нарочито после напада у Њујорку, 11. септембра 2001. године) и од стране произвођача опреме за биометријску идентификацију рекламирају као одлично средство против тероризма. Стручне анализе показују да то није тако.[84] Социолози додатно указују на чињеницу да повећање обима овлашћења и моћи полицијског апарата над обичним грађанима уз помоћ софистициране технологије неће помоћи у решавању проблема криминала и тероризма, за чије решавање су потребна далеко дубља промишљања. С тим у вези, чак и многе присталице биометријске идентификације из кругова западних влада признају да она не би спречила терористичке нападе.[85] Историјске чињенице говоре да су и раније постојале некритичке изјаве западних влада о коришћењу софистициране технологије за надзор ради спречавања тероризма, али да то ипак није спречило терористичке акте.[86] У том контексту, чини се да концепт биометријских идентификационих система и докумената у највећој мери неће испунити оно што се од њега званично очекује.[87]

---

[82] APF, „The Case Against a National Identification Scheme“. Чланак је преузет са адресе: http://www.privacy.org.au/Campaigns/ID_cards/NatIDScheme.html.

[83] *FIDISD3.2*.

[84] Roger Clarke, „Biometric Insecurity“, верзија од 14. маја 2004. Чланак је преузет са адресе: http://www.anu.edu.au/people/Roger.Clarke/DV/AusCERT0405.html.

[85] То донекле признаје чак и један од највећих светских пропонената биометрије, британски министар унутрашњих послова Чарлс Кларк (*Charles Clarke*), наводећи да биометријске личне карте не би помогле у спречавању терористичког напада у Лондону 7. јула 2005. године. Интервјуу под називом: „ID cards would not have helped, says Clarke“, *Telegraph*, 09. 07. 2005, је преузет са адресе: http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2005/07/09/npoll209.xml&sSheet=/news/2005/07/09/ixnewstop.html.

[86] *FIDISD3.2*, стр. 30. – Добар пример је тзв. *Carnivore* технологија, којом су у Америци пресретане комуникације ради спречавања терористичких напада и која се показала неуспешном у случају напада 11. септембра. Комплексност ове проблематике већ унапред осуђује на неуспех сваки даљи покушај у сличном смислу, док се права грађана урушавају драстичном брзином.

[87] BBC, „ID cards are of ’limited value’“, 29. 01. 2006. Вест је преузета са адресе: http://news.bbc.co. uk/2/hi/uk_news/politics/4659228.stm.

Стручне студије указују на чињеницу да овакве системе идентификације највише желе полицијске структуре (ради повећања моћи) и мултинационалне компаније које продају скупу опрему (ради повећања профита), те да целокупан концепт има мало везе са борбом против тероризма.[88] Посебно се истиче да је у свим случајевима где је откривена терористичка завера то учињено преко убачених агената и дојава, при чему је веома тешко видети у чему би увођење биометријских докумената уопште помогло.[89] Суштина, наиме, лежи у чињеници да терористи не крију свој идентитет, већ своје намере.[90] Често се дешава да људи који изводе терористичке нападе буду грађани беспрекорне биографије и без икаквог криминалног досијеа,[91] што је у потпуној колизији са тврдњом да ће биометријска идентификација помоћи у њиховом спречавању. Специјалисти за колективну безбедност тврде да није ствар у идентитету, колико о улози коју појединац има.[92] А у случају да је потребно да лажира свој идентитет, сваки „респектабилан“ терориста и криминалац ће наћи начин да прибави себи биометријске исправе са подацима који му одговарају.[93] Технологија у овом погледу не може бити промовисана као магично решење за проблем јер она то није, [94] пошто се проблеми терористичких напада решавају пре свега обавештајним радом.[95]

Многи стручњаци су сугерисали да биометријске личне карте неће повећати националну сигурност али да ће итекако утицати на појаву нових врста криминалних дела.[96] Неки академски грађани отворено тврде да биометрија неће донети сигурност, већ супротно, да ћемо бити угрожени „биометријском несигурношћу“, управо зато што се о овим стварима говори непрофесионално, ирационално и политички вођено.[97] С тим у вези, постоје случајеви да су биометријски системи идентификације само породили нове врсте кринималних активности.[98] У „информационој ери“ смо по инерцији

---

[88] Andrew Clement и остали, нав. дело.

[89] *RSS*, стр. 16.

[90] Ronald Küster, Wolfgang P. Schulz, нав. дело. – Аутори су поставили сасвим сувисло питање: да ли би убиство Џона Кенедија, Мартина Лутера Кинга или Гандија било спречено да су њихове убице имале биометријска документа? Тиме су желећи да укажу на то да криминалци и терористи крију пре свега своје намере, а не идентитет.

[91] Такав је био случај у бомбашким нападима у Лондону 7. јула 2005. године.

[92] Wendy M. Grossman, „Identifying Risks: National Identity Cards“, ауторизована верзија предавања одржаног на Универзитету у Единбургу, 19. јануара 2005, стр. 10. Документ је преузет са адресе: http://www.law.ed.ac.uk/ahrb/script-ed/vol2-1/idcards.pdf. – То између осталог тврди и Рос Андерсон (*Ross Anderson*), специјалиста за безбедност са Универзитета у Кембрицу

[93] Исто.

[94] Julian Ashbourn, нав. дело, стр. 11.

[95] Исто, 22.

[96] Wendy M. Grossman, нав. дело, стр. 10.

[97] Roger Clarke, „Biometric Insecurity".

[98] *FIDISD3.2*, стр. 23.

често навикли да решење проблема налазимо у технологији, али (као што студије стручних органа показују) некада лек може бити гори од болести.[99] У стручној јавности се с тим у вези поставља и доктринарно питање да ли биометријски систем све грађане третира управо као криминалце и сумњиве људе, уз посебно питање каквом друштву то води сутра.

Занимљиви су резултати компаративних истраживања степена криминалитета земаља које имају режим личних карти (било да су биометријске или не) на обавезујућој основи, добровољној и оних који личне карте уопште немају. Те анализе показује да се не може успоставити корелација између режима личних карти и степена криминалитета (у категоријама општег криминалитета, наркотика, трафикинга, убистава и терористичких напада).[100] Додатно, социолошке студије показују да у Великој Британији озбиљан криминал расте и да су затвори препуни, иако је она практично друштво надзора по питању броја камера на јавним местима.[101] Парадоксално, насупрот свим наведеним истраживањима, владе широм света уводе готово тоталитарне мере због наводне борбе против тероризма, иако оне до сада не показују успешност.[102] У том погледу, независни експерти тврде да ће имплементацијом биометријских база података крађа бити само олакшана, а да биометријска идентификациона документа ни у ком случају не могу спречити терористичке нападе.[103] Аргумент да се биометрија грађанима узима због борбе против тероризма има и једну практичну ману, а то је немогућност имплементирања система у релативно брзом временском року, што ће довести до великих сигурносних пропуста. [104]

Све наведено говори да се начин на који неке владе полако уводе тоталитарне методе надзора и праћења свог сопственог становништа, уз употребу софистицираних метода биометријске идентификације, са разлогом „борбе против тероризма“,[105] може отворено назвати „политиком застрашива-

---

[99] Исто, 30.

[100] *LSEIP*, стр. 116.

[101] Julian Ashbourn, нав. дело, стр. 13.

[102] *FIDISD3.2*, стр. 30. – Примера ради, француска полиција већ има овлашћење да претреса приватну својину без налога, а немачко законодавство губи своју оштрину по питању праћења електронске поште, прислушкивања телефона и праћења финансијских трансакција.

[103] Један од највећих светских стручњака за безбедност и примењену криптографију, Брус Шнајер (*Bruce Schneier*), даје ову прогнозу у интервјуу под називом: „U. K. Identity Card Will Make Fraud Easier, Expert Says“, Bloomberg.com, 26. 04. 2006, на адреси: http://quote.bloomberg.com/apps/news?pid=10000102&sid=a7DltmImquye&refer=uk.

[104] Tony Bunyan, нав. есеј, стр. 6. – Аутор излаже претпоставку да ће по савршеној динамици до 2012. године 50% Европљана добити биометријски пасош, што према њему значи да опасност од терористичких напада у наредних пет година уопште не би била уклоњена због оних 50% преосталих са старим пасошима, ако би биометријски пасоши уопште и помогли.

[105] Синтагма „борба против тероризма“ иначе није добро скројена, јер је тероризам првенствено метод, а не неки одређени објекат или субјекат. У нашој студији се она користи само зато

ња“.[106] Борци за грађанска права са сетом наводе да данас принципи узмичу пред прагматизмом, што доводи до тога да се некадашње државе благостања полако претварају у државе надзора у којима су борба против тероризма и очување демократских начела само маска.[107] У принципу, начин живота („*way of life*“) грађана у земљама западне демократије не уништава криминал нити тероризам, већ неадекватна реакција од стране естаблишмента погођених земаља. У тој реакцији форсирање биометријских система идентификације на националном нивоу у обавезујућем виду представља чист промашај и велики ударац на концепт слободног друштва.[108]

2.7 Биометријски системи идентификације и право на приватност

У оквиру грађанскоправне науке, право на приватност се сврстава у корпус личних права (неки аутори више воле одређење „права на личним добрима“).[109] О приватности у уско правном смислу говори се тек од краја 19. века.[110] Она у правној пракси значи вођење живота слободно, без упада у интиму, у већој мери аутономно и са могућношћу контролног приступа личним информацијама.[111]

Изражавајући жаљење за све већом пролиферацијом података, неки теоретичари права тврде да је приватност de facto укинута мада de jure још увек постоји. Иако је ерозија приватности одавно почела, то ипак не значи да је потребно дићи руке од борбе за оно што је од тих права остало.[112] Пролиферација личних података је проблематична због чињенице да што је већи опсег информација о грађанима доступан одређеним инстанцама, то је већи степен контроле коју оне имају, што готово увек има директан утицај на грађанске слободе.[113] Оног тренутка када информација више није под контролом онога на кога се односи, нико не може гарантовати да ће бити уклоњена или да ће бити лојално коришћена. У том смислу, уколико је приватност података једном изгубљена, тешко (или готово никако) може бити по-

---

што је општеприхваћена – *прим. О.С).*

[106] Tony Bunyan, нав. есеј, стр. 1.

[107] Исто, 2.

[108] Исто.

[109] Обрен Станковић, Владимир Водинелић, *Увод у грађанско право*, НОМОС, Београд 1996, стр. 120.

[110] Malcolm Crompton, нав. дело, стр. 8. – У то време Семјуел Ворен (*Samuel Warren*) и Луис Брендајс (*Louis Brandeis*) популаришу одлуку судије Кулија (*Cooley*) да је приватност „право да човек буде остављен на миру“ („*right to be let alone*“), затраживши заштиту појединца у контексту нових проналазака и начина пословања.

[111] *MBID*, стр. 49.

[112] Julian Ashbourn, нав. дело, стр. 17.

[113] Malcolm Crompton, нав. дело, стр. 8 – Професор Зелман Ковен (*Zelman Cowen*) каже да је човек без приватности једнак човеку без достојанства; страх да Велики Брат посматра и слуша угрожава слободу појединца једнако као затворске решетке.

враћена.[114] Битно је истаћи да губљење приватности података није споредна ствар, већ да се тиме директно угрожава безбедност грађана.[115]

Право на приватност је потврђено многим међународним актима и конвенцијама.[116] С тим у вези, биометријски системи идентификације у контексту приватности су тема великог броја стручних скупова широм света и заокупљају пажњу шире јавности.[117] Због чињенице да биометријски идентификациони системи не користе информације *о* човеку, већ личне податке и најосетљивије *особености*, њихова употреба се у великој мери сматра директним атаком на приватност на концептуалном нивоу.[118] С тим у вези, биометријски системи идентификације утичу како на губљење приватности података о личности, тако и на губљење приватности личних података (можемо их условно назвати и „личне особености"), а посредно и потенцијално на укидање концепта анонимности и псеудонимности токова података, који је једна од одлика слободних друштава.[119]

Додатни проблем представља чињеница да код идентификационих карти са микрочиповима (које су данас основа биометријских система идентификације на националном нивоу) увек постоји ризик од каснијег функционалног проширивања, у смислу додавања нових функција или атрибута у следећој итерацији документа.[120] Посебан проблем је тзв. „ефекат информационе грудве снега", где количина расположивих података о грађанима расте експоненцијално према успостављању нових система идентификације (као што грудва расте док се отиска низ брдо – *прим*). Тај проблем се бази-

---

[114] Claudia Diaz, „Privacy risk scenario", *D2.6: Identity in a Networked World – Use Cases and Scenarios*, FIDIS, август 2006, стр. 11. Брошура је преузета са адресе: https://prof.hti.bfh.ch/arb1/FIDIS/fidis.pdf.

[115] Roger Clarke, „Interview with Dr Ted Dunstone, Director, Biometix Consulting".

[116] *Међународна конвенција о грађанским и политичким правима* (*International Covenant on Civil and Political Rights*) својим 17. чланом брани приватност грађана, прописујући да „нико не може бити изложен произвољном или незаконитом мешању у приватност, породицу, кућу или преписку, нити незаконитом атаку на достојанство и углед". Она се може преузети са сајта Уједињених нација на адреси: http://www.unhchr.ch/html/menu3/b/a_ccpr.htm;
Општа декларација о правима човека својим 12. чланом захтева да „нико не сме бити изложен произвољном мешању у приватни живот, породицу, стан или преписку нити нападима на част и углед" и да свако има право на законску заштиту против оваквог мешања или напада;
Европска конвенција о људским правима дозвољава уплив држави у приватност грађана само у оној мери која потребна у демократском друштву и пропорционална незаобилазним социјалним потребама и националној сигурности (*LSEIP*, стр. 248);
Америчка конвенција о људским правима у свом 11. члану истиче „право на лични живот".

[117] Marie Shroff, нав. дело, стр. 2.

[118] Roger Clarke, „Biometrics and Privacy".

[119] Roger Clarke, „Dataveillance – 15 Years On", Privacy Issues Forum, Wellington NZ, 28. март 2003. Рад се налази на адреси: http://www.anu.edu.au/people/Roger.Clarke/DV/dvnz03.html, а пратећа презентација на http://www.anu.edu.au/people/Roger.Clarke/DV/dvnz03.ppt.

[120] Roger Clarke, „Chip-Based ID: Promise and Peril".

ра на претпоставци да временом нико, а најмање личност на коју се то односи, неће моћи да каже колико, каквих и од кога вођених информација постоји.[121] Да би се предупредио тај проблем, законом мора бити загарантован и у пракси примењив принцип транспарентности, који подразумева да субјект у сваком тренутку има могућност да сазна који се подаци о њему воде, од стране које инстанце, ко има дозволу да им приступа а ко им заиста приступа.[122] Наведени услов се показује као суштински када треба исправити податке или онемогућити профилисање личности у одређеној мери.[123] Код профилисања је посебна невоља што се ради само о статистичкој корелацији, а не о узрочно-последично вези. То може довести до тога да обичан грађанин потпадне под сумњиве јер се поклапа, рецимо, са куповним профилом просечног терористе и безбедносно опасних лица.[124]

Специфичан проблем је тзв. „траг“ (енгл. *audit*) који остаје у бази приликом сваке идентификације неког грађанина, јер се њиме омогућава креирање нове врсте података: места идентификације (што омогућава симплификовану пасивну шему временске позиције) или типа идентификације (тј. разлога идентификовања, без обзира на крајњи исход).[125]

И на крају, у неким случајевима помоћу биометријских података се може открити и здравствено стање грађанина, што може бити додатни уплив у приватност.[126]

У одговору на ова питања, пропоненти биометријских система углавном потежу аргумент да је право на безбедност јаче од права на приватност (што је равно волунтаризму у правно-доктринарном смислу) те да ионако сви можемо лако бити прислушкивани, праћени и профилисани преко мобилних телефона, GPS уређаја и кредитних карти.[127] Оба аргумента су крање лабилна. Први због чињенице да се за одбрану једног права не може урушавати друго, јер се тиме урушава комплетан правни систем, а други из простог разлога што се превиђа чињеница да су мобилни телефони и кредитне

---

[121] Julian Ashbourn, нав. дело, стр. 19.

[122] A. Michael Froomkin, нав. дело, стр. 47.

[123] Профилисање је креирање профила личности (куповног, углавном) који се добија укрштањем различитих база података. Постоје специјализоване агенције које помоћу профилисања личности праве различите категорије људи са туђе или сопствене потребе.

[124] Милан Туба, „Какве нас све лепоте очекују када се реинтегришемо у међународну заједницу“, *Правда*, септембар 1994.

[125] *LSEIP* стр. 249.

[126] Malcolm Crompton, нав. дело, стр. 11. – Погледати додатно и одељак 2.1.2 наше студије.

[127] Bori Toth, нав. дело, стр. 2. – Мобилни телефон на сваких десет-петнаест секунди потврђује базној станици да је у мрежи, што омогућава одређивање локације корисника, док се софистицирано прислушкивање (теоријски омогућено интерсистемским скривеним процедурама) преко телефонског микрофона може онемогућити једино уколико се извади батерија из апарата (*прим. О.С*).

карте одувек били на добровољној основи, те да их појединац може имати и неколико, да их може а не мора користити и да их се по потреби увек може отарасити. Код биометријских идентификационих докумената то није случај, поготово уколико су мултифункционалног типа.

Добровољни режим биометријских докумената у великој мери би решио потенцијалне проблеме око колизије биометријског система идентификације са правом на приватност.[128] Са друге стране, треба избећи клопку формално добровољног, а фактички обавезног режима биометријских докумената,[129] поготово у случају личних карти (из простог разлога што ће у том случају управо они који немају такве личне карте бити сумњиви и дискриминисани), [130] те законски треба решити и строго санкционисати питање евентуалне дискриминације у имплементацији добровољног режима.[131]

Друга кључна ствар за очување приватности јесте искључиво примена једнонаменског (за једну примену, било да је у питању лична карта, возачка дозвола, здравствена књижица...) уместо вишенаменског (у једном документу више докумената, што најчешће омогућава директно профилисање) концепта (биометријских) докумената.[132]

Трећа и можда најбитнија ствар по питању очувања приватности је директна и недвосмислена забрана централне базе биометријских података,[133] поготово јер у контексту биометријских система идентификације она није condicio sine qua non.

Нажалост, због изговора борбе против тероризма често се може чути да од глобалног села свет полако постаје глобални гето,[134] уместо да се тежи успостављању баланса између интереса државе и њених грађана.[135] Од тога да ли ће и у којој мери тај баланс бити успостављен, зависи и будућност права на приватност уопште. На академским грађанима лежи одговорност формирања критичке парадигме по том питању.

---

[128] *LSEIP*, „House of Lords: All Party Briefing for Report Stage Amendments 38 & 54 and 46 & 52: Voluntary v. compulsory regime“, стр. 2.

[129] *RSS,* стр. 42.

[130] Andrew Clement и остали, нав. дело.

[131] У Србији је на аспект потенцијалне дискриминације у наведеном контексту први указао Никола Марковић, председник Друштва за информатику Србије.

[132] Једнонаменски концепт подразумева постојање различитих карти за различите употребе (идентификационе, платне, здравствене) и то са различитим идентификаторима (да би се осујетио покушај укрштања различитих података), док се вишенаменски концепт темељи на интеграцији свих докумената у један (физички или логички), најчешће коришћењем једног идентификатора.

[133] Roger Clarke, „Chip-Based ID: Promise and Peril“.

[134] EBIT, „Sporedni ulazi“, http://www.ekonomist.co.yu/magazin/ebit/29/pra/pra2.htm.

[135] Stephen Mason, нав. чланак, стр. 12.

2.8 Утицај на концентрацију моћи државног апарата

Основно одређење тоталитарне државе је да је она свеобухватна (лат. *totus* – сав, цео). Тај концепт полази од претпоставке да самостална делатност грађана није потребна, те да мора постојати један центар власти, који је позван све да зна, предвиди и испланира. Нажалост, приметно је да један број западних земаља клизи ка тоталитаризму, баш као Источни блок после Другог светског рата, између осталог и због некритичких иницијатива које се темеље на терористичкој претњи. Није стога ни чудно што све више интелектуалаца форсирање употребе биометријских система идентификације посматра као директну аналогију некадашње тоталитарне совјетске парадигме, само са другачијом идеолошком подлогом.[136]

Да би се успоставило информационо контролисано друштво (*controlled 'information society'*),[137] потребно је да се успоставе базе података које покривају различите делатности људи, мрежа која омогућава да рачунари на којима се базе налазе комуницирају међу собом, поуздана идентификациона шема која омогућава да се из више база подаци о једном човеку скупе у један виртуелни регистар и популација спремна да то прихвати.[138] Биометријским системима идентификације се у великој мери праве темељи за такво друштво и успоставља један нови тип власти, малобројна и моћна технократска структура, која ће имати на располагању велики број осетљивих информација.[139] Следећи корак може бити употреба овог система од стране ауторитарних режима, што директно води тоталитарној држави орвеловског типа.[140]

Наиме, код концепта информационо контролисаног друштва велику улогу игра укидање анонимности друштвених процеса (пре свега токова новца), у чему мултифункционалне биометријске карте играју велику улогу. Постоји велики притисак западних влада за увођење управо таквих карти (уместо једнонаменских) како за контролу границе, тако и за приступ

---

[136] Roger Clarke, „Biometrics' Inadequacies and Threats, and the Need for Regulation", верзија од 15. априла 2002. године. Чланак је преузет са адресе: http://www.anu.edu.au/people/Roger.Clarke/DV/BiomThreats.html.

[137] Термин „информационо контролисано друштво" не треба мешати са термином „информационо друштво", јер први носи негативне, а други у великој мери афирмативне конотације. Наиме, када се каже „информационо контролисано друштво", практично се мисли на друштво у коме један центар моћи користи информационе технологије ради контроле и праћења популације. На Западу, НВО сектор који се бори за приватност такво друштво често назива *Surveilance society* или *Database State.* Информационо друштво, са друге стране, је далеко шири појам и представља друштво које у великој мери функционише помоћу информационих технологија, имплементираних тако да буду у служби човека, а не супротно. Могли бисмо рећи да је „информационо контролисано друштво" девијација и злоупотреба концепта „информационог друштва" (*прим. О.С*).

[138] Roger Clarke, „Promises and Threats in Electronic Commerce", верзија од 13. августа 1997. Рад је преузет са адресе: http://www.anu.edu.au/people/Roger.Clarke/EC/Quantum.html.

[139] Simon G. Davies, нав. дело.

[140] Roger Clarke, „Biometrics and Privacy".

владиним сервисима и комерцијалним услугама,[141] користећи као подлогу управо биометријске податке, чиме се концентрација информација расположива државној управи значајно повећава. Највећи проблем у покушају интеграције свих докумената у један (који би вероватно заживео под истим претпоставкама као за обичне биометријске идентификационе карте данас) је што би један исти идентификатор фигурирао приликом обављања свих операција, укључујући и купопродајне трансакције, у ком случају би укрштање различитих база било веома једноставно. Иако земље западне демократије институционално решавају проблем злоупотребе података о личности (помоћу прецизних закона о заштити података и стручних тела које прате рад владиних службеника), висока концентрација информација у рукама владе добијена помоћу вишенаменских карти би се у једном историјски несигурном тренутку сигурно окренула против појединца. Он би, информационо гледано, могао постати потпуно огољен пред државом, што би могло имати огромне последице уколико је неконформистички оријенисан.[142]

Систем обједињених база података се правда потребом функционисања „јединственог шалтера", тј. могућношћу да грађанин на било ком шалтеру добије било који документ, чиме се комфору даје предност у односу на проблем укрштања база. Иако је то несумњиво корисна ствар, поставља се питање да ли би се некритичком имплементацијом отворио пут тоталном надзору грађана у смислу проширивања броја база података које би биле укрштене? Другим речима речено, да ли би у том случају део укрштених база имао и биометријске и остале осетљиве податке, као изговор за модернизацију управе? Уколико би одговор био потврдан, овакав систем би сигурно изменио природу односа државе према грађанима, поготово у земљама у којима се такво решење први пут примењује.[143] Повереници за информације се одавно питају да ли је све то разлог да се јасно дефинишу и законски прецизно нормирају границе употребе ове технологије убудуће.[144] С тим у вези, свака база коју контролише државна управа треба да поседује минималан број података за складиштење идентификатора и аутентификацију карти, што би отклонило опасност од крађе осетљивих биометријских података.[145] Лични подаци (биометрија) треба да буду увек рукама грађана, а то је немогуће уколико постоји позадинска база биометријских података.

Нажалост, према неким стручним извештајима надзор државе над појединцем ће рапидно расти у будућности. Аутори тих извештаја најчешће

---

[141] *RSS,* стр 26.

[142] Roger Clarke, „Chip-Based ID: Promise and Peril".

[143] *LSEIP*, стр. 119.

[144] Marie Shroff, нав. дело, стр.2.

[145] *LSEIP*, стр. 278.

подржавају тезу да се не може ништа учинити по питању смањења надзора државе, већ да треба ићи ка његовој проактивној регулацији.[146] Мишљења смо да је то ипак у великој мери конформистички став, недостојан с(а)весног академског грађанина, те да поред проактивне регулације треба упоредо ићи и на одбрану стечених и загарантованих права.

У погледу тоталитарних претензија државног апарата, апсолутно не постоји начин да прецизно одредимо куда нас досадашња имплементација биометријских (и са њима повезаних) система може одвести у ближој будућности, какве ће то последице са собом носити у социолошком погледи као ни како ће на све то реаговати грађани широм света.[147] Поготово уколико конкретна имплементација у будућности буде имала некритички предзнак.

2.9 E-government, e-commerce, e-banking и биометрија

Успостављање или модернизација државне управе у виду *e-government*-а тј. интерактивне (*on line*) размене информација и пружање услуга грађанима и правним лицима – се често користи као један од аргумената за увођење биометријских система идентификације. То је аргумент који углавном пролази код мање обавештених људи који не знају да је концепт електронске управе знатно лакше и по приватност података безбедније имплементирати уз помоћ небиометријских решења. Годинама велики број e-government апликација функционише у многим развијеним земљама коришћењем небиометријских метода аутентификације за постизање одређене интерактивне услуге. Сличан систем је, у основном облику, успостављен и у неким општинама Републике Србије.[148]

E-government може бити успостављен са или без електронских карти, а уколико је успостављен помоћу њих, оне не морају бити (и у највећем броју случајева у свету нису) биометријске нити идентификационе. Иако су smart карте (без агрегираних биометријских података) једне од најпоузданијих носилаца електронског сертификата и приватног кључа, не треба занемарити чињеницу да је e-government базиран на тој основи често једно у теорији и рекламним проспектима, а друго у пракси.[149] Када се за e-government сервисе користи такво решење, у питању су често секторске и једнонаменске карте. Са друге стране, концепт мултифунционалне карте за обављање свакодневних трансакција,[150] која се грађанима сервира под плаштом комодитета

---

[146] *RSS,* стр. 76.

[147] *FIDISD3.2*, стр. 30.

[148] Добар пример је, рецимо, сајт општине Инђија, на адреси http://www.indjija.net.

[149] *FIDISD3.2,* стр. 6.– Неке од земаља (попут Финске, Естоније, Аустрије и Белгије) су имплементирале e-government решење преко PKI концепта са smart картицама, међутим, у пракси је оно далеко од очекиваног, због неочекивано малог броја корисника који га користи.

[150] Tony Bunyan, нав. есеј, стр. 6.

и практичности,[151] погубан је по приватност. С тим у вези, употреба биометријске личне карте за реализацију e-government сервиса је *потпуно* сувишна. Такво решење је у неким државама одмах после предлагања критиковано од стране надлежних служби и парламентарних тела који брину о приватности грађана.[152] Владе које уводе биометријске или обичне електронске идентификационе карте користе аргумент модернизације управе више да би охрабрили грађане да прихвате концепт електронског идентификационог документа.[153] Притом, главна разлика између идентификације и аутентификације у академским круговима је сасвим јасна, али нажалост, не и у политичким, због чега политичари за решења електронске управе прихватају биометријске, али и многе друге сувишне податке.[154]

Заједнички именилац у готово свим системима где се е-карте критички имплементирају директно за потребе електронских сервиса је да су пројекти редовно мање централизовани и да користе мањи број података (најчешће без биометрије). Са друге стране, када год их предлаже МУП, оне су углавном централизованог типа и са биометријским подацима.[155] Такав концепт доживљава јаку критику академских кругова широм света, који захтевају различите карте са посебним идентификаторима (или макар обезбеђење механизма различитих, дистрибуираних идентификатора у оквиру једне карте), активну употребу механизма анонимности или псеудонимности (у случајевима где прецизна идентификација није потребна) и забрану концепта централне базе података.[156] Уз то, неки академски кругови подвлаче да се не сме се дозволити ни формирање централне базе приватних кључева (који треба да буду само на карти), а да би требало користити појам „карта за електронски потпис“ пре него идентификациона карта, с обзиром да та два концепта треба одвојено посматрати.[157]

Један од најчешћих митова у области идентификационог менаџмента је да је једина аутентификација (потврда) коју треба извршити потврда идентитета.[158] У многим случајевима аутентификација идентитета није ни

---

[151] Исто, 10.

[152] *RSS,* стр. 40.

[153] Dan Balaban, „Grand vision or grand illusion?“, *CardTechnology*, јануар 2006, стр. 36. Часопис преузет са адресе: http://www.cardtechnology.com/attachments/20060130hmfkesir-1-ct_jan_2006.pdf.

[154] Edgar A. Whitley, „Mistaken identity“, *The Parliamentary Monitor*, јун/јул 2006, стр. 32. Текст је преузет са адресе: http://www.csrc.lse.ac.uk/idcard/parlmon.pdf.

[155] *LSEIP*, стр. 95.

[156] Roger Clarke, „Chip-Based ID: Promise and Peril“.

[157] Исто.

[158] Roger Clarke, „Research for eGovernment Key Issues“. Ово је предавање професора Кларка на форуму eGovernment Consultation Workshop 7th Framework Programme for Information Society Technologies, одржаном у Бриселу 26-27. октобра 2005. Ауторизовано предавање је преузето са

битна ни потребна. За многе радње довољна је само потврда неке чињенице, бројчане вредности, атрибута. Примера ради, за неку трансакцију је довољно знати годиште или квалификацију корисника, без улажења у конкретан идентитет, за представљање неке организације потребно је само овлашћење (потврда да се представља нека организација или особа) и томе слично.[159] Наравно, постоје и гранични случајеви, код којих је потребна аутентификација идентитета са једне стране, а анонимност са друге. У случају потврде изласка на гласање, рецимо, потребна је аутентификација идентита, док је код самог чина електронског гласања потребна стопостотна анонимност, што често уме да прави велике проблеме у пракси.[160]

Код електронског пословања, са друге стране, биометријски систем идентификације је сувишан, s обзиром да је обична аутентификација сасвим довољна.[161] С тим у вези, битно је подсетити да највећи број економских трансакција које обављамо са собом носи анонимност, док је форсирање коришћења биометријских технологија у e-commerce (електронска трговина) сврхе директно угрожавање тог начела и води као тоталној идентификацији.[162] Примера ради, уколико је за одређену трансакцију (примера ради, куповину специфичног производа) битан само број година (рецимо, у случају алкохолних пића више од 18, ако је прописано Законом) апсолутно је непотребан и сувишан атрибутиван податак имена или прецизног датума рођења (јер то сасвим непотребно утиче на губљење приватности).[163] Потребно је, дакле, прецизно разграничити у којим случајевима је потребна прецизна идентификација приликом коришћења електронске карте, где је потребан и биометријски податак, а у којим случајевима је потпуна анонимност неопходна (пре свега због проблема профилисања) и биометрија сасвим сувишна, било да се употребљава или не.[164] Иако постоје шеме које обезбеђују

адресе: http://www.anu.edu.au/people/Roger.Clarke/EC/eGovRes0510.html. Придружени материјали на адресама: http://www.anu.edu.au/people/Roger.Clarke/EC/eGovRes0510.ppt и на http://www.anu.edu. au/people/Roger.Clarke/EC/eGovRes0510.mp3.

[159] Исто.

[160] На наведном округлом столу „Elektronski identitet u e-Upravi i zaštita privatnosti“, амерички представник је истакао да су САД имале веома лоше искуство са електронским гласањем (*e-voting*), како због кварова на машинама тако и због притужби на фалсификовање резултата. Холандска хакерска група *Wij vertrouwen stemcomputers niet* („Не верујемо компјутерским системима за гласање“ – *прев.*) је уживо пред ТВ камерама показала сигурносне пропусте везане за алгоритам гласачке машине и могућност надгледања појединачног гласања. После тог догађаја и ирска влада је постала скептична по питању e-voting-а. О томе на: http://www.edri.org/edrigram/number4.19/e-voting?phpsesphpsesID=82ed71e642c541e563ffe680ca04bd2b.

[161] Roger Clarke, „Authentication: A Sufficiently Rich Model to Enable e-Business“.

[162] Roger Clarke, „Five Most Vital Privacy Issues“, верзија од 31. јула 1997. Чланак је преузет са адресе: http://www.anu.edu.au/people/Roger.Clarke/DV/VitalPriv.html.

[163] Edgar A. Whitley, „Mistaken identity“.

[164] Roger Clarke, „Promises and Threats in Electronic Commerce“.

далеко већу приватност грађана, од стране влада се углавном предлажу инвазивна решења, мада су алтернативна решења лако изводљива, поготово у случајевима где није експлицитно потребна прецизна идентификација.[165]

Банке на Западу су у великој мери резервисане када је у питању употреба националног електронског идентификационог документа који би се користио за e-banking, тј. електронску аутентификацију и идентификацију својих корисника приликом обављања финансијских трансакција. Разлог лежи у неповерљивости и чињеници да велике банке користе своја сигурносна решења (такав је случај у Естонији, рецимо, иако њени грађани имају електронске небиометријске карте, и у Малезији, у којој постоје биометријске личне карте).[166]

Политичке структуре често форсирају довођење електронског потписа у ултимативну везу са биометријским системима идентификације, што је потпуно погрешно и са становишта информационих наука и са становишта праксе.[167] Биометрија је потпуно непотребна за било коју имплементацију

---

[165] Roger Clarke, „The Scope for Privacy-Sensitive Biometric Architecture“, верзија од 23. фебруара 2003. Чланак је преузет са адресе: http://www.anu.edu.au/people/Roger.Clarke/DV/BioArch.html.

[166] Dan Balaban, нав. чланак.

[167] Два услова морају бити испуњена да би постојала поуздана информациона архитектура за електронски потпис. Први услов су јаке безбедносне мере за заштиту приватног кључа корисника, а други јаке безбедносне мере за заштиту приватног кључа сертификационог тела. Детаљније о приватном кључу, асиметричној криптографији, електронском потпису, електронским сертификатима и сертификационим телима у критичком апарату поглавља 1.4 и 1.5 наше студије.
Инфраструктура јавних кључева тј. PKI (*Public Key Infrastructure*) је концепт који обезбеђује основне постулате везане за безбедно коришћење електронских трансакција (интегритет поруке, аутентичност страна у комуникацији (аутентификација идентитета), непорецивост и тајност поруке, при чему су прва три захтева обезбеђена електронским потписом). Овај термин често може бити збуњујући (чак и информатичарима), због двојаког приступа. У ширем смислу, PKI се посматра као скуп хардвера, софтвера, људи, регулатива и процедура које су потребне за креирање, складиштење, обраду, дистрибирање и опозив сертификата јавног кључа. Други приступ PKI посматра уже, као конкретно коришћење пара кључева (приватног и јавног) за аутентификацију. Архитектура PKI концепта је у принципу проста и састоји се из клијентског софтвера, серверског софтвера и хардвера. Улога PKI информационе архитектуре је да обезбеди сигурност и поузданост размене информација коришћењем криптографије јавног кључа и употребе тог концепта је за енкрипцију порука и аутентификацију пошиљаоца, електронске поруке и електронских докумената. За детаље погледати *FIDISD3.2,* стр. 6.
Проверљивост и поузданост тврђења да је ималац одређеног кључа заиста особа која се за то представља обезбеђује постојање тзв. *сертификационог тела* (*Certification Authority*), које је надлежно за издавање сертификата, управљање његовим роком и повлачење истог. С обзиром да је електронски сертификат у ствари дигитално потписан тајним кључем сертификационог тела, јасно је да је од круцијалног значаја заштита тог кључа, од кога зависи кредибилитет целог PKI система о коме је реч. За детаље погледати Nikola Marković, Milan Marković, „Uvođenje i prednosti elektronskog poslovanja i elektronskog potpisa - normativno regulisanje -“, излагање на првом југословенском симпозијум о електронској трговини под називом „E-Trgovina 2001“, 29. 05. 2001, Нови Сад.
Инфраструктуру јавних кључева могу обезбедити различите инстанце и организације и углавном свуда у свету сертификациона тела су по правилу комерцијалне институције (најчешће компаније попут Поште или Телеком оператера). Најпознатија поштанска сертификациона тела која су

тог типа – smart карте додуше помажу за поуздано смештање приватног кључа и (квалификованог) електронског сертификата (што је услов за креирање (квалификованог) електронског потписа), али је додатно агрегирање биометрије на њима сувишно, осим за потенцијалну употребу откључавање карте, за шта је погоднији (и далеко коришћенији) PIN код.

водећа (или међу водећим) у својим земљама су: Post.Trust (http://www.post.trust.ie), Пошта Ирске (http://www.anpost.ie); Postecom (http://www.postecom.it), Пошта Италије (http://www.poste.it); Signtrust (http://www.signtrust.de), Пошта Немачке (http://www.deutschepost.de); Certinomis (http://www.certinomis.com), Пошта Француске (http://www.laposte.fr); Certipost (http://www.certipost.be), Пошта Белгије (http://www.post.be); Multicert (http://www.multicert.pt), Пошта Португалије (http://www.ctt.pt); Buypass (http://www.buypass.no), Пошта Норвешке (http://www.posten.no); Post Signum (http://www.postsignum.cz), Пошта Чешке (http://www.cpost.cz); E-paraksts (http://www.e-me.lv), Пошта Летоније (http://www.pasts.lv); Сертификатска агенција Поште Словеније (http://postarca.posta.si), Пошта Словеније (http://www.posta.si); Hongkong Post e-Cert (http://www.hongkongpost.gov.hk), Пошта Хонг Конга (http://www.hongkongpost.com).

Међу наведеним познатим поштанским сертификационим телима, у стручним презентацијама (погледати P. Donohoe, E-Business Programme Manager, „The Information Society - an inspiration and an aspiration for the Posts“, Post Expo 2006, Амстердам, Холандија) наводи се и сертификационо тело Јавног предузећа ПТТ саобраћаја „Србија“ – Центар за електронско пословање Поште – *CePP*, које се назива Сертификационо тело Поште Србије (*Post Serbia Certification Authority*).

Дакле, практично говорећи, основни предуслов за коришћење електронског потписа у пракси је доступност PKI информационе инфраструктуре, док сертификати обезбеђују окружење поузданости рада. Детаљније у *FIDISD3.2*, стр. 9.

С обзиром да је дужина приватног кључа велика (ради сигурности), непрактично је да се он укуцава ручно (то би био вишеминутни посао, уз обавезне грешке у куцању). Стога се практикује да приватни кључ корисника може бити ускладиштен на различитим местима: USB stick-овима, мобилним телефонима, хард дисковима, а у последње време микрочиповима на smart картама, док се сам приступ картици (њено откључавање) најчешће врши помоћу PIN кода или шифре. Могућност биометријског откључавања smart карте је кључни начин потенцијалног коришћења биометријских података у електронској управи (погледати Roger Clarke, „Message Transmission Security"), мада је у пракси редак. Изводе се и пробни пројекти у којима се биометријски подаци директно користе као дигитални потпис или као приватни кључ у PKI окружењу (због претпоставке да су јединствени за сваког корисника), али непремостив проблем у том случају је чињеница да биометријски податак није довољно тајан и инваријантан.

За нашу студију, *најбитније* је нагласити следеће: веза између електронског потписа и биометријских система идентификације није непосредна нити условљавајућа, већ посредна и опциона – она може да постоји, не мора, у пракси је готово нема и најчешће је потпуно сувишна.

Треба навести и чињеницу да имплементација електронског потписа у Европској Унији показује велике разлике у приступу, јер још увек није постигнут консензус на који начин доћи до четири кључне одреднице (лакоћа коришћења, напредни приступ, квалификовано и акредитовано решење) какво је назначено у директивни 99/93/EU. Такође, у неким земљама ЕУ (Аустрија и Белгија) регистрација и сертификација се обавља преко јавног, док се у другим земљама (Немачка и Шведска) обавља преко приватног сектора, што уз чињеницу да у ЕУ не постоји кључно, главно сертификационо тело говори да електронски потписи у техничком смислу у ЕУ нису интероперабилни (не могу се користити решења једне земље у другој) те да су далеко од опште стандардизације. Детаљније у *FIDISD3.6,* стр. 11.

Велики проблем код PKI концепта се назире у будућности, уколико би се остварили неки планови за увођењем концепта глобалног PKI (односно неке врсте колекције националних, регионалних и интернационих PKI) којим би се аутоматизовали сви процеси, с обзиром да би све интеракције и трансакције појединца биле познате преко његовог сертификата. (S. Brands, нав. дело, стр. 20).

Иначе, алтернативе PKI концепту су *Web Of Trust* (пример имплементације је PGP - *Pretty Good Privacy*) и SPKI (*Simple Public Key infrastructure*), чије представљање превазилази оквире ове студије.

У сваком случају, за e-government уопште треба тежити решењу које чува анонимност грађана у свим могућим случајевима, поготово онде где експлицитна идентификација није потребна.[168] Употреба PKI концепта помоћу личне карте може имати својих предности, али се поставља питање безбедности, приватности и практичне неизводљивости уколико не постоји довољан број читача карти.[169]

Занимљиво је да многе европске земље имају концепт електронског потписа који није искључиво везан за било какве електронске карте, мада су оне преферабилне (такав случај је у Литванији, Аустрији, Финској). У тим земљама процедура коришћења електронског потписа може се обавити и помоћу мобилног телефона, па чак и коришћењем USB stick-а.[170] Уз то, треба навести да у већини држава ЕУ грађани могу да обављају е-сервисе, са дигиталним сертификатима и припадајућим кључевима који се налазе на хард-дисковима, што значи да сертификат не мора да буде ускладиштен на smart картама или USB smart stick-овима. Управо преко сертификата складиштених на хард дисковима рачунара обави се највећи број електронских трансакција у западним земљама. Иако је пожељно да грађани користе smart решења, то се од грађана не захтева ултимативно – имају слободу по том питању. Грађани ЕУ најчешће не купују сертификате на картицама, делом и због додатних трошкова око картице и због чињенице да је за smart картице потребно купити и специјални читач (поред јавно доступних), а делом због понекад компликоване инсталационе процедуре.

Оно што је веома битно нагласити је да се сви сервиси електронске управе и потенцијална интеракција различитих база података морају претходно законом прецизно нормирати, а њихова примена контролисати од стране независног експертског тела.

Све наведено даје закључак да су биометријски системи идентификације, поготово у склопу e-government (а у великој мери и за e-commerce и e-banking) решења сувишни и претерано инвазивни, да могу представљати озбиљан проблем из аспекта приватности и угрожавања информационе етике, те да је аргумент њиховог увођења са разлогом модернизације управе пренаглашен и непостојан.

---

[168] *FIDISD3.2,*стр. 6. – Анонимности или псеудонимност у неким земљама омогућава и законски оквир (такав је случај са Немачком, рецимо).

[169] *FIDISD3.6*, стр. 45. – У контексту безбедности и приватности, проблем може представљати место складиштење кључева. Можда је најбоље решење у Финској, где је приватни кључ у рукама искључиво имаоца карте и може се користити само убацивањем PIN кода познатог само имаоцу карте, који га по потреби може и променити. Карта се аутоматски закључава уколико је три пута заредом укуцан погрешан PIN код. Овим приступом се на једноставан начин обезбеђује питање безбедности код електронског потписа: где је приватни кључ складиштен и како се штити.

[170] Исто, стр. 9. – То је тзв. процедурално решење електронског потписа. У случајевима попут Белгије и Немачке, где се користе само smart карте, имамо тзв. решење везано за картицу.

2.10 Поузданост биометријских система идентификације

Теоријским радовима и експерименталним студијама је дефинитивно потврђено да ће постојати групе људи на којима отисак прстију као идентификатор неће давати добре резултате, због оштећења коже редовно присутних код физичких радника.[171] О томе говоре званичне студије изводљивости неких западних влада.[172]

Експерти за биометријску идентификацију наводе да, противно популарним веровањима, биометријски отисак не остаје *потпуно* исти током целог живота јер на то утичу многи фактори: температура, влага, прљавштина..., док фацијални скенови праве још више проблема.[173] Овај аргумент није у контрадикцији са тврдњама да уколико се биометрија украде, крађа је (због релативне непроменљивости податка) почињена заувек. Наиме, аргумент променљивости говори о специфичним променама које могу збунити биометријски систем за идентификацију, док аргумент *суштинске* непроменљивости говори о задржавању карактеристичких биометријских својстава кроз цео живот, ма колико да постоје одступања у различитим временским интервалима која могу збунити аутоматски систем.

С тим у вези, тврдња да су биометријски системи идентификације непогрешиви је чиста илузија, мада их многи управо тако перципирају.[174] Та чињеница да се биометријски системи идентификације базирају на вероватноћи, ма колика она била, може довести до одређених проблема. Примера ради, ако би само један посто људи приликом идентификације спало у *false negative* (немогућност поклапања са претходно унетом информацијом), то би значило непотребно задржавање и малтретирање стотина људи дневно само на граничним прелазима.[175]

Са друге стране, иако је критикован управо по питању поузданости (рецимо, могућност крађе или погађања шифре), PIN код се не базира на степену вероватноће као биометријски системи података и у том контексту је далеко предвидљивији као улазни податак.[176]

---

[171] Bori Toth, нав. дело, стр.3.

[172] *LSEIP*, стр. 174. – Студија изводљивости коју је за потребе британске владе извео *Центар за математичка и научна израчунавања Националне лабораторије за физику* (*Centre for Mathematics and Scientific Computing at the National Physical Laboratory*) је показала да систем нема стопостотну поузданост приликом идентификације популације, те да је за поузданост потребно увођење великог броја биометријских идентификатора (који укључују чак и распоред вена и гласовне компоненте), што ствара нове проблеме интрузивности технологије.

[173] Wendy M. Grossman, нав. дело, стр, 13. – То је тврђење Џејмса Вејмана (*James Wayman*), британског експерта из области биометријске идентификације, који је радио истраживање за британску владу.

[174] Malcolm Crompton, нав. дело, стр. 13.

[175] *FIDISD3.6*, стр. 22.

[176] Исто.

2.11 Закључак

Иако постоје и проблеми техничке природе, проблематика биометријских система идентификације није примарно технолошког, већ концептуалног карактера, с обзиром да у слободним друштвима у којима се први пут уводи прети да из темеља редефинише однос грађанина и државе. Прикупљање огромног броја биометријских података сваког грађанина, правно-философски гледано, представља повреду права на приватност заштићену мултилатералним међународним конвенцијама о заштити основних људских права, имплементираних у многим националним законодавствима. Са друге стране, поставља се сасвим сувисло питање да ли таквим поступком држава практично шаље сигнал да су сви сумњиви, што би било de facto (ако не de jure) укидање претпоставке невиности, фундаменталне за свако слободно друштво. Консеквентним развојем биометријских система идентификације и њиховом некритичком употребом, паноптичка (над)државна структура тоталног надзора може постати реалност у релативно кратком временском року. Све већа концентрација информација о грађанима у рукама режима водила би у том смислу ка информационо контролисаном друштву, чијем успостављању би посебно погодовао концепт централне базе биометријских (и осталих) података и коришћење јединствених идентификатора за различите радње, уз постепено укидање концепта анонимности и псеудонимности грађана приликом обављања различитих електронских трансакција.

Разлози које пропоненти увођења аутоматизованих биометријских система наводе као разлог најчешће нису фундирани на објективним чињеницама или су пак пренаглашени, док сама имплементација долази у колизију са општеприхваћеним цивилизацијским нормама. Проблеми етичког, правно-политичког и информационо-безбедносног карактера указују да је потребно активно учешће академске и стручне јавности, као и више времена за осмишљавање правилног решења које би постигло прави баланс између права грађана и потреба данашњице. Имплементација оваквих система ван тог приступа у будућности води тоталитарној парадигми чији обим још увек не можемо да наслутимо. Уколико би се данас дозволила некритичка имплементација биометријских система идентификације, будућа решења би се сасвим сигурно отргла контроли грађана. Стога је императив на критичком и проактивном осмишљавању правилног приступа овој проблематици, уз уважавање етичких принципа и воље грађана. Саморегулаторни принципи који се заснивају на реактивном приступу могу само довести до иреверзибилног угрожавања концепта слободног друштва.

Имплементација биометријских система идентификације у свету — аналитички преглед —

Свако друштво које би се одрекло мало слободе да би добило мало сигурности, неће залужити ниједно, а изгубиће обоје.

Бенџамин Френклин

Конкретна имплементација биометријских система идентификације у свету варира у зависности од различитих критеријума.

Први критеријем је степен грађанских слобода (који се различито схвата у зависности од правно-политичког устројства и историјата конкретне земље). Приметно је да се биометријски системи идентификације најпре, у највећем броју и увек обавезујуће, имплементирају у земљама Блиског и Далеког истока, у којима су грађанске слободе у највећем броју случајева спорне.

Други критеријум је везан за различите начине имплементације: биометријске личне карте, пасоши, друга документа или пак биометријска идентификација без икаквог докумената.

Трећи критеријум је режим обавезности односно добровољности.

Да би се стање у свету објективно сагледало, најбоље је парцијално посматрати земље према групама зависно од историјских и правно-политичких особености, управо кроз категорије типова докумената и подкатегорије режима обавезности.

3.1 Биометријске личне карте

Биометријске личне карте представљају тип званичног националног идентификационог документа који у себи агрегира биометријске податаке у електронском облику. Мали број земаља у свету данас има биометријске електронске личне карте на националном нивоу у обавезујућем виду. Најмодерније smart карте тог типа од скора постоје у само неколико развијених земаља у свету, док већ неколико година постоје у земљама ниског стандарда грађанских слобода.[1] Прилично су распрострањене и у земљама са изузетно малобројном популацијом.[2] Реакције јавности на такве пројекте углавном су зависиле од степена развијености грађанско-правних норми, слободе говора, академске свести и независности судских инстанци.[3]

3.1.1 Земље „common law" система

Ниједна од главних земља обичајног права данас нема чак ни обичне „папирне" (или пак „пластифициране") личне карте.[4] Изузетак је Велика Британија, где због огромног отпора мислеће заједнице и политичке опозиције још увек није могуће макар приближно одредити како ће се завршити пројекат планираног увођења биометријског система идентификације грађана на националном нивоу. Разлог зашто је лична карта страна овим земљама лежи у њиховом социолошком миљеу, у коме су грађани навикли да имају загарантовану приватност у односу на државу.[5] Са друге стране, овај анимозитет према личним картама се у великој мери ослања и на чињеницу да су такви документи у историји људског рода често служили за велике злочине.[6] Стога не чуди чињеница да се у земљама обичајног права воде жестоке дебате о томе да ли уопште треба уводити *било какве* личне карте, јер се за потребе

---

[1] APF, „National ID scheme; Elsewhere in the World". Чланак је преузет са адресе: http://www.privacy.org.au/Campaigns/ID_cards/Resources.html#NatIDSchemes.

[2] Bori Toth, нав. дело, стр. 1.

[3] Постоје случајеви да су надлежни судови после увођења сличних пројеката доносили одлуке да је у питању противуставни пројекат који се коси са правом на приватност грађана. О томе детаљније у одељку 3.1.4.1, где је приказана студија случаја везана за Јапан и Тајван.

[4] CIPIC, „National ID Cards". Чланак је преузет са адресе: http://www.cippic.ca/en/faqs-resources/national-id-cards.

[5] *LSEIP*, стр. 80.

[6] Обавезујући режим личних карти има историјски терет честих злоупотреба. Навешћемо само неколико примера: у Немачкој то је био срамни „J" жиг у исправама, у Јужноафричкој републици личне карте су коришћене да би се црнци изузели од друштвених активности, у Руанди је ознака *Туши* у личним картама коришћена као механизам за велико етничко чишћење супарничког племена. За дубљи увид у проблематику погледати чланак под називом „Group Classification on National ID Cards as a Factor in Genocide and Ethnic Cleansing", аутора Џима Фусела (*Jim Fussell*) на адреси http://www.preventgenocide.org/prevent/removing-facilitating-factors/IDcards/, као и текст Џулије Ширс (*Julia Scheeres*) под називом „ID Cards Are de Rigueur Worldwide", *Wired*, 25. септембар, 2001, на адреси http://www.wired.com/news/conflict/0,2100,47073,00.html.

идентификације ионако користи возачка дозвола или пасош. На просторима ових земаља, покушаји увођења биометријског система идентификације чак и међу индијанска племена су доводили до бурних реакција.[7]

У Аустралији је 80-тих година прошлог века покушај увођења националног идентификационог документа доживео тотални крах,[8] док је предлог из 2005. године, за увођење биометријских докумената, наишао на огроман отпор академске јавности и угледних институција,[9] као и на негативне реакције више штампаних медија.[10] Судећи према тим реакцијама, мала је могућност да ће аустралијска влада данас успети са предлогом увођења биометријских личних карти.

Канадска влада је пре неколико година имала у виду увођење биометријских идентификационих докумената. Тим поводом је канадски парламент оформио посебну комисију која је прво проучила предлог из различитих аспеката и документовала искуства других земаља, да би потом донела посебан извештај (датиран 8. октобра 2003).[11] Извештај се негативно изразио према увођењу биометријских идентификационих карти у Канади, због чега је тај пројекат одложен на неодређено време. Овај извештај су са нескривеним симпатијама дочекале готово све светске организације које се боре за приватност грађана.[12] Комисија која је радила извештај за канадску владу је у закључку поменула да би увођење личних карти у канадско друштво пореметило основне вредности на коме оно почива.[13]

---

[7] Kahentinetha Horn, „Smart Cards to be tried on Mohawks and Crees “. Текст је преузет са адресе: http://noii-van.resist.ca/smart_cards.html, MNN Mohawk Nation News. – Представници племена Мохавка и Крија су се отворено успротивили плану који је то предвиђао за Аборицине у Квебеку.

[8] APF, „The Australia Card Proposal 1985–87“. Текст је преузет са адресе: http://www.privacy.org.au/Campaigns/ID_cards/Resources.html#OzCard.

[9] Велики број угледних аустралијских институција и организације је устао против овог предлога. То су, између осталог, *Федерална полицијска асоцијација* (AFPA), која тврди да овакве карте неће помоћи у борби против криминала и тероризма, затим аустралијска *Индустријско-трговиска комора* (ACCI), са саопштењем да таква карта неће спречити крађе, а де ће пуно коштати земљу, потом аустралијска *Медицинска асоцијација* (AMA), која је реаговала због предлога да се карта повеже са здравственим сектором, *Аустралијска рачунарска асоцијација* и многе друге. Против тог предлога је устао и огроман број организација које се боре за грађанска права. За детаљан списак погледати линк : http://www.privacy.org.au/Campaigns/ID_cards/Opponents.html.

[10] „Yet another crisis of identity card?“, The Melbourne Age, 18. јул 2005; „Identity card not part of war on terror“, The Brisbane Courier-Mail, 19. јул 2005; „Smile for the cameras: technology and the ID card debate“, The Sydney Morning Herald, 19. јул 2005; „Universal ID still on the cards“, Sydney Morning Herald, 6. фебруар 2006. Више детаља на линку: http://www.privacy.org.au/Campaigns/ID_cards/Opinions.html.

[11] Standing Committee on Citizenship and Immigration, *A national identity card for Canada?,* октобар 2003. Документ је преузет са интернет адресе канадског парламента: http://cmte.parl.gc.ca/Content/HOC/committee/372/cimm/reports/rp1085068/cimmrp06/cimmrp06-e.pdf. У даљем тексту *NICC*.

[12] Privacy International, „Canadian parliamentary report ridicules id cards as pointless, costly and dangerous“, Media release, 08. 10. 2003. Извештај је преузет са адресе: http://www.privacyinternational.org/article.shtml?%20cmd[347]=x-347-183137&als[theme]=ID%20Around%20the%20World.

[13] *NICC*, стр. 28.

Иако у САД не постоји формални програм увођења националне личне карте, тзв. *Real ID Act* то чини „на мала врата“, путем усаглашавања возачких дозвола које америчке државе издају на националном нивоу.[14] Са друге стране, таква иницијатива је већ судски оборена у једној од држава чланица федерације,[15] а посланици друге државе су гласали за укидање тог закона.[16] С тим у вези, организације које се боре за очување права на приватност одмах су указале на опасност од потенцијалног стварања централне базе података, поготово у контексту ранијих дешавања.[17]

Real ID Act је настао после извештаја комисије одређене за испитивање догађаја који су се одиграли 11. септембра, која је закључила да су скоро сви учесници отмице авиона имали су неки вид идентификационог документа. У том нападу, неки од терориста имали су возачке дозволе које су прибављене помоћу лажних докумената,[18] због чега је комисија закључила да је потребно усвојити нове техничке стандарде за документа за идентификацију попут возачке дозволе. Резултат те иницијативе био је управо *Real ID Act* од 2005. године, усвојен од стране Конгреса.[19] Бољим познаваоцима ове проблематике није промакао начин на који је контроверзни закон донет – као додатак на хитан закон о додатном финансирању америчких трупа у Ираку, мимо знања огромне већине америчких сенатора. Више угледних сенатора је изразило револт чињеницом да је изостала било каква дебата у Сенату по том питању, и да сенатори нису могли да расправљају о његовим вредностима или недостацима, већ им је закон представљен у виду уцене – као „патриотски“ тест да ли подржавају или не подржавају америчке трупе у „рату против тероризма“, тј. примарни, хитни закон о додатном финансирању америчких војника у Ираку који је предложен, уз

---

[14] EPIC, „National ID Cards and REAL ID Act“. Рад је преузет са адресе: http://www.epic.org/privacy/id_cards/.

[15] Џорџија је забранила скупљање отисака прстију за потребе возачких дозвола, због страховања од крађе идентитета. Видети о томе у извештају организације Privacy International под називом „US State of Georgia passes law banning fingerprints in licenses“, 08. 04. 2005, на адреси: http://www.privacyinternational.org/article.shtml?%20cmd[347]=x-347-180966&als[theme]=ID%20Around%20the%20World.

[16] Скупштина државе Мејн је гласала за укидање спорног закона. Погледати извештај о томе на сајту владе ове државе: Senator Libby Mitchell, „Joint Resolution Memorializing the President of the United States and the Congress of the United States to Repeal the Real ID of 2005“, на адреси: http://www.mainesenate.org/mitchell/realid.htm.

[17] Marc Rotenberg, „Real ID, Real Trouble?“, *Communications of the ACM*, *Vol. 49, No. 3*. Чланак је преузет са адресе: www.epic.org/privacy/id_cards/mr_cacm0306.pdf. – Примера ради, пљачка одељења за моторна возила Лас Вегаса у којој је украдена информација за преко 8 хиљада ималаца возачких дозвола.

[18] Accenture Technology Labs, нав. дело, стр. 4. – У САД се документа попут возачке дозволе и пасоша прибављају на основу потврде о рођењу (*birth certificate*). Она је слична изводу из матичне књиге рођених.

[19] Marc Rotenberg , нав. чланак.

који је *Real ID Act*, као секундаран, захваљујући специфичним правилима америчког Конгреса, ишао по аутоматизму. Може се закључити да сам маневар путем којег је *Real ID Act* постао закон у САД указује на суштинску слабост аргумената у његову корист, и бојазан исхода истинске дебате о њему, тј. о националним биометријским личним картама, од стране снага које су га и предложиле.[20]

За сада се у Америци биометријске електронске карте на ширем обавезујућем нивоу користи само људство које је укључено у активности Министарства одбране (*Department of Defense*).[21] Рачуна се да приближно четири милиона војних лица и цивила запослених у овом министарству носи овакве идентификационе карте (*Common Access Cards*), које се користе и за електронско потписивање докумената.[22] У овом пројекту као и у *Real ID Act*-у, мислећи чланови друштва виде покушај владе да на заобилазан начин уведе биометријске личне карте.[23]

У САД је, иначе, више пута покушано у току протеклих деценија да се *Social security number* (јединствени број социјалног осигурања, донет још 1936. године) претвори у универзални идентификатор (попут ЈМБГ у Србији), што би се могло искористити и за званичан идентификациони документ и формирање неке врсте централног регистра. Такви су се покушаји сваки пут до сада завршили неуспехом.[24]

Са друге стране, *Social security number* се све више користи за разне сврхе, због чега је крађа идентитета криминал са највећим порастом у САД, јер преко тог идентификатора криминалци долазе до огромног броја података простим укрштањем различитих база података које га имају у саставу својих поља.[25] Та чињеница се често узима као одличан пример на коме се види како централна база података води ка огромним губицима по питању крађе осетљивих података и велике материјалне штете.[26]

---

[20] Види детаљан опис Real ID Act-а, као и маневра путем којег је донет, код Charlotte Twight, *Limited Government, Ave Atque Vale*, Independent Review, Volume X, No. 4, Spring 2006, Oakland, CA, USA. Рад је преузет са адресе: http://www.independent.org/pdf/tir/tir_10_4_01_twight.pdf

[21] Ову информацију је истакао Жил Бернабе (*Gil Bernabeu*) у предавању под називом „Global Platform Technical Activities for ID“, на конференцији Porvoo9 одржаној 11-12. маја 2006. у Љубљани. Сиже предавања је преузет са адресе: http://porvoo9.gov.si/pdf/thu_13_1635_GBernabeu_GlobalPlatform_Porvoo9.pdf . Наведени податак налази се на 7. страни сижеа.

[22] „Smart Cards Win Some, Lose One, In U.S.“, (непотписан чланак), Global Newswatch, *Card-Technology*, новембар 2006., стр. 12. Часопис је преузет са адресе: http://www.cardtechnology.com/attachments/20061218lzr1p6co-1-ct_nov_2006.pdf.

[23] EPIC, „Your Papers, Please: From the State Drivers Licence to a National Identification Systtem“. Чланак је преузет са адресе: http://www.epic.org/privacy/id_cards/yourpapersplease.pdf.

[24] EPIC, „National ID Cards and REAL ID Act“.

[25] Wendy M. Grossman, нав. дело, стр. 11.

[26] *FIDISD3.2*, стр. 30. – Ова штета се у случају САД процењује на око 48 милијарди долара у последњих 5 година.

3.1.1.1 Студија случаја – Велика Британија

Предлагач биометријског система идентификације за грађане Велике Британије била је лабуристичка партија Тонија Блера. Поводом тог предлога су се неколико година водиле жестоке парламентарне дебате,[27] о чему на сајту британске владе постоји званична документација.[28] Највеће страхове међу противницима овог система подигла је чињеница да је према спорном предлогу закона у самом централном регистру требало да се води око 49 различитих типова информација.[29] Владин *Заједнички комитет за људска права* објавио је извештај у коме наводи да би такав закон потенцијално био у колизији са европском *Конвенцијом о људским правима*,[30] а многи званичници су указали да се увођењем те врсте идентификација отвора простор ка тоталном надзору државе,[31] те да су владина образложења погрешна и не воде одбрани већ угрожавању права грађана.[32]

Дефинитивно најтемељнију и медијски најшире пропраћену критику предлога закона британске владе упутили су професори престижне Лондонске школе економије и политичких наука (*London School of Economics and Political Science*, у даљем тексту LSE).[33] Њихов извештај је парламентарну расправу подигао на озбиљан академски ниво. Реакција владе на тај извештај била је крајње негативно интонирана,[34] а као одговор, LSE је првобитну студију потврдила још једним извештајем.[35] Због увреда које су неки слу-

---

[27]Парламентарна дебата у Великој Британији по том питању је повремено попримала облик парламентарне кризе. Припадници Конзервативне партије су најавили да би укинули закон после доласка на власт, уколико би он био изгласан у парламенту. Дом Лордова је чак 5 пута одбијао закон, после чега је прошла значајно измењена легислатива. Више информација у BBC-јевом прилогу „Q&A: Identity card plans“ на адреси http://news.bbc.co.uk/1/hi/uk_politics/3127696.stm.

[28] Погледати страницу британског Парламента под називом *Home Affairs - Minutes of Evidence*, на којој су изложена сведочења учесника ове дебате, на адреси: http://www.publications.parliament.uk/pa/cm200304/cmselect/cmhaff/130/3121101.htm.

[29] BBC, „What data will ID cards store?“, 11. јул 2006. Интервју је преузет са адресе: http://news.bbc.co.uk/2/hi/uk_news/politics/4630045.stm

[30] Mikro, „Neizvesna sudbina britanskog Zakona o izdavanju biometrijskih ID kartica“. Вест од 17. 03. 2005. је преузета са адресе: http://www.mikro.co.yu/ser/vesti/vesti.php?datum=2005-03-17&ID=6852.

[31] BBC, „ID plan excessive, says watchdog“. Прилог је преузет са адресе: http://news.bbc.co.uk/2/hi/uk_news/politics/4627881.stm.

[32] Patrick Wintour, „ID cards 'will reveal details of daily life'“, *Guardian,* 28. 06. 2005. Текст је преузет са адресе: http://www.guardian.co.uk/idcards/story/0,15642,1516115,00.html.

[33] У студији LSE (под називом *The Identity Project*, датираној од јуна 2005, у критичком апарату наше студије коришћеној под скраћеницом *LSEIP*), који је потписало око стотину професора и стручних сарадника, оцена владиног пројекта биометријских личних карти је крајње негативна. Закључак под називом „ID Cards - UK's high tech scheme is high risk“ се налази на адреси: http://www.lse.ac.uk/collections/pressAndInformationOffice/newsAndEvents/archives/2005/IDCard_FinalReport.htm.

[34] Министар Чарлс Кларк га је чак назвао „партизанским пројектом“.

[35] LSE, *Research Status Report*, Лондон, јануар 2006. Студија је преузета са адресе http://www.csrc.lse.ac.uk/idcard/statusreport.pdf. Закључак овог извештаја под називом „ID Cards - LSE declines

жбеници британске владе упутули на рачун људи који су радили ове критичке извештаје,[36] академска јавност и парламентарна тела су устали у заштиту академских слобода.[37] Запрепашћујућа је чињеница да је чак и међу неким академским грађанима било реакција *ad hominem* на извештај LSE,[38] на шта је од стране ове престижне установе аргументовано и у достојанственом тону одговорено.[39]

Сумарни закључак LSE је да је владин предлог сувише комплексан, технички небезбедан, превише прескриптиван и без потребне јавне подршке.[40] Поред чисто техничких питања, LSE је указала на контрадикторне изјаве владиних службеника по питању могућности вишеструког идентитета (копирања карте)[41] и поставила више до данас неодговорених питања.[42]

После вишемесечних парламентарних дебата и критике мислеће јавности прошао је у великој мери измењен закон (донет 30. марта 2006),[43] према коме је компромис између заговорника и противника закона постигнут је на тај начин што је уведен прелазни период, од 2008 до 2010. године, у коме идентификационе карте неће бити у обавезујућем виду. Са друге стране, лични подаци британских држављана који пре тог буду поднели молбу за издавање пасоша ће ипак бити унети у Националну базу идентификационих података (*Национални идентификациони регистар* - NIR).

Иако је некакав компромис постигнут, представници конзервативне партије отворено су најавили да ће поништити закон када дођу на власт,[44] док су либералне демократе устврдиле да је то најнелибералнији закон донет у Великој Британији у последњих 50 година и да редефинише однос између државе и грађанина.[45]

---

to issue further costings because of 'secrecy and contradictions'", 15. 01. 2006, налази се на адреси: http://www.lse.ac.uk/collections/pressAndInformationOffice/newsAndEvents/archives/2006/IDCard_StatusReportJan06.htm

[36] Пре свега на рачун Сајмона Дејвиса (*Simon Davies*), једног од вођа пројекта.

[37] *HCICT*, стр.30.

[38] Dr John Daugman, „Inquiry on Use of Scientific Evidence in Policy Formation and Assessment", University of Cambridge, преузето из *HCIC*T, Appendix 6. – У реакцији професора Догмана наводи се да у истраживању LSE нису учествовали научници, већ да је све урађено под иницијативом Сајмона Дејвиса, гостујућег професора LSE и директора организације Privacy International.

[39] LSE, „Memorandum from the London School of Economics and Political Science Identity Project Team", преузето из *HCICT*, (Appendix 8).

[40] *LSEIP*, Conclusions in Detail.

[41] LSE, *Research Status Report*, стр. 45.

[42] Исто, стр. 46-49.

[43] EBP, „UK National Identity Register on its way", 26. 09. 2006. Вест је преузета са адресе: http://www.europeanbiometrics.info/news/newsdetail.php?Id_news=282.

[44] Privacy International, „UK Government narrowly wins ID card bill", 30. 03. 2006. Извештај преузет са адресе: http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-531723.

[45] EBP, „UK House of Commons passes ID Cards Bill", 18. 10. 2005. Вест је преузета са адресе:

Грађане Велике Британије највише брине проблем централне базе података, размене тих података са разним службама и остављање трага у бази о месту и времену идентификације.[46] Неки званичници британске владе забринути су због проблема који могу уследити после 2008. године, с обзиром на став грађана према биометријском систему, непознаницама и чињеници да систем није довољно тестиран.[47] Забринутост посебно расте због чињенице да се прецизно не зна које би се све базе у будућности додавале и како би биле укрштане. Влада је са друге стране отворено најављивала потребу укрштања база података, попут оних које се односе на децу (школских, здравствених итд), што је британски известилац за информације директно окарактерисао као потенцијалну стигматизацију невине деце која би се уклопила у негативан профил.[48]

Оно што је уследило половином децембра 2006. године је очигледно потврдило ставове професора LSE. Влада је издала званичан документ у који је унела велики број промена у биометријски пројекат (у највећем делу управо према критици ове престижне установе), због чињенице да је дошло до великих проблема приликом имплементирања система.[49] Највеће промене у владином плану јесу напуштање првобитног концепта централне базе података (мада не у потпуности, јер нови приступ само раздваја биографске, биометријске и административне информације) [50] и одустајање од скена рожњаче као биометријског идентификатора.

Реакције опозиционих партија говоре да овај пројекат нема светлу будућност. Са друге стране, студије пробиометријских табора показују да су грађани Велике Британије ипак већином за национални идентификациони документ, те да је такав случај чак и у Канади.[51] Међутим, студије независних медија говоре о изразито негативним реакцијама грађана,[52] док нека испитивања јавног мњења иду чак дотле да је могуће да ће милиони грађана одбити

---

http://www.europeanbiometrics.info/news/newsdetail.php?Id_news=44.

[46] EBP, „UK National Identity Register on its way“.

[47] EBP, „UK Home Office advisor urges biometrics testing“, 23. 10. 2006. Вест је преузета са адресе: http://www.europeanbiometrics.info/news/newsdetail.php?Id_news=311.

[48] EDRI, „FIPR report on children's databases - likely to harm rather than help“, *EDRI-gram 4.22*, 22. новембар 2006. Анализа је преузета са адресе: http://www.edri.org/edrigram/number4.22/fipr-children-database.

[49] Погледати тим поводом реакцију професора LSE под називом „LSE Identity Project authors say government has taken the first step towards common sense but still risks total failure“, на адреси http://www.csrc.lse.ac.uk/idcard/StrategicActionPlanResponse.htm.

[50] EBP, „Opportunity of Mega ID database questionned in UK“, 21. 12. 2006. Вест је преузета са адресе http://www.europeanbiometrics.info/news/newsdetail.php?Id_news=359.

[51] EBP, „Canada: Biometrics in favour, poll shows“, 02. 10. 2006. Резултат истраживања је преузет са адресе: http://www.europeanbiometrics.info/news/newsdetail.php?Id_news=287.

[52] Према званичним истраживањима BBC-а против овог закона се изјаснило 83% грађана. Анкету под називом „Do you support ID cards?“ погледати на http://news.bbc.co.uk/1/hi/talking_point/4625971.stm.

складиштење њихових података у централну базу, чак и по цену новчане казне и одласка у затвор.[53] Студије урађене од стране пробиометријских организација показују и да велика већина грађана не зна основне ствари у вези са биометријском идентификацијом, те да се трећина грађана противи формирању централне базе података, макар она помогла и борби против тероризма.[54]

Проблематика централних база података у британском друштву није везана само за биометријске пројекте. Због чињенице да ће милиони података о здравственим корисницима, ван њихове воље, бити убачени у централизовну базу којој ће приступ имати око 250 хиљада радника британског Националног здравственог сервиса, велики број организација, стручњака и службеника дигао је глас против.[55] Са друге стране, већ сада постоје огромни притисци од стране полицијских и имиграционих органа за приступ овој бази.[56] Британска медицинска асоцијација (*The British Medical Association*) насупрот томе тражи од владе да се подаци у централну базу складиште искључиво уколико се пацијенти са тиме експлицитно слажу.[57] Посебан проблем представљају упозорења да је систем небезбедан на неауторизован приступ. [58] Према неким проценама, више од 50% грађана захтева добровољност уноса својих здравствених података у централну базу.[59]

Све наведено говори да је британско друштво дубоко поларизовано како по питању биометријских личних карти тако и по питању концепта централних база биометријских (и осталих) података.

3.1.2 Земље Европе и Европске Уније

Европске земље немају кохерентан став по питању личних карти, било по питању самог постојања (постојање или непостојање личних карти), режима (добровољност или обавезност) или конкретне имплементације (папирне, пластифициране, електронске или електронске са биометријом). Исто је и са земљама које су чланице ЕУ. У многим од тих земаља употреба идентификационих карти је секторска јер се користе у областима социјалног и/или здравственог осигурања.

---

[53] Philip Johnston, „Millions may resist database, says poll“, *Telegraph*, 5. 12. 2006. Чланак је преузет са адресе: http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2006/12/04/ndata04.xml.

[54] EBP, „Opinion: Biometrics gain British citizens approval“, 24. 10. 2006. Анализа је преузета са адресе: http://www.europeanbiometrics.info/news/newsdetail.php?Id_news=308.

[55] David Leigh, Rob Evans, „Warning over privacy of 50m patient files“, *Guardian*, 1. 11. 2006, Чланак је преузет са адресе: http://society.guardian.co.uk/health/news/0,,1936403,00.html.

[56] Исто.

[57] Исто.

[58] Исто.

[59] EDRI, „Campaign launched in UK to opt out of central medical database“,EDRI-gram 4.23, 6. 12. 2006. Прилог је преузет са адресе: http://www.edri.org/edrigram/number4.23/uk_medical_database.

Не постоји ни заједнички став према употреби биометријских личних карти, јер један број земаља их планира или уводи, док нешто већи број земаља не сматра да су биометријски подаци у личним картама нешто што је преко потребно за безбедност.[60] Са друге стране, земље ЕУ се углавном негативно односе према концепту централне базе података уколико га треба применити на своје грађане, али га зато увелико примењују за имигранте, апликанте за азил и визу.[61]

3.1.2.1 Иницијативе, препоруке и директиве телâ ЕУ

Савет Европске Уније је разматрао правне основе за стандардизацију увођења биометријских отисака у личне карте на тлу ЕУ. Приликом расправе представника земаља ЕУ дат је предлог за уношење биометријских података у личне исправе грађана који живе у ЕУ, чему су се снажно успротивиле неке чланице, захтевајући ширу јавну дебату о правним и финансијским аспектима, а не само техничким.[62] На састанку који је трајао 13-14. јула 2006. године донела је одлука да Савет Европе нема ингеренција да одлучује о таквим стварима, те да су његови закључци необавезни за национална законодавства.[63] Са друге стране, у политичком смислу ти закључци се нелојално користе међу политичким структурама да би се на националном нивоу легитимисало увођење биометријског система идентификације и да би већина земаља увела такав систем, када би се и формално покренуло питање хармонизације.[64]

У анексу ЕУ документа *8943/1/06* под називом „Минимални стандарди безбедности за личне карте издате од стране држава-чланица које су валидне као путне исправе“ (*Minimum security standards for identity cards valid for travel issued by Member States*) предлагале су се безбедносне мере за небиометријске личне карте, док се у последњем параграфу помињали биометријски подаци, у смислу да би их требало уградити уколико се лична карта користи као документ за путовање кроз шенгенску зону и у регулацији биометријског пасоша,[65] а према прописима Савета о биометријским пасошима.

---

[60] *FIDISD3.6*, стр. 16. – Наводи се да је у контексту будућих идентификационих планова 5 земаља отворено пробиометријски, а 8 антибиометријски настројено.

[61] Исто, 23. – За азиланте се води тзв. *Eurodac* база података, у којој се чувају њихови отисци прстију десет година од дана узимања, док се за апликанте за визу користи база под називом VIS, у којој се подаци чувају пет година по истеку визе.

[62] EBP, „Debate on Biometrics on National ID Cards“, 25. 08. 2006. Чланак је преузет са адресе: http://www.europeanbiometrics.info/news/newsdetail.php?Id_news=250. – Белгија и Чешка Република су се оштро успротивиле наведеном предлогу.

[63] Statewatch, „EU: Biometrics and national ID cards back on the table“. Документ је преузет са адресе: http://www.statewatch.org/news/2006/jul/09eu-id-cards.htm.

[64] Исто.

[65] Исто.

Та регулација подразумева бесконтактни чип на карти, који са друге стране нема већина земаља ЕУ која је увела електронске идентификационе документе. Савет ЕУ је 4-5 децембра 2006. године, донео прелазну верзију документа под бројем *15801/06.* У одељку под називом „Identity cards - Member States' Resolution“ наводи се да личне карте које би се користиле за потребе путовања по ЕУ треба да имају биографске податке машински читљиве према ICAO 9303 (*Part 3 Volume 1*) спецификацији, а *уколико* оне садрже биометријске податке они треба да буду складиштени и читљиви према поменутој спецификацији (*Part 3 Volume 2*).[66] То у принципу значи да су питања узимања (а самим тим и складиштења) биометријских података остављена на решавање националним законодавствима којима је дата *потпуна аутономија* по том питању и да нико не обавезује национална законодавства да користе биометријске податке у исправама, макар оне биле коришћене и за друге сврхе осим идентификационих у оквиру матичних држава.[67]

Уз то, најновија директива (*9010/1/06*) за израду униформисаних возачких дозвола за земље чланице ЕУ предвиђа документ налик на кредитну картицу, са роком трајања од 10 година (да би фотографија на документу била што ажурнија), али *без обавезног микрочипа*, који је као у случају личних карти остављен као опција националним законодавствима.[68]

Са друге стране, Европска комисија израђује стандард на основу кога, *уколико* нека земља жели да уведе личне карте са чипом, он буде читљив свакој од земаља чланица.[69] Дакле, када су у питању личне карте, мада постоје препоруке, националним законодавствима је дата *потпуна аутономија*.

Све наведено, ипак, показује да постоји одређени (политички) притисак за увођење биометријских личних карата у Европи, иако не постоји формално-правни основ на коме би се он базирао. Биометријски пропоненти се труде да објасне како не треба дозволити да европске земље каскају за далекоисточним земљама које развијају биометријске системе само због новеле коју је средином прошлог века написао Џорџ Орвел.[70] Са друге стране, велики број Европљана изражава бојазан да би се увођењем оваквих система идентификације полако, али сигурно, створила полицијска држава. [71] Ве-

[66] Ова спецификације се користи код биометријских пасоша, који су обрађени у одељку 3.2 наше студије.

[67] Council od the European Union, *15801/06,* Press Release, 2768th Council Meeting, Justice and Home Affairs. Документ је преузет са адресе: http://www.statewatch.org/news/2006/dec/jha-dec-prel.pdf.

[68] Council od the European Union, Directive …/…/EC Of the European Parliament and of the Council, *9010/1/06* , Press Release, Брисел, 18. септембар 2006. Документ је преузет са адресе: http://www.statewatch.org/news/2006/dec/eu-driving-licences-proposal-9010-rev1-06.pdf. – У вези са наведеним, погледати стр. 5 (тачка 17) и стр. 7 (тачка 2) документа.

[69] Louis Berney, нав. чланак, стр. 24.

[70] *BETR*, стр 111.

[71] Julian Ashbourn, нав. дело, стр. 13.

лики број грађана Европе се пита због чега је потребно толико мешање државе у њихов приватни живот, будући да су забринути због могућих последица које такав приступ може да носи, мада има и грађана који некритички верују да је то само због тероризма и организованог криминала. [72]

3.1.2.2 Земље Европске Уније без личних карата

У ЕУ неколико земаља уопште не познаје режим идентификационих докумената. Према нашим сазнањима, то су Данска и Ирска,[73] док их Летонија (Латвија) за сада нема, мада планира њихово увођење у неком виду.[74]

3.1.2.3 Земље Европе и Европске Уније са личним картама на добровољној основи

Постоји одређени број земаља како Европе, тако и Европске Уније које регулишу режим личне карте на добровољној основи. Постоји тренд да се за ту сврху уведу електронске личне карте, али најразвијеније земље још увек имају лична документа у папирном (тј. пластифицираном) облику. Такав је, примера ради, случај са Француском, која је детаљније обрађена у поглављу 3.1.2.5.

Неколико земаља ЕУ на добровољној основи издаје електронске личне карте, као што је случај са Шведском и нордијским земљама. Иначе, Нордијске земље имају концепт јединственог идентификационог броја и опционалних дигиталних сертификата за карте из приватног сектора (за банке, рецимо).[75] Шведска је крајем 2005. године представила национални идентификациони документ са биометријским подацима, која се добија на добровољној основи и може да се користи као валидан документ за путовања у оквиру Шенген зоне.[76] Специфичност шведског документа је што комбинује контактну и бесконтактну технологију на једном документу, [77] вероватно управо због потребе да се прилагоде машински читљивим путничким документима за путовање кроз Шенген зону, а који треба да буду бесконтактног типа (у случају да садрже опциони микрочип).

Норвешка такође издаје електронску личну карту за потребе e-banking-а, на добровољној основи и без биометријских података.[78]

---

[72] Исто, 17.

[73] LSE, *Research Status Report*, стр. 6.

[74] Privacy International & EPIC, *PHR Privacy and Human rights Report 2005*, стр. 450. Студија је преузета са адресе: http://www.privacyinternational.org/article.shtml?%20cmd[347]=x-347-542783&als[theme]=Privacy%20and%20Human%20Rights.

[75] Accenture Technology Labs, нав. дело, стр. 4.

[76] *LSEIP*, стр. 77.

[77] *FIDISD3.6*, „Overview on ID Documents in Europe“.

[78] Louis Berney, нав. чланак, стр. 24.

Финска на добровољној основи издаје електронске карте без биометријских података (тзв. *FINEID*), које садрже само електронски сертификат[79] и базиране су на PKI инфраструктури и сертификатима који се базирају на пару кључева и користе уз употребу PIN-а.[80] Занимљиво је да је у тој земљи само 10% грађана тражило имплементацију механизма за коришћење електронског потписа на својим картама, што говори о малој употреби истих за e-government.[81] То донекле чуди с обзиром да је Финска била прва земља Европе која је увела електронске карте,[82] али иако је већ шест година у употреби и мада омогућава разноврсне радње, за наведене потребе је користи тако мали проценат грађана.[83] Стога ова земља, уз Шведску, жели да повећа обим ових трансакција тако што ће електронске сертификате везати за стандардну опрему која долази уз мобилне телефоне (SIM карте).[84] Иначе, занимљиво је да се финска карта не користе за класичне потребе идентификације.[85]

У Италији постоји комбинација обавезујућег и необавезујућег режима. Биометријски отисци за централни регистар узимају се на добровољној основи,[86] због чега готово нико од грађана не даје отиске прстију.[87] Обавезни режим личних карти је увео Мусолини 30-тих година 20. века, али су се отисци прстију одувек у свести грађана повезивали само са криминалцима и њиховим досијеима.[88] За небиометријске електронске карте не постоји централна база података већ су сви подаци складиштени на самој карти.[89] Грађани Италије користе више различитих електронских карти које нису личне нити су обавезујуће.[90]

---

[79] EDRI, „French minister demands compulsory biometric ID“, EDRI-gram 3.8. Прилог је преузет са адресе: http://www.edri.org/edrigram/number3.8/ID. – Финска карта има само информације о носиоцу, без икаквих биометријских података.

[80] *FIDISD3.6*, стр. 30. – Јавни кључеви код *FINEID*-а су складиштени у тзв. отвореном директоријуму где су јавно доступни, док је приватни кључ само на карти и може бити активиран искључиво PIN кодом. Три погрешно укуцана PIN кода аутоматски закључавају карту. PKI може бити одрађен између било које две тачке и нема потребе за трасфером идентификационих података у централни систем. Од личних података на карти су само име и презиме и јединствени електронски идентификатор. На картици не постоји адреса, јединствени матични лични број, датум рођења нити било шта слично. Као део сертификата на карти може се убацити и електронска пошта имаоца. Карта може бити блокирана у сваком тренутку, на захтев имаоца.

[81] Dan Balaban, нав. чланак, стр. 32.

[82] *FIDISD3.6*, „Overview on ID Documents in Europe“.

[83] Исто, 30. – У те радње спадају електронско попуњавање формулара, провера личних података, пореских података и слично. За те потребе је користи само око сто хиљада од око пет милиона становника

[84] Dan Balaban, нав. чланак, стр. 34.

[85] *FIDISD3.6*, нав. одељак.

[86] EDRI, „French minister demands compulsory biometric ID“.

[87] *LSEIP*, стр. 74.

[88] Исто, 73.

[89] *MBID*, стр. 122.

[90] Dan Balaban, нав. чланак, стр. 34.

Аустрија је одмах после Финске увела електронску карту која се користи и за e-government, али такође нема биометријске податке.[91] Аустријска електронска карта (*Bürger-karte*) није званичан идентификациони национални документ (нема фацијалну информацију), није у обавезујућем виду нити је подобна као документ који може да се користи за путовање по Европи.[92] Ово решење не користи биометријске податке, али има централну базу небиометријских података грађана.[93] Ово решење у пракси показује исте слабости као и финско – свега један проценат целокупне популације Аустрије користи погодности електронског потписа помоћу овог документа.[94]

Веома је занимљив случај Мађарске, која је већ 1991. године на нивоу Уставног суда променила дотадашњи концепт централног регистра, који је жестоко прокритикован.[95] У Мађарској је од тада употреба вишенаменског јединственог идентификационог броја (преко кога је скупљан огроман број података) проглашена неуставним, забрањено је коришћење у наведеном смислу и строго нормирана будућа употреба.[96]

Сличан је и случај Португала, који уводи биометријске личне карте,[97] али без јединственог идентификационог броја, с обзиром да би то било у колизији са позитивним законодавством те земље (у Португалу члан 35. Устава забрањује увођење јединствених националних бројева).[98]

У Швајцарској се још увек разматрају будућа решења. Швајцарски стручњаци позивају на један озбиљан начин разматрања проблематике биометријских личних карти, пре свега по питању проблема централне базе биометријских података и могућности формирања алтернативног модела. [99]

3.1.2.4 Земље Европе и Европске Уније са личним картама на обавезујућој основи

Белгија, Немачка, Грчка и Шпанија су земље ЕУ које су од самог почетка имале режим обавезних личних карата, али са различитим решењима.[100]

---

[91] *BETR,* стр. 55.

[92] Herbert Leitold, „European Electronic Identity Practices, Country Update of Austria“, излагање на Porvoo9 скупу. Сиже презентације је преузет са адресе: http://porvoo9.gov.si/pdf/THU_11a_1400_Country_update_Austria.pdf.

[93] *FIDISD3.6*, стр. 31. – И поред тога, због добро спроведене процедуре заштите података, ово решење је имало добар пријем код грађанских органихзација које се боре за приватност.

[94] Исто.

[95] *LSEIP*, стр. 73.

[96] Privacy International & EPIC, нав. студија, стр. 377.

[97] *BETR*, стр. 97.

[98] Privacy International & EPIC, нав. студија, стр. 577.

[99] *MBID*, стр. 128.

[100] То је подвучено у сведочењима пред британским парламентом, под називом *Examination of*

Грчка их поседује у папирном облику без икакве електронике и биометријских података у електронском облику.[101]

Белгијско решење (*BELPIC*) је у електронског типа, али без биометрије (тачније без отисака прстију).[102] Основни циљ белгијског документа је био у афирмацији електронске управе, али га дан-данас за те потребе користи веома мали број људи из једног простог разлога – недовољног броја читачâ smart картица повезаних на PC рачунаре.[103] Сертификационо тело је власништву поште и једне фирме.[104] Белгијско решење је доживело велики број критика, пре свега из аспекта приватности, везано за могућност укрштања различитих база података (због употребе *RRN* јединственог броја када год је карта коришћена у било које сврхе) и због чињенице да ималац карте није могао да контролише опсег информација које би му одређена организација узимала.[105] Смернице за следећу генерацију Белгијских smart карти које је урадио конзорцијум истраживача и индустријских предстваника Фландрије предвиђају да ималац карте даје најмањи могући број података организацијама са којима ступа у интеракцију, те да сваки грађанин пред различитим организацијама буде видљив под различитим псеудонимом. То би онемогућило упоредно укрштање база података и омогућило анонимност у свим случајевима где прецизна идентификација није потребна и где је довољна проста аутентификација.[106] Занимљиво је да код белгијског решења грађанин у сваком тренутку може деактивирати чип на својој карти.[107]

У Шпанији, у којој су личне карте уведене ради контроле имиграције за време режима генерала Франка,[108] однедавно у оквиру тзв. *DNIE* пројекта почиње издавање биометријских личних карата и то кроз приметно јаку медијску кампању.[109]

Witnesses, Questions 60 – 79. Сведочења су преузета са адресе: http://www.publications.parliament.uk/pa/cm200304/cmselect/cmhaff/130/3121105.htm.

[101] Privacy International & EPIC, нав. студија, стр. 356.

[102] EDRI, „French minister demands compulsory biometric ID“. – У Белгији, рецимо, електронска лична карта ће бити обавезна до краја 2006, али још увек без конкретних планова о увођењу биометријских података. До сада је у Белгији издато око 3 милиона картица (од укупно 10,5 милиона становника). Више о белгијској карти на: http://eid.belgium.be.

[103] Dan Balaban, нав. чланак, стр. 33.

[104] *Certipost* – предузеће је у власништву Поште Белгије и фирме Belgacom (*De Post*). Више детаља на адреси: http://www.certipost.be.

[105] Stefan Brands, „The problem with the Belgian eID card“, The Identity Corner, 7. 4. 2005. Чланак је преузет са адресе: http://www.idcorner.org/?p=121.

[106] IDABC, „Flemish project addresses privacy shortcomings of Belgian e-ID card“, 12. 10. 2005. Извештај је преузет са адресе: http://ec.europa.eu/idabc/en/document/4983/332.

[107] На округлом столу „Elektronski identitet u e-Upravi i zaštita privatnosti“ ово је истакао професор Дени де Кок (Danny De Cock), један од аутора пројекта BELPIC.

[108] *LSEIP*, стр 76.

[109] EBP, „eID card is launched in Spain“, 20. 03. 2006. Вест је преузета са адресе: http://www.

Холандија ће у новим документима узимати биометријске податке и то на обавезујућој основи, мада се још увек се не зна прецизан опсег биометрије која ће се узимати од грађана.[110]

Естонија издаје обавезне електронске личне карте, али без биометријских података,[111] уз издавање дигиталног сертификата за обављање електронских трансакција са управом, које корисник може деактивирати на свој захтев. Сертификационо тело у овој земљи је формирано од две банке и два телеком оператера.[112] Занимљиво је да естонске карте омогућавају и електронско гласање, али да је на последњим изборима само 2% грађана Естоније са правом гласа искористило ту могућност,[113] иако је највећи број грађана Естоније добио ову карту.[114]

И остале земље ЕУ које издају личне карте на обавезној основи се налазе негде између ова четири модела: папирних, пластифицираних, електронских без биометрије и електронских са биометријом.

Некадашње југословенске републике имају различита решења за овај документ.

Словенија има обичну пластифицирану личну карту са вишим нивоом заштите, а имплементирала је велики број e-government апликација. Приметно је да Словенија и напредне земље у окружењу не стављају нагласак на биометријске личне карте, већ на биометријске пасоше,[115] због условљавања САД визним режимом.[116] Мада не поседује електронске (биометријске) личне карте, ова земља има прилично добро развијен систем електронске управе.[117] То је један од очигледних показатеља да постојање електронске, а још мање биометријске карте, није никакав condicio sine qua non за модернизовање управе.

---

europeanbiometrics.info/news/newsdetail.php?Id_news=132.

[110] EDRI, „French minister demands compulsory biometric ID“.

[111] ID, „ID Card“. Информације преузете са адресе http://www.id.ee/pages.php/030301.

[112] Certification Centre (*Sertifitseerimiskeskus*), на адреси www.sk.ee.

[113] Dan Balaban, нав. чланак, стр. 30. – Укупно 9300 од 800 000 грађана са правом гласа.

[114] „ID Card Issuing Statistics“. Статистика је преузета са http://www.id.ee/pages.php/03030102 – Милион становника од око 1,35 милиона укупног становништва.

[115] EDRI, „New biometric passports in Slovenia, као и Passports with biometrics for Romanians“. Вест преузета са адресе: http://www.edri.org/edrigram/number4.9/passports. – Словенија, Аустрија и Румунија су очигледан пример.

[116] Mikro, „SAD odložile uvodjenje biometrijskih pasoša“, 16. 05. 2005. Вест је преузета са адресе: http://www.mikro.co.yu/ser/vesti/vesti.php?datum=2005-06-16&ID=7140.

[117] Dušan Kričej, „E-Governmentin Slovenia, Bestpractice“; Anka Bolka, „Slovenia's eID good practice cases, Health Insurance Card System - Status and Challenges“, излагање на Porvo9 скупу, чија се скраћена презентација може преузети са адресе: http://porvoo9.gov.si/pdf/THU_01_0915_DKricej_Porvoo9.pdf.

Хрватска је увела обичне пластифициране картице вишег нивоа заштите са машински читљивом зоном,[118] слично Словенији,[119] дакле без микрочипа и биометрије. Занимљиво је да на обрасцу хрватске личне карте не фигурира ЈМБГ, што је решење које је веома битно за приватност грађана, с обзиром да им тај број више не може узимати свака инстанца (банке, рецимо) и да је отежана могућност евентуалног укрштања разнородних база.

Од балканских земаља ниједна нема биометријске електронске личне карте, осим БиХ у одређеном виду, чија лична карте у себи агрегира биометријске податке који су кодирани у баркоду и на самој површини карте, али такође без микроконтролера.[120] Такво решење, које се ослања на централни регистар, OHR је увео због специфичних услова у овом протекторату, што се види из званичних саопштења ове институције.[121] Међутим, ни то решење није спречило манипулације око држављанства, јер је било случајева да су неке од особа које су осуђење за тероризам у свету имале ову електронску карту, сасвим прописно издату у босанском МУП-у.[122] У овој земљи се после увођења овог система посебна пажња поклања заштити података.[123]

Дакле, оно што је заједнично за различита решења Словеније, Хрватске и Бих је да на својим модернизованим личним картама немају микрочип.

3.1.2.5 Студија случаја: Француска и Немачка

Француска и Немачка разрађују концепт *European Citizen Card*, који би могао постати нека врста незваничног стандарда у смислу интероперабил-

---

[118] Погледати члан 7, став 3, *Закона о особној исказници* на сајту хрватског МУП-а на адреси: http://www.mup.hr/91.aspx.

[119] Погледати *Zakon o osebni izkaznici* на сајту словеначком парламента, на адреси: http://www.uradni-list.si/1/ulonline.jsp?urlid=2005100&dhid=78815.

[120] OHR Political Department, „BiH Citizen Identity Card“. Текст обраћање за јавност је преузет са адресе: http://www.ohr.int/ohr-dept/pol/spu/lprojects/default.asp?content_id=5844.

[121] SFOR, „Transcript - Press Conference“, 25. 2. 2002, Coalition Press Information Center. Транскрипт конференције за штампу је преузет са адресе: http://www.nato.int/sfor/trans/2003/t030225a.htm. –У саопштењу се наводе следећи разлози за увођење овог система: борба против криминала и креирања лажних докумената, борба против лажирања идентитета зарад коришћења пензионог система и бенефиција за ветеране рата, сузбијање нелегалног власништва над имовином што спречава повратак избеглица, уређење пореског система и потреба да се ЕУ убеди да БиХ може ефикасно да контролише своју границу.

[122] Nataša Krsman, „Siniša Macan: Pooštrićemo mjere zaštite ličnih podataka“, *Nezavisne novine*, 03. 06. 2006. Интервју преузет са адресе: http://www.nezavisne.com/revija/tekst060604-01.php.

[123] Исто. – У овом интервјуу, Синиша Мацан, директор Дирекције за имплементацију пројекта заштите личних података грађана (CIPS), на питање које све институције имају право да затраже податке од CIPS-а каже: „Све институције које прођу одговарајућу процедуру код Комисије за заштиту личних података. То подразумијева да се прво региструју као корисник, а Комисија за заштиту личних података има своју процедуру која подразумијева да провјере који је њихов правни основ за тражење података... Када докажу комисији да су у стању технички да чувају те податке, комисија то све повјерава и потом их региструју као корисника и иде налог у CIPS. ...ако се неки податак злоупотријеби ми имамо механизме да докажемо ко је то и како учинио.“

ности различитих имплементација електронских (личних) карти.[124] Осим тога, у развоју планова за такав модел треба да буду и заједнички усвојени технички стандарди безбедности.[125] У сваком случају, ако једног дана стандард буде заживео он *неће* бити обавезујући за национална законодавства (с обзиром да питање националног идентификационог документа спада искључиво под њихову јурисдикцију), али ће бити препознато као валидно на нивоу земаља чланица ЕУ.[126] Веома је битно истаћи да, према овом плану, *уколико* карте неке земље садрже биометријске податке (дакле, то није условљавајући фактор), они треба да буду компатибилни ISO/IEC *7816–11* стандарду, тј. форми 1:1 идентификације (без централне базе података).[127]

У Француској су личне карте су уведене за време колаборационистичког Вишијевог режима. Франсоа Митеран је 1981. године био против електронских личних карти, говорећи да оне значе ускраћивање грађанских права, а да Француска као земља слободе не може да их прими. У овој земљи за сада постоје само обичне папирне личне карте, пластифициране, које нису обавезне и држава их још увек издаје са важењем од десет година.[128]

У последњих неколико година појавиле су се две различите платформе за увођење новог типа идентификационих докумената у овој земљи. Једна је предложена од стране Министарства за државну реформу, а друга од стране Министарства унутрашњих послова и разликују се пре свега по питању концепта позадинске базе података.[129] Наиме, Министарство унутрашњих послова је захтевало централни регистар за тзв. INES пројекат, док је Министарство државне реформе предложило децентрализацију података и дистрибуиране идентификаторе.[130] Министарство унутрашњих послова је свој предлог дало на јавну дебату и он је жестоко прокритикован од релевантних и стручних институција.[131] Неколико великих организација је

---

[124] Dan Balaban, нав. чланак, стр. 34.

[125] Lorenzo Gaston, „CEN/TS 15480 standard European Citizen Card Progress“, излагање на конференцији Porvo9, чија се скраћена верзија може преузети са адресе: http://porvoo9.gov.si/pdf/fri_14_0930_LGaston_eccmay_12.pdf.

[126] Исто.

[127] Jan van Arkel, „Common requirements for (global) interoperable eID“, излагање на конференцији Porvo9. Скраћена верзија излагања може се преузети са адресе: http://porvoo9.gov.si/pdf/FRI_17_1130_JvanArkel_Porvoo9.pdf.

[128] Облик (пластификација) и рок важења (десет година) је потврђен и од стране Драгана Спасића, једног од учесника на округлом столу „Elektronski identitet u e-Upravi i zaštita privatnosti“.

[129] *LSEIP*, стр. 67.

[130] Исто, стр. 69.

[131] Privacy International, „French report highly critical of new French ID Card project“. Извештај је преузет са адресе: http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-247752&als[theme]=ID%20Around%20the%20World. – Предлог владе под кодним именом INES је критиковали су и Национална комисија за информатику и права грађана (*Commission nationale de l'informatique et des libertés*) и Форум за грађанске слободе на Интернету (*Le Forum des droits sur l'internet*).

покренуло кампању против тог предлога због најаве централне базе биометријских података.[132] Министар унутрашњих послова, Никола Саркози, је због ових критика јавности на рачун INES пројекта, изјавио да треба још промислити и да је питање биометријских личних карти различито од питања биометријских пасоша, који је далеко важнија тема за земље ЕУ.[133] Ово показује да је Француска класичан пример друштва у коме је иницијатива невладиног сектора који се бори за право на приватност успорила пребрзо доношење биометријског решења за личне карте.[134]

У сваком случају, за свој нови систем који ће се вероватно заснивати на биометријској идентификацији Француска се залаже да остане на добровољној основи, као и досадашње решење.[135] Влада планира се да се са пројектом почне не пре 2008. године, да документ служи и као путна исправа у Европи, а да не садржи информације о социјалном и здравственом осигурању.[136]

Немачка има папирна пластифицирана документа која намерава да замени електронским, али још увек без потпуно дефинисаног решења.[137] Ова земља је, са друге стране, већу пажњу посветила развијању биометријских пасоша.[138] Уставна забрана формирања централног регистра се у овој земљи очигледно покушава заобићи мекшим путем, јер је већ прошла легислатива по којој ће се формирати антитерористичка централна база,[139] централна база школских података,[140] као и да ће од јула 2007. сваки становник добити јединствени порески број,[141] што је основа за индексирање још једне базе. Приметни су страхови мислећих грађана да је то први корак који води ка успостављању сложеног режима прикупљања података.[142] Постоје чак и озбиљни коментари да је Немачка на прекретници, те да је битно одредити нове границе између грађанских права и слобода и опште безбедности.[143]

---

[132] EDRI, „French campaign against biometric ID card“, EDRI-gram 3.11, 02. 06. 2005. Вест је преузета са адресе: http://www.edri.org/edrigram/number3.11/biometrics.

[133] *BETR*, стр. 77.

[134] Dan Balaban, нав. чланак, стр. 35.

[135] LSE, *Research Status Report*, стр. 5.

[136] Fabrice Mattatia, „European Electronic Identity Practices, Country Update of FRANCE“, излагање на конференцији Porvo9. Сиже излагања је преузет са адресе: http://porvoo9.gov.si/pdf/THU_11d_Country_update_France.pdf.

[137] EDRI, „French minister demands compulsory biometric ID“.

[138] Mikro, „Nemačka usvojila plan o biometrijskim pasošima“, 25. 07. 2005. Вест је преузета са адресе: http://www.mikro.co.yu/ser/vesti/vesti.php?datum=2005-07-25&ID=7234.

[139] Mile Lasić, „Verska pripadnost kao znak terorista“, Danas, 8. септембар 2006. Текст је преузет са адресе: http://www.danas.co.yu/20060908/evropa1.html.

[140] EDRI, „Privacy Commissioners act together“, *EDRI-gram4.21*, 8. 11. 2006. Вест је преузета са адресе: http://www.edri.org/edrigram/number4.21/privacy.

[141] Heise online, „Bundesrat gives the green light to identity number“, 07. 11. 2006. Вест је преузета са адресе: http://www.heise.de/english/newsticker/news/80622.

[142] Исто.

[143] Политика, „Жигосање сумњивих“, 13. 09.2006, стр. 4.

Иначе, немачки концепт неидентификационих електронских карти се ослања на једнонаменске електронске карте за различите потребе (секторске smart карте за здравство и социјално осигурање), што је по приватност грађана далеко боље решење од вишенаменског концепта.[144]

Аналитички приступ показује да Француска и Немачка покушавају да ускладе свој идентификациони национални систем, који би касније можда покушале да наметну као ЕУ стандард,[145] иако је то правно гледано немогуће (с обзиром да је то одувек било питање које су решавала национална законодавства).[146] Занимљиво је да су им тренутни планови режимски различити, јер Француска планира бесконтактни документ на добровољној бази (пре свега за потребе путовања и e-government апликација), док немачки план оквирно предвиђа бесконтактне карте на обавезујућој основи,[147] што говори да ће питање режима (обавезујући/необавезујући) бити решавано одвојено.

3.1.3 Стање у европским земљама са већински православним становништвом

Ниједна од земаља са већински православним становништвом нема ни обавезне ни опционе биометријске личне карте. Током деведесетих година предложени пројекат електронских карти у Грчкој је дочекан са великим негодовањем грађана, што је био повод за масовне протесте које је предводила Црква, због чега је влада повукла предлог.[148] У Русији постоје неки концепти електронских карти (попут тзв. „Картице Московљанина“), али они су на добровољној основи и не представљају државни идентификациони документ. У Русији и Украјини постоји приличан отклон грађана пре-

---

[144] *FIDISD3.6*, „Overview on ID Documents in Europe“.

[145] *BETR* стр. 62.

[146] На округлом столу „Elektronski identitet u e-Upravi i zaštita privatnosti“ говорник из ПТТ Србија, мр Драган Спасић, је навео да од прве четири фирме у свету по броју произведених и продатих smart картица, три су из Француске (*GemPlus*, *Axalto* (sada *Gemalto*) и *Oberthur*), а једна из Немачке (*Giesecke & Devrient* (G&D)). Он је поставио питање зашто Француска и Немачка као најнапредније државе у области smart картица од којих се праве електронске личне карте нису увеле електронске личне карте за своје грађане. Према његовом излагању и презентацији „The European Citizen Card (ECC) - Challenges for Interoperability and Security“ (autora Michael Bauera iz firme G&D) са конференције у оквиру које је одржан поменути округли сто, фирме из Француске и Немачке раде на усвајању заједничког стандардна „CEN / TC 224 / WG 15 (*European citizen card*)“ и док га не усагласе неће уводити електронске личне карте. На сугестију да би у том случају у неком догледном времену Француска и Немачка могле да наметну свој стандард за електронске личне карте осталим земљама ЕУ (зарад интероперабилности, рецимо), Дени де Кок, један од аутора пројекта BELPIC (*Belgian Electronic ID Card Project*), је рекао да не постоји ниједно наддржавно тело које националном законодавству може наметнути решење личне карте.

[147] Према у претходној фусноти наведеној презентацији M. Bauer-a, под називом „The European Citizen Card (ECC) - Challenges for Interoperability and Security“.

[148] *Жички Благовесник (Хроника најављеног слободоубиства)*, одељак „Гласови помесних цркава“, Епархија жичка, јул 2006, стр. 4.

ма покушају увођења електронских личних карата, према централном регистру и идентификационом бројевима као супституенту имена и презимена у друштвеним процесима.[149] Са друге стране, Бугарска најављује план да ускоро представи биометријски лични документ којим ће њени грађани, према речима службеникâ владе, моћи слободно да путују по Европи.[150]

У земљама са већински православним становништвом далеко је актуелнија израда биометријских пасоша,[151] због визног услова САД, што је потпуно одвојено питање од биометријских личних карти. Тако Грчка, рецимо, нема планове за увођење електронских личних карти,[152] иако је кренула са пројектом израде биометријских пасоша за своје грађане.

Поводом питања електронских и биометријских докумената, на захтев верника и свештенства реаговало је неколико Синода помесних православних цркава,[153] од којих се по прецизности саопштења издваја став Синода Руске православне цркве (Московске патријаршије), поводом планирања неких суседних земаља да уведу биометријске идентификационе карте.[154] Синоди су реаговали како због очувања права на приватност и угрожавања безбедности грађана, а тако и због чињенице да је верујући народ забринут због конотација са тоталитарним режимом најављеним у *Јовановом Откровењу*,[155] што уноси немир не само међу православне хришћане, већ и међу припаднике осталих хришћанских деноминација.[156]

По истом питању је реаговала и СПЦ, што ће бити детаљно обрађено у четвртом одељку, који се бави случајем биометријских система идентификације у Републици Србији и њиховим импликацијама на друштвени живот.

---

[149] Исто. – У Русији и Украјини верници Православне цркве су се чак добили и право да не користе ИНН број (попут ПИБ-а у Србији), већ да се запотребе плаћања пореза користи сопствено име.

[150] Southeast European Times, „Nove bugarske lične karte polovinom 2007. godine“, 13. 11. 2006. Вест је преузета са адресе: http://www.setimes.com/cocoon/setimes/xhtml/sr_Latn/newsbriefs/setimes/newsbriefs/2006/11/13/nb-05.

[151] Такав је пример Румуније. Погледати EDRI извештај, „Passports with biometrics for Romanians“, на адреси: http://www.edri.org/edrigram/number4.9/passports.

[152] *FIDISD3.6*, „Overview on ID Documents in Europe“.

[153] *Жички Благовесник*, нав. одељак – Реаговали су синоди Руске, Грчке и Украјинске православне цркве (Московске патријаршије), као и Протат Свете горе Атонске.

[154] Руски Синод у свом саопштењу наглашава да у евиденцији људи помоћу информационих технологија од стране државне инстанце нема ничег лошег, али да биометријски систем идентификације доноси неке опасности, због чега се тражи могућност алтернативе и слободног избора. Инсистира се на прецизној законској регулативи по том питању, а било какав вид поткожних биочипова се у потпуности одбацује као неприхватљив. У изјави се такође позива верујући народ да прихватање или неприхаватње оваквих докумената *не смеју* користити за одбацивање људи као недостојних или пак сејање раскола у Цркви. За детаљнији увид погледати текст под називом *Систем електронске идентификације људи*, објављен у *Православљу* бр. 939. У питању је превод текста преузетог са званичног сајта Московске патријаршије (www.patriarhija.ru).

[155] Жички Благовесник, нав. одељак.

[156] Исто.

3.1.4 Стање у осталим земљама света

Неколико земаља у остатку света је имплементирало основне електронске, а неколико биометријске личне карте на националном нивоу. Углавном су предњачиле далекоисточне земље попут Малезије,[157] која је међу првима увела национални биометријски систем идентификације грађана,[158] а затим Сингапур[159] и Тајланд[160]. Наведене земље имају тзв. вишенаменске карте, јер помоћу једног документа ималац обавља више радњи и трансакција,[161] што је једна од кључних замерки организација које се боре за приватност грађана.[162] Јужна Кореја је такође међу првима развила вишенаменски биометријски идентификациони документ са чипом,[163] али су по питању централизованог рачунарског система за идентификацију грађана у тој земљи реаговале неке НВО, што је довело до преиспитивања целог система.[164]

У Хонг Конгу постоје биометријске smart електронске карте, али без централне базе података,[165] док у целој Кини не постоје биометријске личне карте за националну идентификацију грађана. Постоје само smart карте без биометрије (за сада на нивоу Шангаја), које грађани користе на добровољној основи за разне електронске услуге.[166] Кина додуше ускоро уводи електронске карте за потребе идентификације грађана које ће бити бесконтактног типа и неће садржати биометријске податке.[167] НР Кина је резервисана према коришћењу биометријских идентификатора и централне базе биоме-

---

[157] Privacy International, *PHR2004 report: Malaysia.* Студија је преузета са адресе: http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-83539.

[158] Leo Benedictus, „A brief history of the passport“, *The Guardian*, 17. 10. 2006. Текст је преузет са адресе: http://travel.guardian.co.uk/article/2006/nov/17/travelnews.

[159] AFP, „ID Card 2005 – Resources: Elsewhere in the World“.

[160] SecureIDNews, „Thailand introduces national ID with biometric technology“, 15. 04. 2005. Вест је преузета са адресе: http://www.secureidnews.com/weblog/2005/04/15/thailand-introduces-national-id-with-biometric-technology/.

[161] Примера ради, у Тајланду, Малезији и Макау поред идентификационог документа оне представљају и возачку дозволу, а користе се и за друге секторе (здравствени, социјално осигурање итд.). Такво решење у Европи је приметно само у Белгији. Погледати табелу код Louis Berney, нав. чланак, на стр. 24.

[162] У до сада највећој светској студији из области приватности и људских права (1200 страна А4 формата, око 6000 фуснота), публиковане почетком новембра месеца 2006. године под називом *PHR Privacy and Human rights Report 2005* организације EPIC и Privacy International су Малезију, Сингапур и Тајланд поставили на последња места комплетне листе, великим делом због начина идентификације грађана и недостатка елементарне приватности.

[163] Roger Clarke, „Chip-Based ID: Promise and Peril“.

[164] APF, „The Korean National Education Information Systems (NEIS)“. Чланак је преузет са адресе:http://www.privacy.org.au/Campaigns/KoreaNEIS/.

[165] *LSEIP*, стр. 59.

[166] Privacy International, *PHR2004 - People's Republic of China,* 16. 11. 2004. Студија је преузета са адресе: http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-83511.

[167] Louis Berney, нав. чланак, стр. 24.

тријских података, пошто је закључено да они немају довољну поузданост на огромним популацијама,[168] што значи да их неће бити ни у пројекту тог будућег документа који је у разради.

Биометријски вид идентификације је веома популаран у земљама са малобројном популацијом,[169] какве су Брунеји и Макао,[170] Ел Салвадор,[171] Мауританија,[172] што је логично с обзиром да на малом броју показују мањи проценат грешке приликом обраде података у бази. Сасвим је могуће да преко тих земаља велики произвођачи опреме за биометријски идентификацију желе да сломе потенцијални отпор у већим државама.

На Блиском истоку ситуација је разнолика. Постоје земље, попут Ирана, које поседују обичне идентификационе карте са машински читљивом зоном.[173] Султанат Омана издаје биометријске личне карте и унапређује их за e-government, као прво решење тог типа у региону.[174] Катар и Саудијска Арабија такође имају биометријске личне карте,[175] док Мароко намерава да уведе бесконтактни биометријски систем са централном базом биометријских података повезаном са AFIS системом.[176] Међу земљама које су увеле вишенаменски електронски документ, налазе се Бахреин и Израел.[177] За земље Блиског истока је карактеристично да готово не постоји реакција јавности на увођење биометријских личних карти.[178]

Индија се спрема да уведе електронске личне карте и већ у првој фази најављује мултифункционалну употребу, уз директно укрштање база података,[179] што би омогућило лако профилисање грађана, због чега је дошло до зебње у мислећим круговима. Међутим, у овој земљи тај пројекат се одвија

---

[168] *LSEIP*, стр. 58.

[169] Louis Berney, нав. чланак, стр. 24. – Пројектовани број корисника у Брунејима је 400 хиљада, а у Макау 460 хиљада људи.

[170] Исто.

[171] *NICC*, стр. 35.

[172] Исто. 40.

[173] Исто, 38.

[174] EBP, „Gemalto develops the first smart card-based e-government solution ever in the Middle East“, 21. 09. 2006. Вест је преузета са адресе: http://www.europeanbiometrics.info/news/newsdetail.php?Id_news=269. – Султанат Оман је иначе прва земља на Блиском истоку која је имплементирала *smart* биометријске карте на националном нивоу.

[175] Louis Berney, нав. чланак, стр. 23.

[176] EBP , „New ID Biometrics in Morocco“, 05. 10. 2005. Вест је преузета са адресе: http://www.europeanbiometrics.info/news/newsdetail.php?Id_news=28.

[177] Louis Berney, нав. чланак, стр. 24. – Бахреин их користи и у здравственом сектору и као возачке дозволе, док их Израел користи за контролу границе и генерисање електронског потписа.

[178] Исто, 23.

[179] Ти планови се виде из докумената које влада даје на свом сајту. Погледати PowerPoint презентацију владе Индије на адреси: http://www.mit.gov.in/plan/ppt/national%20ID.ppt.

изузетно споро.[180] Њен историјски ривал, Пакистан, већ има smart карте које поред биометрије агрегирају огроман број додатних података, у обиму готово невиђеном у остатку света.[181]

3.1.4.1 Студија случаја: Јапан и Тајван

У Јапану не постоје биометријске личне карте. Такозвани *JukiNet* електронски идентификациони систем (бесконтактни чип садржи само основне податке без биометрије) који је на добровољној бази већ је проглашен неуставним у оквиру једне префектуре.[182] *JukiNet* је иначе прилично хладно примљен од грађана, па чак и од градских власти у неким случајевима,[183] а његова сигурност је у великој мери оспорена.[184] У Јапану тек треба да се води дебата око увођења националног електронског документа, по питању начина имплементације и количине података које ће он агрегирати (тренутни предлози не обухватају биометријске податке попут отиска прста).[185]

На Тајвану је прикупљање отисака прстију обичних грађана имало судски епилог. Потпредседница Тајвана Анета Лу је маја 2005. године покренула кампању против прикупљања отисака прстију обичних грађана, са образложењем да то није фактор у решавању криминалних случајева, наводећи уз то да је формирање централне базе биометријских отисака осетљиво на криминалне упаде.[186] Иницијативи се придружило око стотину организација које се боре за људска права, да би цео спор епилог добио на Врховном суду, који је стварање базе биометријских отисака ставио привремено ван снаге, јер уколико би пројекат био евентуално проглашен неуставним, велики ресурси би били узалуд потрошени.[187] Пројекат стварања националне ба-

---

[180] Louis Berney, нав. чланак, стр. 25. – Чак и после две трећине потрошених средстава и пет година од објаве овог система, пројекат још увек није стартовао.

[181] *NICC*, стр. 42.

[182] Суд Ишикава (*Ishikawa*) префектуре је 30. 05. 2005. прогласио неуставним пројекат *JukiNet* пројекат којим су скупљане информације о грађанима, са образложењем да исти није у складу са 13. чланом Устава те земље и да се њиме нарушава приватност грађана. У судском спору је пресуђено да овај систем не може бити на обавезној основи и да се информације о грађанима који су уложили жалбу избришу из система. Локалне власти Јокохаме (*Yokohama*) су чак и пре тога одбијале да региструју 3 милиона својих грађана, да би касније сугерисали грађанима да не користе систем. Више о томе у *LSEIP*, стр. 59 и извештај: Privacy International report, „Japanese Court Rules ID System Unconstitutional". Извештај је преузет са адресе: http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-228843&als[theme]=ID%20Around%20the%20World.

[183] *LSEIP*, стр. 59.

[184] Исто, 94.

[185] Prof. Nagaaki Ohyama, „New e-Japan strategy and unified eI Dunder discussion", излагање на Porvoo9 конференцији. Сиже је преузет са адресе: http://porvoo9.gov.si/pdf/THU_08_1130_NOhyama_nicss_Porvoo9.pdf.

[186] *LSEIP*, стр. 63.

[187] Исто, стр. 64.

зе отисака прстију у овој земљи биће стопиран све док се не одреди његова сврсисходност и законитост.[188]

3.1.5 Биометријске личне карте – сумарни закључак

Невелик број земаља у свету увео је биометријске електронске личне карте. Најразвијеније земље света их за сада углавном немају, чак ни на добровољној основи, осим евентуално у секторском погледу. На Западу се невладин сектор (који се бори за грађанско право на приватност) и академске институције противе њиховом увођењу, сматрајући да оне повећавају моћ полицијског апарата и омогућавају размену података између различитих агенција. Структуре власти правдају увођење таквог режима идентификације углавном борбом против тероризма и системом отпорним на фалсификовање докумената, а све чешће и потребом унапређења управе. Политичке елите западних земаља, схватајући непопуларност биометријских система идентификације, покушавају да их уведу на заобилазне начине, користећи разне необавезујуће препоруке и кампање. Међутим, без отпора јавности овакви пројекти пролазе само у блискоисточним и неким далекоисточним земљама познатим по ограниченим грађанским слободама.

Земље западне демократије (а посебно оне које припадају систему обичајног права) које планирају увођење биометријских личних карти се суочавају са великим притиском јавности, мислећих грађана, академских институција и организација за људска права, тако да њихово увођење у најмању руку није извесно. Европске земље које поседују електронске личне карте својим грађанима углавном не узимају биометријске податке и у великом броју случајева их издају на добровољној основи.

У слободном свету постоји неколико случајева у којима су слични пројекти одбијени, било због реакција јавности или одлука надлежних судова.

3.2 Биометријски пасоши

У Европи и свету је далеко већа проблематика увођење биометријских пасоша, због захтева САД о којима ће бити речи у наредној глави. Битно је нагласити да су биометријски пасоши и биометријске личне карте и теоријски и практично два различита пројекта (једно је национални идентификациони документ, док је друго путничка исправа која се користи на међународном нивоу) и да их као такве треба и посматрати.

Идеја за стварање биометријских пасоша је постала актуелна после доношења тзв. *Patriot Act*-а од стране америчког Конгреса. Доношење тог до-

[188] Privacy International, „Taiwan Constitutional Court places fingerprinting plan on hold“, 22. 06. 2005. Извештај је преузет са адресе: http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-249615.

кумента директно је иницирано догађајима који су се десили 11. септембра 2001. године. *USA Patriot Act* је потписан 26. октобра 2001. године од стране председника Буша, после брзог и готово анонимног пролаза кроз оба дома Конгреса.[189]

Терористички напади који су се тада десили и одговор америчке администрације били су кључни притисак на ICAO (*International Civil Aviation Organization* – Међународна организација за цивилно ваздухопловство), организацију УН која је задужена за доношење сигурносних и осталих стандарда за пасоше, за доношење новог стандарда.[190]

3.2.1 Настанак и пропозиције ICAO 9303 стандарда

ICAO је све до 2003. године држала став да је што се биометрије тиче потребан и довољан услов агрегирање дигиталне фотографије имаоца пасоша (из једне, фронталне перспективе, са могућношћу скенирања обичне слике без икаквих мерења, што не спада у биометрију у ужем смислу). Међутим, те године је дала препоруку да земље чланице *могу* (а не морају – *прим.*) користити и биометријске идентификаторе попут отиска прста.[191] Постоји више разлога за одлуку да се биометријски отисци прстију не траже ултимативно. Један од техничких разлога је и чињеница да различити произвођачи опреме за биометријску идентификацију имплементирају различите алгоритме за препознавање отиска, што значи да је вероватно да пасоши не би били интероперабилни уколико би чипове израђивале различите фирме.[192]

Према ICAO пропозицијама[193] електронски пасоши треба да садржи бесконтакни чип (према ISO (*International Organization for Standardization*) 14443 стандарду) који треба да буде читљив до 10цм.[194] ICAO је даље одредио да, зарад сигурносних мера, безбедност података на чипу буде обезбеђена тако што ће бити везани електронским потписом.[195] ICAO 9303, уз наведено, подржава и коегзистенцију различитих технологија (бар кодови, магнетне траке, контактни чипови). Овај стандард *не захтева* увођење цен-

[189] David Loukidelis, *Privacy and Security: Seeking a Middle Path,* ауторизовано излагање повереника за информације и приватност Британске Колумбије, на 5th Annual CACR/Ontario IPC, Универзитет у Торонту, 28-29. октобар 2004. Излагање је преузето са адресе: http://www.oipcbc.org/publications/speeches_presentations/CACRspeech102704.pdf

[190] *LSEIP*, стр. 48.

[191] Исто, 49.

[192] Kevin Woodward, „How Smart Card Chips Found Their Way Into Passports“, *CardTechnology*, јун-јул 2006, стр. 33. Часопис је преузет са адресе: http://www.cardtechnology.com/attachments/20060721pv67v73z-1-ct_june_2006.pdf.

[193] ICAO, *Doc 9303.* Документ се налази на адреси: http://www.icao.int/mrtd/publications/doc.cfm.

[194] *MBID,* стр. 115.

[195] *FIDISD3.6*, стр. 8. – У тој спецификације се не помиње експлицитно RFID већ бесконтактна *smart* технологија, мада се између то двоје често не праве разлике чак и у стручним круговима.

тралне базе биометријских података, тј. директно омогућава идентификацију 1:1 и *не захтева* узимање отисака прстију нити физичко присуство особе ради сликања за документ (јер се дигитализовањем може искористити и обична слика која већ постоји у стандардном пасошу).[196]

Дакле, биометријски (електронски) пасоши су посебна врста машински читљивих путничких докумената (*Machine Readable Travel Document*) урађених на основу ICAO 9303 спецификације, који агрегирају податке на минијатурном чипу бесконтактног типа.[197] Притом, за дигиталну слику лица, спецификација не захтева мерење и однос фацијалних тачака, тако да она не представља биометријски податак у ужем смислу, већ обичну дигитализовану слику стандардне слике.[198] Отисци (јагодица) прстију према овој спецификацији су потпуно опциони и остављени националним законодавствима. Уз све наведено, необично је важно подвући чињеницу да ICAO за потребе идентификације путем пасоша не налази за потребно формирање централне базе података, што значи да позив било које владе на њено формирање (било за евиденцију својих грађана било странаца) уоште нема утемељење ни у једној међународној обавези.[199]

3.2.2 ЕУ и имплементација биометријских пасоша

Земље Европе (на првом месту *Visa Waiver* земље, чијим грађанима не треба виза за улазак у САД)[200] су биле принуђене да удовоље захтевима САД које су од њих захтевале израду биометријске пасоша у одређеном року. Око биометријских пасоша у односима ЕУ и САД је било пуно неспоразума.[201] Наиме, иако је 18. фебруара 2004. године Европска комисија дала предлог да само дигитализована слика лица буде обавезан део нових пасоша ЕУ, 13. децембра исте године је донета регулатива по којој су за нове пасоше (или замену старих који су истекли) обавезна и два отиска прста.[202] То је уједно постала и регулатива за земље потписнице Шенгенског споразума (с обзи-

---

[196] Statewatch, „EU: Biometrics - from visas to passports to ID cards“. Чланак је преузет са адресе: http://www.statewatch.org/news/2005/jul/09eu-passports-id-cards.htm.

[197] *FIDISD3.6*, стр.8.

[198] Statewatch , „EU states will be free to fingerprint children from day one of their life as soon as it is technologically possible“. Извештај је преузет са адресе: http://www.statewatch.org/news/2006/jul/08fingerprinting-children.htm.

[199] *LSEIP*, стр. 51.

[200] Андора, Аустралија, Аустрија, Белгија, Брунеји, Данска, Финска, Француска, Немачка, Исланд, Ирска, Италија, Лихтенштајн, Луксембург, Монако, Холандија, Нови Зеланд, Норвешка, Португал, Сан Марино, Сингапур, Словенија, Шпанија, Швајцарска, Шведска и Велика Британија. – Извор: *LSEIP*, стр. 48.

[201] Mikro, „Nesporazumi Evropske unije i SAD oko biometrijskih pasoša“, 06. 04. 2005. Вест је преузета са адресе: http://www.mikro.co.yu/ser/vesti/vesti.php?datum=2005-04-06&ID=6920.

[202] *BETR*, стр. 54.

ром да Норвешка и Исланд нису чланице ЕУ),[203] које у своје нове пасоше треба да укључе исте податке (поред дигиталне слике лица и два отиска прстију),[204] као и да морају имати додатне механизме за заштиту података.[205] Крајњи рок наведен да земље Шенгенске зоне уведу биометријске пасоше је 28. јун 2009. године.[206] Пошто се путовање по шенгенској зони обично изводи преко личних карти (уколико се оне користе као путничка исправа), постојала је могућност да се од земаља те зоне тражи да у личне карте такође уграде биометријске податке који се налазе у новом пасошу,[207] мада је то напослетку остављено на опционој основи као аутономно питање националних законодавстава (погледати поглавље 3.1.2.1).

Информације на биометријском пасошу ће бити заштићене помоћу приватног кључа, а сертификат за дигитални потпис и пар кључева ће се добијати преко сертификационих тела у земљама које ће израђивати ICAO компатибилне пасоше,[208] што и јесте у складу са условом ICAO да информације на пасошу буду везане електронским потписом. Са друге стране, у најмању руку је зачуђујуће да се ЕУ одлучила да у пасош као додатне податке уноси и два отиска прстију, с обзиром да то није био ни захтев ICAO ни САД (захтев је био само дигитализована слика лица).[209]

Прве земље које су кренуле са увођењем бесконтактних пасоша базираних на RFID (*Radio Frequency Identification* – бесконтактна идентификација на бази радио таласа) биометријских пасоша су Белгија, Немачка, Шведска и Норвешка.[210] Од земаља ЕУ, Грчка ће међу последњим израдити биометриј-

---

[203] У месту Шенген (војводство Луксембург) је 14. јуна 1985. године донет споразум, од стране пет земаља (Немачка, Француска, Белгија, Холандија и Луксембург), који је за циљ имао слободно кретање грађана и роба у оквиру граница земаља потписиница (дакле, без пасоша и пратећих формалности). За борбу против организованог криминала на основу тог споразума (члан 93) створен је Шенген информациони систем, гигантска база података у којој се чувају подаци о грађанима земаља потписница. Овај споразум је неколико година чуван у тајности, да би јуна 1990. земље учеснице приступиле његовом остварењу. Касније су се придружиле Италија (1990), Шпанија и Португал (1991), Грчка (1992), Аустрија и Данска (1994). Енглеска и Ирска су одбиле да се придруже, позивајући се на чињеницу да је то највећа регистрација грађана у историји људског рода и да је тај систем антидемоктатски. Данас се под том зоном налази 15 чланица ЕУ и две које су ван ЕУ (Норвешка и Исланд).

[204] *HCICT*, стр. 14. – Пун назив документа је *Council Regulation No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States*.

[205] *MBID*, стр. 117.

[206] EBP, „Pilot project for biometric passports in Switzerland “, 05. 09. 2006. Вест је преузета са адресе http://www.europeanbiometrics.info/news/newsdetail.php?Id_news=258.

[207] Tony Bunyan, нав. есеј, стр. 5.

[208] Kevin Woodward, „Directory Holds The Key To E-Passport Authentication ", *Card Technology*, септембар 2006, стр. 26. Часопис је преузет са адресе: http://www.cardtechnology.com/attachments/200609198f8hr24y-1-ct_sept_2006.pdf.

[209] *FIDISD3.6*, стр. 20.

[210] EBP, „Biometric passports introduced in Sweden and Norway“, 07. 10. 2005. Вест је преузета са адресе: http://www.europeanbiometrics.info/news/newsdetail.php?Id_news=31.

ски пасош.[211] Већ имплементирана решења електронских пасоша у великом броју случајева *немају* централну базу биометријских података (Данска, Швајцарска, Шведска, Норвешка...),[212] што је и логично, с обзиром да то уопште није међународна обавеза. Концептуално, нови пасоши ЕУ не би требало да имају централну базу података, мада је националним законодавствимо остављена слободна воља да реше то питање (да држе или не држе централну базу податка за биометријске пасоше).[213] Иако за пројекат новог ЕУ пасоша на концептуалном нивоу нема централне базе података (начелно, у питању би требао да буде 1:1 начин идентификације), неки компетентни аутори ипак наводе да ће се у једном временском тренутку, под притиском политичких структура, биометријски подаци складиштити у централне базе државног, а потом наддржавног нивоа. [214]

Швајцарци имају можда најбоље решење за ову проблематику: пилот пројекат издавања пасоша у трајању од 5 година, на добровољној основи (осим за грађане који желе да путују у САД),[215] после чега ће се приступити даљој разради система.[216] У Русији ће, према најавама званичника, нови пасоши са чипом бити израђени не раније до у наредне две године, само је још увек нерешено питање које ће конкретне биометријске податке на крају садржати.[217]

3.2.3 Биометријски пасоши у земљама обичајног права

Медији су објавили да ће САД увођење биометријских пасоша за своје грађане завршити до 2017. године.[218] Те вести су углавном биле непотпуне, јер нису садржале информацију да ће иницијални пројекат садржати *само* дигитализовану слику лица,[219] а да ће то решење према ICAO 9303 стандарду бити међународно потпуно интероперабилно.[220] Иронично је да су САД би-

---

[211] EBP, „Greece set for ePassports“, 09. 05. 2006. Вест је преузета са адресе: http://www.europeanbiometrics.info/news/newsdetail.php?Id_news=157.

[212] *LSEIP*, стр. 52.

[213] *FIDISD3.6*, стр. 23.

[214] Tony Bunyan, нав. есеј, стр. 5.

[215] EBP, „Swiss citizens may 'opt-out' of biometric passports until 2011“, 08. 09. 2005. Вест је преузета са адресе: http://www.europeanbiometrics.info/news/newsdetail.php?Id_news=21.

[216] *MBID,* стр. 119.

[217] EBP, „Biometric IDs to be Widely Availabe in 3 Years“, 29. 05. 2006. Прилог је преузет са адресе: http://www.europeanbiometrics.info/news/newsdetail.php?Id_news=172.

[218] Mikro, „Počinje izdavanje RFID pasoša u SAD“, 31. 07. 2006. Вест је преузета са адресе: http://www.mikro.co.yu/ser/vesti/vesti.php?datum=2006-07-31&ID=8271.

[219] Department of State, *Federal Register Vol. 70,* No. 33, 18. 02. 2005. Документ је преузет са адресе: http://a257.g.akamaitech.net/7/257/2422/01jan20051800/edocket.access.gpo.gov/2005/05-3080.htm.

[220] Statewatch, „EU: Biometrics - from visas to passports to ID cards“.

ле spiritus agens пројекта биометријских пасоша, а да највише касне у њиховој изради.[221] Такође је иронија случаја да САД у своје биометријске пасоше уграђују *само* дигитализовану слику лица (без биометријских мерења), док велики број земаља света у пасоше уграђује и биометријске отиске (иако им то нису захтевале ни САД нити је то предвиђено ICAO спецификацијом).

С обзиром да припада *Visa Waiver* групи земаља, Аустралија је од 2005. године почела са спровођењем законског оквира за биометријске пасоше које захтева САД, које ће такође обухватати *само* дигитализовану слику лица, без детаљних фацијалних података.[222]

Слично је у Новом Зеланду, у коме биометријски пасоши треба да имају *само* дигитализовану слику лица, без отисака прстију.[223]

Све наведено је страховито битно јер показује да земље обичајног права агрегирање података какви су биометријски отисци прстију на нови пасош за сада сматрају сувишним и непотребним за своје грађане.

Одступање од правила да се узима само дигитализована слика лица у земљама обичајног права показује само Велика Британија. Либералне демократе су се прикључиле кампањи у којој позивају грађане те земље да обнове своје старе пасоше да би избегли убацивање својих података у централну базу биометријских података, јер свако ко буде аплицирао за нови пасош или буде обнављао стари мораће да преда своје биометријске податке који ће бити коришћени и за централну базу за личне карте (које су у плану), што је велики проблем, с обзиром на углавном критички став британске јавности према централној бази биометријских података.[224]

3.2.4 Биометријски пасоши у земљама трећег света

Земље трећег света се буквално „намамљују“ на биометријски пасош тако што им се тиме нуди да са „црне листе“ (земље којима су потребне визе) пређу на „белу“ (земље којима не требају визе) [225] и аргументом да ће се и посетиоцима са визама узимати отисци. [226] Једна од првих земаља Далеког истока у свету која је креирала биометријски пасош за своје становнике био

---

[221] Kevin Woodward, „E-Passports Await Real-World Tests“, *CardTechnology*, март 2006, стр. 28. Часопис је преузет са адресе: http://www.cardtechnology.com/attachments/200604054yolcsdx-1-ct_march_2006.pdf.

[222] ZDNet Australia, „Senate passes passport biometric, RFID legislation“. Вест је преузета са адресе: http://www.zdnet.com.au/news/security/soa/Senate_passes_passport_biometric_rfid_legislation/0,130061744,139180464,00.htm.

[223] Marie Shroff, нав. дело, стр.7.

[224] EBP, „UK: Liberal Democrats urge citizens to renew their passports“, 25. 05. 2006. Вест је преузета са адресе: http://www.europeanbiometrics.info/news/newsdetail.php?Id_news=181.

[225] Tony Bunyan, нав. есеј, стр. 4.

[226] Исто, 5.

Тајланд, у коме је процедура обраде биометријских података, благо речено, проблематично и неозбиљно решена.[227]

3.2.5 Критички осврт на увођење биометријских пасоша

За разлику од биометријске личне карте у систему са централном базом података, биометријски пасош је нешто сврсисходније решење, у смислу да показује да документ припада његовом имаоцу и да подаци не излазе из њега (тј. да нема централне базе, уколико би концепт 1:1 идентификације остао на снази).[228] Занимљиво је да пробиометријски кругови постепено увођење отисака прстију свих грађана (а не само криминалаца) за потребе увођења биометријских личних карти правдају управо чињеницом да ће се ти подаци већ узимати за нови ЕУ пасош.[229] То наравно не стоји, јер је кључна ствар чињеница да према ICAO спецификацији електронских пасоша *не постоји* захтев за позадинском базом биометријских података, већ је у питању класична 1:1 идентификација (тј. аутентификација идентитета).

Са друге стране, расту страховања да би електронски пасош у одређеном временском року могао да прерасте у неку врсту глобалног идентификационог документа,[230] с обзиром да га у иностранству грађани показују у хотелима, приликом замене новца, а у неким земљама чак и у Интернет кафеима.[231] Постоје веома упорни предлози за формирање наддржавне базе података биометријских отисака, који би укључио земље западне цивилизације (пилот пројекат се изводи између САД и Велике Британије). То би се у пракси остварило децентрализованим приступом размене биометријских података између ЕУ и осталих земаља (превасходно САД).[232] Пројекат се оправдава пре свега из аспекта економских трошкова, али се признаје да то може довести до великих проблема због загарантованих грађанских слобода.[233] Стога велики број академских грађана директно упозорава на безбед-

---

[227] Kevin Woodward, „E-Passports Await Real-World Tests“, стр. 31. – На Тајланду је процедура следећа: у посебним кабинама се узимају биометријски подаци грађана, који се потом нарезују на CD и отпремају у Бангкок, где Министарство унутрашњих послова на основну снимљених података у року од шест недеља израђује пасоше. Ово је вероватно једна од најнебезбенијих процедура у целом свету када су електронски пасоши у питању, мада грађани Тајланда вероватно немају изражену свест о томе, с обзиром да им влада пре свега сугерише да пасош не савијају и да не седе на њему, а не како да чувају податке од неовлашћеног копирања и коришћења.

[228] Julian Ashbourn, нав. дело, стр. 19.

[229] *BETR*, стр. 18.

[230] Bruce Schneier, „Fatal Flaw Weakens RFID Passports“, *Wired*, 2. 11. 2006. Чланак је преузет са адресе: http://www.wired.com/news/technology/0,69453-0.html.

[231] Исто. – Такав је случај у Италији, рецимо.

[232] EBP , „Exploring traveller’s biometric data sharing“, 02. 11. 2006. Чланак је преузет са адресе: http://www.europeanbiometrics.info/news/newsdetail.php?Id_news=319.

[233] Исто.

носне пропусте оваквог приступа.[234] Постоје и реакције академских институција и тела ЕУ. FIDIS (*Future of Identity in the Information Society*),[235] тело које има подршку ЕУ, је у новембру месецу 2006. године навело да су европске владе ефикасно натерале грађане да се прилагоде новом стандарду тзв. машински читљивих докумената попут RFID пасоша, или, у једном броју случајева, биометријских идентификационих карти, који драматично смањују њихову безбедност.[236]

Поставља се и питање *интероперабилности* пасоша, тј. читљивости на свим читачима који су урађени према стандарду ISO 14443 (главни међународни стандард за бесконтакте чипове), јер се у лабораториским условима показало да ниједан читач не може да прочита чипове свих произвођача који су урађени према тој спецификацији.[237] Испоставило се и да је узимање квалитетне дигиталне слике лица теже него што је очекивано, уколико се иста узима као пуни биометријски податак (дакле, са мерењем фацијалних особености) јер мора бити довољно квалитетна за софтвер за аутоматско препознавање лица на пунктовима.[238]

Дебате око сигурности RFID пасоша које су вођене између службеника влада и представника НВО сектора који се бори за приватност грађана показују огроман број нерешених питања (пре свега из области безбедности) са којима се суочавају владе које желе да уведу овакве системе.[239] Највећи светски стручњаци из области рачунарске безбедности су се негативно изразили по питању овог концепта, позивајући се пре свега на чињеницу да не постоје адекватни правнотехнички механизми заштите података на пасошу а посредно ни личности која га носи. Брус Шнајер (*Bruce Schneier*), један од

---

[234] Mikro, „Britanski e-pasoši laki za `provaljivanje`“, 29. 11. 2006. Текст је преузет са адресе: http://www.mikro.co.yu/ser/vesti/vesti.php?datum=2006-11-29&ID=500224. – Питер Гутман са Универзитета у Окленду (Нови Зеланд) сматра да су RFID пасоши „катастрофа која треба да се догоди“. Гутман упозорава да је безбедност грађана угрожена јер би и терористи покушали да украдене податке искористе да би извршили атентат на неку личност.

[235] Будимпештанска декларација ове организације биће у целости наведена у последњем одељку.

[236] FIDIS, *Budapest Declaration on Machine Readable Travel Documents (MRTDs)*, 08. 11. 2006. Декларација је преузета са адресе: http://www.fidis.net/press-events/press-releases/budapest-declaration/.

[237] Kevin Woodward, „Electronic Passports: Is a Global Certification Body Necessary?“, *CardTechnology*, април 2006, стр. 32. Часопис је преузет са адресе: http://www.cardtechnology.com/attachments/20060516n1xjiwx3-1-ct_april_2006.pdf.

[238] Kevin Woodward, „Deadline Nears For U.S. Federal Employee ID“, antrfile „Getting Good E-Passport Photos is Tougher than Imagined“, *CardTechnology*, мај 2006, стр. 27. Часопис је преузет са адресе: http://www.cardtechnology.com/attachments/200605319z8l4fwd-1-ct_may_2006.pdf. – У Великој Британији је проценат одбијених слика (узетих уз фацијалне особености) за нови пасош био 7.5%, било због сенки или зато што лице није било добро позиционирано.

[239] Погледати с тим у вези дебату између Мојре Харти (Maura Harty) и правног заступника ACLU-а Берија Стајнхарда (Barry Steinhardt) коју је објавио *The Wall Street Journal*, под називом „Are E-Passports More Secure?“ од 29. септембра 2006. на адреси: http://online.wsj.com/public/article/sb115938787873075826-6abupmiajvcs1i_ubvogrwp867k_20070929.html.

највећих светских криптолога и стручњака за безбедност информационих система, тврди да је биометријске пасоше могуће очитавати са знатно веће удаљености него што то тврде службеници америчке владе, наводећи да би то омогућило креирање механизма који би активирао експлозив у тренутку када поред читача прође одређена особа.[240] Овај стручњак тврди даће то поговото бити могуће у наредним година са напретком антенске технологије, због чега отворено позива све људе да обнове стари пасош.[241] Иако су према ISO 14443 стандарду чипови на пасошима оптимизовани да буду читани на удаљености од 10-15цм, стручне и експерименталне студије показују да је хватање комуникације између читача и чипа могуће и са даљине од 2 до 10м.[242] Стручни конзорцијуми с тим у вези позивају да се пасош носи само када је то преко потребно и да се у другим случајевима држи у Фарадејевом кавезу, ради спречавања неауторизованог приступа информацијама.[243]

Професор Рос Андерсон (*Ross Anderson*) који ради у Компјутерској лабораторији Универзитета у Кембрицу тврди да би информације украдене из електронског пасоша криминалци итекако могли да искористе и поставља питање да ли је то само врх леденог брега безбедносних пропуста.[244]

Иако владе тврде да чипови у пасошу поседују посебне алгоритме за енкрипцију чиме је онемогућено њихово читање од стране неауторизованих појединаца на неауторизвоан начин, тиме проблем није решен, јер сваки од чипова мора имати јединствен идентификациони број да би се избегла колизија између различитих уређаја који пролазе поред читачког пункта. Одређену особу је лако идентификовати у случају да исправе имају само фиксни идентификациони број, уколико постоји база на коју се он односи.[245] Истраживања су показала на који начин је могуће одређени чип једнозначно идентификовати (а посредно и његовог носиоца).[246] Додуше, решење је у прављењу бесконтактних чипова према спецификацији која додељује случајне, динамичке бројеве, али многи стручњаци изражавају сумњу да се произвођачи уопште држе тог стандарда (због повећања трошкова израде).[247] С тим у вези, треба рећи да је smart контактна технологија данас далеко поузданија од RFID решења које се предлаже за е-пасоше.[248] RFID решење је иначе

---

[240] Bruce Schneier, „Fatal Flaw Weakens RFID Passports“.

[241] Bruce Schneier, „The ID Chip You Don’t Want in Your Passport“, *Washington Post.* Чланак је преузет са адресе: http://www.schneier.com/essay-125.html.

[242] FIDIS, *Budapest Declaration on Machine Readable Travel Documents (MRTDs).*

[243] *FIDISD3.6*, стр. 46.

[244] „Cracked it! “, (непотписан чланак), *The Guardian*, 17. 11. 2006. Чланак је преузет са адресе: http://www.guardian.co.uk/idcards/story/0,,1950226,00.html.

[245] Bruce Schneier, „Fatal Flaw Weakens RFID Passports“.

[246] Исто.

[247] Исто.

[248] Исто.

прилично оспоравано по питању безбедности података не само код нових пасоша, већ и код платних картица које су базиране на њему,[249] јер се у лабораторијским тестовима испоставило да се осетљиве информације (попут имена и броја картице) могу извући због слабих заштитних механизама.

Јавност је нестрпљиво очекивала експерименталне тестове сигурности нових пасоша.[250] На тако нешто није се дуго чекало. Прво је јавно компромитован холандски пасош, због једноставног алгоритма који је коришћен приликом додељивања тајног кључа. Он је био предвидљив јер су улазни подаци за његово генерисање били датум рођења и истицања пасоша, серијски број и збир за проверу. [251] О том случају је објављена је и кратка студија.[252]

Немачки истраживач Лукас Грунвалдс (*Lukas Grunwalds*) је у августу на конференцији посвећеној безбедности у Лас Вегасу показао како се *tag* (тј. бесконтактни чип) може лако клонирати,[253]док су друга два истраживача на истој конференцији показала на који начин је теоријски могуће даљински активирати експлозив приликом проласка особе са електронским RFID пасошом.[254]

После сличног истраживања Гардијана (*Guardian*) које је показало да је нове британске пасоше могуће клонирати употребом јефтине опреме,[255] британска влада се суочила са захтевима да повуче око 3 милиона микрочипованих пасоша.[256] Информациони експерт Адам Лури (*Adam Laurie*), човек који је јавности познатак као проналазач огромног броја безбедносних пропуста код *BlueTooth* телефона,[257] је користећи јавно доступну документацију (углавном од стране ICAO) за само 48 сати написао програмски код који му

[249] Погледати технички извештај који су направили Thomas S. Heydt-Benjamin, Daniel V. Bailey, Kevin Fu, Ari Juels, and Tom O'Hare под називом „RFID Payment Card Vulnerabilities Technical Report", 10. 11. 2006, на адреси: http://www.nytimes.com/packages/pdf/business/20061023_card/techreport.pdf.

[250] Kevin Woodward, „E-Passports Await Real-World Tests", стр. 26.

[251] Engadget, „Dutch RFID e-passport cracked - US next?". Вест је преузета са адресе: http://www.engadget.com/2006/02/03/dutch-rfid-e-passport-cracked-us-next/.

[252] Harko Robroch, „ePassport Privacy Attack". Студија је преузета са адресе: www.riscure. com/2_news/200604%20CardsAsiaSing%20ePassport%20Privacy.pdf.

[253] „The Month: Researchers raise concern over RFID security", (непотписан чланак), *SC Magazine*. Текст је преузет са адресе http://www.scmagazine.com.au/feature/3067,the-month-researchers-raise-concern-over-rfid-security.aspx.

[254] Овом догађају су и српски медији посветили пажњу. Погледати специјално издање новина Danas под називом Com_Media, од 9. августа 2006. године, под називом „Hakeri mogu da kloniraju čipove sa ličnim podacima", на адреси http://www.danas.co.yu/20060809/commedia1.html.

[255] Steve Boggan , „Recall demand after cloning of new biometric passports", *The Guardian*, 17. 11. 2006. Чланак је преузет са адресе: http://www.guardian.co.uk/idcards/story/0,,1950229,00.html.

[256] Највећи притисак на владу је од стране либералних демократа. Погледати: Steve Boggan, нав. чланак.

[257] The Guardian, „Cracked it!".

је омогућио да извуче податке са чипа на пасошу, користећи пропуст који је влада направила у веома јакој 3DES енкрипцији пасоша (за креирање тајног кључа коришћена је информација публиковану у пасошу).[258] Такав приступ британске владе овај безбедносни стручњак је окарактерисао као креирање челичних врата на кући и стављање кључа под отирач.[259]

Истине ради, треба навести да су владе и произвођачи опреме реаговали са реалном тврдњом да чак и ако неко успе са клонирањем информација које се налазе на пасошу, нико неће моћи да их измени јер су везани електронским потписом.[260] То у великој мери јесте тачно али не отклања проблеме око пресретања комуникације чипа и пункта као ни компромитовања клонираног материјала. Реакције службеника владâ и пружање објашњења да још увек нису имплементирану сви сигурносни механизми ипак нису имали ефекта јер су наведени догађаји су унели велику дозу скепсе међу широ јавности, тако да је подршка грађана овој врсти докумената нагло опала.

3.2.6 Будимпештанска декларација уместо закључка о имплементацији биометријских пасоша

За сумарни закључак о биометријским пасошима упутно је почети са ставом стручног конзорцијума FIDIS. Ово тело ЕУ састављено од врхунских европских истраживачких установа, факултета, института и компанија из области информатике и електронског пословања у тзв. *Будимпештанској декларацији* упозорило је на чињеницу да нова биометријски путничка документа драстично смањују приватност и безбедност грађана и да повећавају ризик од крађе идентитета.

У абстракту своје декларације (*Budapest Declaration on Machine Readable Travel Documents* (MRTDs) стручњаци FIDIS конзорцијума тврде да су у недостатку адекватне информационе инфраструктуре владе европских држава ефикасно приморале грађане да усвоје нови тип докумената (*Machine Readable Travel Documents* – машински читљива путничка документа). Основна замерка је да ће та документа моћи да се читају са великих даљина, што отвара простор за крађу идентификационих података од стране неауторизованих трећих лица и омогућити праћење људи који носе такав документ. Друга битна замерка је да се информације које се налазе на документу експлоатишу како од јавног тако од приватног сектора за различите сврхе, што крши европске принципе приватности.

Као проблематични аспекти сигурности наводе се крађа биометрије која је неповратна, затим недовољна заштита пасоша, шпијунирање комуни-

[258] Steve Boggan , нав. чланак.

[259] The Guardian, нав. чланак.

[260] Kevin Woodward, „Directory Holds The Key To E-Passport Authentication“, стр. 27.

кације чипа на пасошу и читачког пункта, клонирање RFID тагова, па чак и постављање паметних бомби.

Међу препорукама које је ово стручно тело дало политичарима, индустрији и истраживачима Европе је и: строго наменско одређивање ко може да врши аутентификацију пасоша, поготово у контексту биометријских информација и приватног сектора који би био заинтересован за њих, детаљно обавештавање грађана са сигурносним ризиком који прати употребу оваквих докумената, обезбеђивање сигурносних мера какав је Фарадејев кавез и израда организационих и техничких мера за спречавање злоупотреба података и крађе идентитета. Због њеног значаја, Будимпештанска декларација је у целости објављена у последњем поглављу књиге.

На закључке овог конзорцијума треба додати и то да је потпуно несхватљиво због чега је ЕУ проширила скуп биометријских података за нови пасош и на отиске прстију, јер тако нешто није био ни захтев САД нити ICAO (тј. УН), те да није добра пракса нелојалног условљавања земаља из остатка света да их такође имплементирају. Код концепта биометријских пасоша је једно од најбитнијих питања истрајност у одржању концепта без базе података, на принципу 1:1 идентификације. Међутим, нови систем Шенген 2 (SIS II – *Schengen Information System*), који треба да ступи на снагу током 2007. године, већ се у великој мери приближава централизованој бази података на нивоу ЕУ, са могућностима произвољног проширивања базе. Систем већ наилази на критике, између осталог због заобилажења националних законодавстава и самог Европског парламента током његовог креирања, што постаје све чешћи случај приликом увођења оваквих технологија широм света.[261]

3.3 Специјална употреба биометријских система идентификације на националном и наднационалном нивоу

У ЕУ се, у току завршних радова на овој студији, воде дебате о узимању биометријских података од деце избеглица преко *EURODAC* регулације донете 2000. године,[262] јер постоје неслагања око обима података и узраста за који би се подаци узимали.[263] О брзини развоја ових ствари говори и чињеница да је Немачка 2001. предложила да свака држава чланица води базу података о грађанима из земаља трећег света који у њима бораве, што је у то

[261] За детаљну критику овог концепта погледати Ben Hayes, *Construction of EU's Big Brother database,* Statewatch, мај 2005, на адреси: http://www.statewatch.org/news/2005/may/sisII-analysis-may05.pdf.

[262] Statewatch, „EU states will be free to fingerprint children from day one of their life as soon as it is technologically possible".

[263] Statewatch, „EU: Fingerprinting of children - the debate goes on". Документ је преузет са адресе: http://www.statewatch.org/news/2006/aug/02eu-fingerprinting-children.htm.

време одбијено од осталих чланица, али већ 2003. године све чланице су се сложиле да имигрантима узимају биометријске отиске прстију, да им доделе биометријске личне карте са чипом и да те податке складиште у базе.[264] Стручњаци из области биометријске идентификације наводе да је чињеница да се идентификационим менаџментом полако еродирају традиционалне вредности ЕУ, те да ће имигранти на такво друштво гледати са сумњом и неће хтети у њега да се уклопе.[265]

Финци ће нови AFIS систем (чија је основна намена иначе у идентификацији криминалаца преко отисака прстију)[266] користити за визе, пасоше и идентификационе карте за азиланте.[267] Ирска (која за своје грађане не издаје личне карте), треба да почне са коришћењем Motorola AFIS биометријског система за имигранте и криминалце.[268] После критика организација које се боре за заштиту права на приватност, Министарство правде Ирске ће уградити механизме за раздвајање те две базе.[269]

Постоје случајеви (у Великој Британији, рецимо) да се биометрија узима и у неким школама, поготово у мензама и библиотекама, што доводи до великог отпора родитеља, али и људи који су запослени у образовном сектору.[270] Велики број организација је жестоко напао овај концепт, сматрајући га незаконитим, небезбедним, по приватност катастрофалним решењем, због чега је уведен обавезан пристанак родитеља у многим школама.[271] Многи сматрају да се овим деца навикавају на један систем идентификације да би га без отпора прихватили на националном нивоу када одрасту.[272]

По питању имиграната, у САД се користи биометријски систем идентификације под називом *US VISIT*,[273] који је у великој мери утицао да сличне системе за своје имигранте уведу Канада и Аустралија. Америчка влада

---

[264] Tony Bunyan, нав. есеј, стр. 3.

[265] Julian Ashbourn, нав. дело, стр. 22.

[266] AFIS (*Automated Fingerprint Identification*) систем је као аутоматски систем препознавања отисака прстију који се појавио 1960. године, ради брзе претраге великих база података отисака, углавном коришћених за обраду база криминалаца. Извор: *MBID*, стр. 69.

[267] EBP, „Finnish Police take delivery of new AFIS“, 28. 04. 2006. Вест је преузета са адресе: http://www.europeanbiometrics.info/news/newsdetail.php?Id_news=152.

[268] EBP, „New AFIS in Ireland “, 04. 12. 2006. Вест је преузета са адресе: http://www.europeanbiometrics.info/news/newsdetail.php?Id_news=351.

[269] Исто.

[270] Janette Owen, „Where do we stand on fingerprinting pupils?“, *The Guardian*, 21. 11. 2006. Текст је преузет са адресе: http://education.guardian.co.uk/schools/teach/story/0,,1952673,00.html.

[271] Погледати шта о томе каже организација LeaveThemKidsAlone „10 Things You Should Know About Schools Fingerprinting Children“. Текст је преузет са адресе: http://www.leavethemkidsalone.com/10things.htm

[272] Исто.

[273] EPIC, „United States Visitor and Immigrant Status Indicator Technology: (US-VISIT)“. Чланак је преузет са адресе: http://www.epic.org/privacy/us-visit/.

овај систем оправдава контролом и спречавањем илегалног уласка и рада имиграната. У протеклој деценији САД су користиле и друге видове небиометријских система идентификације избеглица са одређених подручја, који су у великој мери били дехуманизовани.[274] САД узимају биометријске податке и за странце који често прелазе границу ове земље.[275]Аустралија такође имплементира својеврсан биометријски систем идентификације који се користи само за имигранте,[276] а слично томе и Канада.[277]

Јапан је усвојио стратегију САД да узима електронске отиске и слике странаца који улазе у земљу, мада је таква одлука наишла на веома оштро противљење Демократске странке у тој земљи, која изражава бојазан због приватности и чињенице да у међународној заједници не постоји чврст консензус око питања узимања биометрије странцима, те да су једино САД по том питању резолутне.[278]

Биометријски системи идентификације се често користе у ратним зонама, попут Фалуџе (Ирак) или за контролу осетљиве границе (авганистанско-пакистанска, рецимо).[279] У Уједињеним Арапским Емиратима користе се за контролу границе, уз употребу скена рожњаче као идентификатора. [280]

У последње време су учестали покушаји популарисања коришћења људског тела као лозинке, без икаквих карти или PIN кодова.[281] С тим у вези, неке банке користе скен рожњаче као сигурносни механизам да би провериле да ли је одређена особа ауторизована да подигне новац са рачуна.[282]

За додатни увид у специфичне системе биометријске идентификације, погледати и поглавље 2.1 ове студије.

3.4 Сумарни закључак

Биометријски системи идентификације на (над)националном нивоу се у свету уводе са несхватљиво мало критичког става. Брзина којом се све остварује, насупрот безбедносним упозорењима врхунских стручњака из обла-

[274] Познат је случај наредбе председника Била Клинтона који је 1994. године одредио да се код 50 хиљада кубанских и хаићанских избеглица користи систем са наруквицама за електронско праћење локације. То је био тзв. DMPITS систем.

[275] A. Michael Froomkin, нав. дело, стр. 8.

[276] EBP, „Australia implement biometrics for immigration“, 22. 09. 2006. Вест је преузета са адресе: http://www.europeanbiometrics.info/news/newsdetail.php?Id_news=280.

[277] EBP, „Canada tests biometrics in immigration field trial“, 14. 06. 2006. Вест је преузета са адресе: http://www.europeanbiometrics.info/news/newsdetail.php?Id_news=191.

[278] USA Today, „Joining USA, Japan to fingerprint and photograph foreign visitors“. Вест је преузета са адресе: http://www.usatoday.com/travel/news/2006-05-17-japan-fingerprint_x.htm?csp=34.

[279] *LSEI*P, стр. 57.

[280] *HCICT,* стр. 14.

[281] A. Michael Froomkin, нав. дело, стр. 8.

[282] Исто.

сти информационих технологија, безбедности и компјутерског права, да адекватни и поуздани правнотехнички механизми заштите још увек не постоје – просто забрињава. Извесно је да ће многи од тих система у пракси доживети крах, у мањем или већем обиму, и да неће испунити очекивања због којих су уведени. Са друге стране, вероватно ће бити и система који ће се показати поузданим у одређеној мери (то пре свега важи за имплементације којима ће претходити вишегодишња припрема, провера и пилот-пројекти).

Но чини се да је најбитније питање: шта ће бити следећа итерација данашњих верзија биометријских система идентификације, када се покажу пропусти и рањивости у пракси? Да ли ће то бити енормно проширивање биометријског скупа података на све могуће идентификаторе, што би водило невиђеном упаду у приватност? Или ће то бити системи без докумената који ће функционисати на принципу централне базе података и скривених камера високе резолуције, чији ће процесори у реалном времену обрађивати лица свих пролазника? Или је можда следеће решење неки вид имплантата, што се већ спроводи у оквиру неких затворених подсистема? Тешко да се одговор на ово питање може наћи само једном студијом.

Одређивање граница биометријских технологија, уз пожељно уважавање принципа добровољности, једини је начин да се избегне сценарио друштва под тоталним надзором и некритичких имплементација базираних на политичком волунтаризму, чему данашње иницијативе очигледно воде. У томе велика одговорност лежи на академским институцијама које су per se призване на сведочење критичког става и које треба активније да се укључе у проблематику имплементације биометријских система идентификације, пре свега на ширем (државном односно наддржавном) нивоу. Реакције професора Лондонске школе економије и политичких наука, Аустралијског националног универзитета, Правног факултета Универзитета у Отави као и FIDIS стручног конзорцијума дају блистав пример критичког и неконформистичког става какав се очекује и од чланова осталих академских и стручних установа у свету и Србији.

Република Србија: Биометријски пројекат

...Велики број активности је био и остао промашен, погрешно оцењен, нелогичан и политички мотивисан – укратко, крајње непрофесоналан.

Roger Clarke, „Biometric Insecurity“

Историјат биометријског пројекта идентификације грађана у Републици Србији је случај sui generis и заслужује посебно поглавље из више разлога. На првом месту, треба истаћи чињеницу да је тај пројекат имао одлучујући утицај на креирање ове студије. Други разлог је у политичкој, економској, правној и технолошкој специфичности, која показује велике подударности са блискоисточним и донекле далекоисточним земљама, а далеко мање са државама из окружења. Трећи разлог лежи у потреби за детаљним разјашњењем овог проблема грађанима Србије, с обзиром на огроман број дезинформација које су неретко долазиле од надлежних министарстава и државних медија, као и неких пропонената и опонената биометријског система. И на крају, потребно је оставити историјски документ као сведочанство генерацијама које долазе, а које на основу њега могу извући битне закључке за сопствено окружење.

4.1 Куповина рачунарског биометријског система: историјат, планови и (не)законитост

Септембра месеца 2003. године тадашњи министар полиције Републике Србије, Душан Михајловић, се преко средстава јавног информисања обратио јавности, наводећи да је са фирмом *Motorola* склопљен уговор вредан 20 милиона евра, „чија ће примена побољшати имовинску и личну сигурност грађана, остваривање њихових права и безбедност државне границе".[1] Притом је наведено да је у питању најсавременији биометријски систем идентификације и да су средства за тај пројекат обезбеђена из републичког буџета.[2]

Нека западна средства информисања су такође пренела ту вест, истичући да ће тиме бити креирана како биометријска база за криминалце тако и за обичне грађане Србије, те да ће она обухватати дигиталне отиске прстију и дигиталне слике лица са специјалним информацијама о фацијалним особеностима,[3] које ће се узимати употребом посебних скенера.

Истовремено, МУП Србије је дао званично саопштење, које је било препуно спорних ставова и дезинформација.[4] Између осталог, готово све земље које су наведене у саопштењу као примери земаља које користе поменути систем *нису* имале (нити данас имају) биометријске личне карте, а саопштење је срочено тако да управо имплицира такав закључак.[5] *Motorola* је, са друге стране, дала реалније саопштење по том питању, наводећи да је то први идентификациони систем те врсте у Европи.[6]

У каснијим изјавама високих представника ове фирме, навођено је да идентификациони систем у Србији спада у најкомплексније системе ове фирме који су до сада ушли у рад.[7] Поред техничких детаља система, од стране

---

[1] Танјуг, „MUP-Mihajlovic: Novi informacioni sistem poboljsace sigurnost gradjana ", 11. септембар 2003. Вест је преузета са адресе: http://www.mfa.gov.yu/Srpski/Bilteni/Srpski/b120903_s.html#N25.

[2] Исто.

[3] HPC wire, „Motorola Gives Serbia $21 Million For Integrated ID System". Вест је преузета са адресе: http://www.taborcommunications.com/hpcwire/hpcwirewww/03/1010/106157.html.

[4] МУП Србије, „Veliki korak u modernizaciji rada policije", 4. 12. 2003 – KZN. Саопштење је преузето са адресе: http://www.mup.sr. gov.yu/domino%5Carh.nsf/4122003.

[5] Исто. – Међу земљама које користе *Printrak* решења су поменуте у саопштењу МУП-а: Словенија, Грчка, Швајцарска, Норвешка, Данска ... али није речено *која* је конкретно имплементација у питању, поготово што ниједна од наведених земаља ни дан данас није увела биометријске личне карте, чак ни на добровољном нивоу, док их Данска не поседује ни у каквом виду.

[6] М. Анђелковић, „За двадесет милиона евра Србија уводи документа која нико нема", Балкан, 17. 01. 2004. – Реч је о изјави Натана Гидрона (*Nathan Gidron*), потпредседника *Motorola*-е, која је дата у оквиру наведеног текста.

[7] „Interview with Darrin Reilly, Vice President and General Manager Biometrics Business unit, Motorola Inc.", март 2006. Интервју је преузет са адресе: http://www.findbiometrics.com/Pages/feature_motorola_mar06.htm. – На питање новинара да ли је *Motorola* игде у свету продала систем за биометријску идентификацију већег броја грађана („*large scale*" систем), потпредседник биометријског одсека ове фирме је на првом месту навео Србију (која је према његовој процени систем од 10 милиона корисникâ).

српског МУП-а наведене су неке нерелеватне предности овог система идентификације, између осталог да нису више потребне фотографије, да нема више прљања прстију, као и да се лична карта може послати поштом.[8] Наведено је да су грађани Србије овим системом и корак ближе укидању визног режима, мада нигде није наведено на основу ког документа, међудржавног уговора или договора се то тврди. У изјавама службеникâ МУП-а је било речи и о амбициознијим плановима, али они се нису остварили.[9]

Информације о новим биометријским личним картама и њиховом увођењу су пренели електронски и штампани медији, углавном преносећи саопштење српског МУП-а или његових званичника. Међутим, већ првих дана после најаве тог пројекта су се појавили и критички чланци, који су упозорили на могућу незаконитост и правну лабилност конкретног пројекта.[10]

После годину дана се огласила и Буџетска инспекција Министарства финансија, са подношењем неколико кривичних и прекршајних пријава због склапања наведеног уговора о куповини опреме.[11] У саопштењу инспекције је речено да су куповином опреме за биометријску идентификацију од фирме Motorola *прекршени* Закон о буџетском систему и Закон о јавним набавкама,[12] јер приликом реализације тог уговора није тражена сагласности Управе за јавне набавке.[13] Притом је истакнуто да спорни уговор има и клаузулу која штити произвођача, што очито представља склапање штетног уговора по државу,[14] као још једног кривичног дела.

Званична саопштења МУП-а тим поводом су на сваки могући начин штитила постигнути споразум око куповине опреме.[15] У истим саопштењима константно је пласирана дезинформација да су овакви документи услов за испуњавање међународних стандарда и усаглашавање наших докумената са европским и светским стандардима, препорукама и директивама, те

---

[8] М. Анђелковић, нав. чланак.

[9] У Дневном телеграфу од 1. октобра 2003. је наведено да до краја 2006. већи део личних докумената попут возачких и саобраћајних дозвола, оружаних листова и томе слично треба да замене smart карте.

[10] R.D, „Motoroli i Arijusu isti posao? “, Danas, 10. 12. 2003. Чланак је преузет са адресе: www.danas.co.yu/20031210/frontpage1.html.

[11] K.P, „Nezakonit tender za opremu MUP-a“, Blic, 30. 9. 2004. Чланак је преузет са адресе: http://www.blic.co.yu/blic/arhiva/2004-09-30/strane/tema.htm#1.

[12] Исто.

[13] Transparentnost Srbija, „Inspektori Ministarstva finansija Srbije o odlivu kapitala vrednog više od milijardu evra“, вест је пренета из Вечерњих новости од 30. 09. 2004. Текст је преузет са адресе: http://www.transparentnost.org.yu/ts_mediji/stampa/2004/septembar_2004/3009-04.html

[14] Исто.

[15] У саопштењу МУП-а под деловодним протоколом *01.broj: 32/05* од *1.03.2005*, се између осталог каже да законитост поступка куповине опреме представља одвојено питање од реализације пројекта. Ту такође стоји да је нови министар полиције, Драган Јочић, поставио питање сврсисходности куповине опреме у време када МУП није имао средстава за нормално функционисање, али да су уговори обавезујући и имају веома строге клаузуле.

да оваква идентификациона документа морају да испуне стандарде који су услов за придруживање ЕУ.[16]

4.2 Реакције јавности пре доношења Закона о личној карти

Реакције јавности пре доношења закона биле су различите. Критички гласови су били учестали, али је медијска блокада била очигледна. Стога је веома важно дати макар кратку хронологију критичких реакција пре доношења Закона о личној карти, а који медијски нису адекватно пропраћени.

4.2.1 Стручни скупови пре усвајања Закона: Жички симпосион

Жички симпосион је први стручни скуп који је размотрио питање пројекта биометријског система идентификације у Србији и оспорио га из правног, етичког, безбедносног и информатичког аспекта. Одржан је 26. марта 2005. године у Жичи и у Краљеву, у организацији епископије жичке и са благословом епископа Хрисостома. Симпосион је окупио стручњаке из различитих области,[17] који су донели закључак у десет тачака.

У наредних годину дана, због збивања на домаћој и светској сцени, тај закључак је нешто проширен и додата му је још једна тачка, те га је као таквог, у виду апела јавности, потписао велики број угледних српских интелектуалаца.[18] Значај овог симпосиона је вишеструк, али пре свега се огледа

---

[16] Погледати саопштење МУП-а 01.broj: 32/05 1.03.2005. на адреси http://www.mup.sr.gov.yu/domino%5Carhiva.nsf/1mart05mup. – „...Апсолутно се не ради о штампању докумената, већ о изради електронских идентификационих докумената у складу са међународним стандардима. Набављена опрема и софтвер ослања се на постојећу инфраструктуру МУП-а и задовољава потребу за усаглашавањем идентификационих докумената са европским и светским стандардима, препорукама и директивама – до јануара 2006.године...“; „...Идентификациона документа морају да испуне европске стандарде, који су постављени и представљају услов за придруживање, тако да евентуални приход није приоритет и представљао би приход буџета Републике Србије, који би допринео лакшем измиривању преузетих обавеза у наредним годинама...“

[17] Учесници симпосиона били су: академик Никола Милошевић (редовни члан САНУ), проф. др Милорад Стевановић (Универзитет у Крагујевцу и Бањалуци), доц. др Синиша Влајић (информатичка катедра ФОН-а), Снежана Стојковић (Министарство просвете), протођакон мр Радош Младеновић, уредник Жичког благовесника и управник Дома владике Николаја у Краљеву, публициста Владимир Димитријевић и Оливер Суботић. Почетку радног дела стручног скупа је присуствовао и епископ жички Хрисостом.

[18] Између осталих, принцеза Линда Карађорђевић, проф. др Никола Милошевић (редовни члан САНУ), Милован Данојлић (дописни члан САНУ), проф. др Александар Липковски (Математички факултет БУ), проф. др Љубомир Протић (Математички факултет БУ), проф. др Љиљана Чолић (Филолошки факултет БУ), проф. др Мирјана Стефановски (Правни факултет БУ), проф. др Милорад Стевановић (Технички факултет Универзитета у Крагујевцу), проф. др Зоран Аврамовић (Философски факултет Универзитета у Косовској Митровици), проф. др Вељко Ђурић (Философски факултет Универзитета у Косовској Митровици), др Жарко Видовић, философ, Предраг Р. Драгић-Кијук, књижевник, мр Дејан Мировић, правник и публициста, протођакон Радош Младеновић, управник Духовног центра Светог Владике Николаја у Краљеву, Владан Глишић, Бошко Обрадовић, Бранимир Нешић и комплетно уредништво часописа „Српски сабор Двери“, Алексан-

у чињеници да је то био први стручни скуп који је поставио питање легалности пројекта биометријске идентификације грађана у Србији, упозорио на његове консеквенце по приватност и безбедност грађана и успоставио корелацију са случајевима из светске праксе. Представници власти и МУП-а нису дали своје мишљење о тачкама овог симпосиона, које су јуна 2006. године објављене у дневној штампи у виду плаћеног огласа тј. апела властима Србије за одлагањем пројекта док се не спроведе темељна јавна дебата.[19]

Због практичног и историјског значаја овог стручног скупа, тачке Жичког апела су у целини објављене у последњем делу књиге.

4.2.2 Медијски извештаји, публикације, критички текстови и реакције невладиног сектора пре усвајања Закона

Прва критичка публикација на тему биометријских система идентификације и односног пројекта у Србији се појавила у жичкој епархији, већ крајем 2003. године. У питању је била непотписана брошура са насловом „За живот без жига“, чији је аутор, према нашим сазнањима, Владимир Димитријевић, професор књижевности и публициста. Ова брошура је била компилација критичких текстова организације *Privacy International*, академских чланака професора Роцера Кларка, као и неколико закључака наведеног састављача и преводиоца о српском пројекту биометријске идентификације грађана.[20]

Од штампаних медија, критичке текстове је објавило више часописа и дневних новина, но највећи број таквих текстова објављен у *Православљу*, званичним новинама Српске патријаршије, а први текст у НИН-у.[21]

Од представника НВО, прво критичко саопштење дао је директор *Центра за развој интернета,* Слободан Марковић, који је у интервјуу почетком 2004. године рекао да није пружена довољна правна заштита пода-

---

дар Павић, политиколог, један од оснивача НВО „За живот без жига“, Владимир Димитријевић, публициста, Борислав Челиковић, историчар, Оливер Суботић. (списак потписника преузет из Жичког благовесника, спец. јул. издање „*Хроника најављеног слободоубиства*“, 2006).

[19] Оглас је изашао јуна месеца у дневним новинама *Глас јавности*.

[20] Назив брошуре је вероватно настао под утицајем руског друштвеног покрета „За живот без идентификационих бројева“. Њен значај је у чињеници да је то први директни демантиј дезинформација пласираних од стране српског МУП-а и први зборник критичких и стручних текстова на ту тему (додуше, без критичког апарата, што јој оспорава научну вредност у ужем смислу). Иста брошура је нешто касније инкорпорирана у једно поглавље у зборнику текстова под називом „Печат Христов и жиг звери“, у издању Православне мисионарске школе при храму Св. Александра Невског у Београду. Назив ове брошуре је две године касније послужио као инспирација једној групи грађана која је формирала истоимену НВО.

[21] Први критичких текст је „Добар дан, Орвеле!“, објављен у Нин-*у*, 25. 03. 2004. Остали текстови: „Незаконит тендер за опрему МУП-а“, *Блиц*, 30. 09. 2004.; „Електронска идентификациона документа“, *Православље,* 905/2004; „Одговор на дигитални изазов 21. века“, *Православље* 914/2005; „Искушења технологије и тоталитаризма“, *Православље* 940/2006; „Нове личне карте за брзу шпијунажу“, *Српске новине Огледало*, бр. 43; „Електронски конц-логор“, *Геополитика.*

така нити се довољно полемисало у стручној јавности.[22] Прва јавна трибина организована је од стране НВО *Српски сабор Двери*.[23] Остатак НВО сектора се није активно бавио овим питањем, али су постојали гранични примери. Тако, рецимо, НВО *Transparentnost Srbija* није давала своја саопштења, али је на сајту редовно преносила критичке текстове из дневне штампе које су указивале на корупционашке афере у вези са биометријским пројектом.[24]

Непосредно пред доношење закона је публикована и наша књига, у којој се у оквиру неколико текстова даје критика биометријског система идентификације у Србији.[25]

Медијске промоције ставова који су се критички односили према биометријским системима идентификације су углавном игнорисане од стране највећих електронских медија.[26]

4.3 Владина иницијатива за парламентарну процедуру

Пројекат увођења биометријских личних карти у Републици Србији је јединствен пример у Европи, јер је потпуно инвертован начин реализације пројекта у односу на праксе европских земаља. Наиме, свуда у слободном свету о томе се *прво* воде јавне дебате. Потом, уколико постоји подршка стручне јавности и грађана, следи парламентарна дебата. У случају позитивног исхода у парламенту, приступа се тендеру за куповину опреме, после чега (или упоредо) се врши тестирање *потенцијалне* опреме и *тек* онда приступа куповини од стране најповољније понуде.

У Србији је прво купљена опрема (и то кршењем системских закона), потом је тестирана (пошто је купљена) и три године после тога је дошло до парламентарне дебате, да би тек после парламентарног процеса уследила права јавна дебата. Чак и земље у окружењу које по свим параметрима има-

---

[22] Z.Ž., „Sporedni ulazi“, EBIT, бр. 29. Текст је преузет са: http://www.ekonomist.co.yu/magazin/ebit/29/pra/pra2.htm.

[23] Та трибина је одржана децембра месеца 2004. године на Машинском факултету, када је приказан божићни број „Жичког благовесника“, посвећен проблему дигиталних изазова уопште. Учесници трибине били су епископ жички Хрисостом, чија је божићна посланица у потпуности била усмерена ка потреби критичког односа према информационим технологијама, доцент Синиша Влајић (информатички одсек ФОН-а) и Оливер Суботић (испред часописа Православље).

[24] Transparentnost Srbija, нав. чланак.

[25] Оливер Суботић, *Човек и информационе технологије: поглед из православне перспективе*, поглавље „Проблем информационог тоталитаризма“, Православље, Београд, 2006. – Наведено поглавље књиге не поседује критички апарат, што му оспорава научни карактер у ужем смислу, али садржи податке који имају вредност за утврђивање хронологије и начина грађанског отпора.

[26] Представљање специјалног броја Жичког благовесника у *Media centru* (непосредно пред доношење Закона о личној карти), под називом „*Хроника најављеног слободоубиства*“, посвећеног искључиво овој проблематици, је изостало на свим телевизијским медијима. У *Media centru* је тада било неколико телевизијских екипа, али ниједна телевизија није пренела тај материјал, док су остали догађаји из *Media centra* који су се десили истог дана уредно пренети.

ју значајно мањи ниво грађанских слобода су сличне предлоге стављале прво на јавну расправу, после које би следила процедура по закону.[27] Уз то, озбиљне земље које размишљају и о мање захтевним пројектима *обавезно* ангажују домаће информатичке стручњаке у оквиру консултантских група за предлог и анализу, а пројекат се углавном даје домаћим компанијама на развијање, уколико за тако нешто постоје услови.

Пошто због очигледне незаконитости једно време није било речи о пројекту биометријских личних карти, у 2006. години су се опет појавиле најаве да ће грађани Србије ипак добити нову врсту докумената и да ће бити оформљена централна база биометријских података. С тим у вези, 8. јуна 2006. године је покренута парламентарна дебата о предлогу новог закона о личној карти. Министар полиције, Драган Јочић, је у свом образложењу углавном поновио аргументе који су наводили његови претходници из прошлог сазива који су реализовали спорни уговор, додавши још неке специфичности закона.[28] Средства јавног информисања су пренела вест о томе, при чему су се опет појавиле недопустиве дезинформације о земљама које имају биометријске личне карте.[29] Највећа дезинформација је јавности пласирана од стране првог канала државне телевизије,[30] при чему је речено да готово све земље ЕУ имају такве личне карте и да су оне услов за улазак у ЕУ.[31] Сличну дезинформацију су пренеле и неке друге гледане телевизије.[32]

Србија је вероватно једина земља у Европи у којој је поводом пројекта биометријске идентификације изнето толико погрешних информација од стране службеника државних институција, без позива на њихову одговорност и једина земља која је ретроактивно законски регулисала незаконито

---

[27] Црногорска влада је, рецимо, предлог о новим личним картама прво ставила на увид јавности и на јавну расправу, иако тај предлог обухвата мање проблематичних места него у случају Србије. За детаље преузети документ црногорске владе са адресе http://www.gom.cg.yu/files/1103905246.doc.

[28] Сајт Владе Србије, „Јочић образложио Предлог закона о личној карти“. Документ је преузет са адресе; http://www.srbija.sr. gov.yu/vesti/vest.php?id=51662.

[29] Агенција Конекта, „Građani Srbije imaće uskoro elektronska dokumenta“, преузето од *Политике*, 10. јун 2006, аутор Душан Телесковић. Ту је чак наведено да су у развоју ове технологије посебно напредовали Канада и Велика Британија, у којима се и дан данас воде дебате о самом увођењу таквих докумената и где уопште није ни извесно да ли ће систем уопште бити пуштен у погон и заживети. Видети опширније на http://www.konekta. net/sr/index.php?read=13.

[30] У информативном програму од 15.00 часова, дана када је представљен предлог закона у парламенту, новинарка РТС-а је пред министром Јочићем навела да готово све земље ЕУ имају оваква документа и да је њихово увођење један од услова за улазак у ЕУ. Присутни министар није демантовао ту дезинформацију.

[31] Погледати нашу реакцију у тексту „Корак ближе орвеловској Србији“, објављеном у *Православљу*, бр. 942.

[32] B92 је између осталог пренела дезинформацију да електронске личне карте постоје у Хрватској, иако хрватске личне карте имају само машински читљиву зону, без икаквог микрочипа и са регистром који има мање података него у случају Србије. Погледати вест „Elektronske lične karte u Srbiji?“ на адреси: http://www.b92.net/info/vesti/index.php?yyyy=2006&mm=06&dd=09&nav_id=200511.

купљену опрему за биометријску идентификацију грађана – очигледно је да предлог Закона о личној карти (предложен 8. јуна 2006. године српском Парламенту)[33] не би ни постојао да три године раније није купљена прескупа опрема за биометријску идентификацију и то на *незаконит начин*.

4.3.1 Грешке и некритички ставови у образложењу Предлога закона о личној карти

У *образложењу предлога Закона о личној карти* је наведено доста тога нетачног, непрецизног и спорног. Тако је наведено да је интегрисан аутоматизован систем уз помоћ електронских картица заживео у многим државама,[34] поновно је поменута омиљена теза пробиометријских кругова да овакве карте помажу у борби против тероризма,[35] поновљена је еклатантна бесмислица да се оваквим документима врши усклађивање са европским и светским стандардима[36] и слични аргументи који су већ темељно искритиковани у претходним поглављима наше студије. Притом је наведено да је фалсификовање докумената онемогућено,[37] превиђајући чињеницу ко је аутор целокупног система, ком законодавству је подређен и за кога ради сличне системе. Могућност злоупотреба није смањена, како се наводи у образложењу,[38] него, напротив, повећана због чињенице да се прикупља огроман број осетљивих података и смешта у централизовану електронску базу, те да је могућа појава потпуно нових видова криминала. Разлог у виду модернизације рада државних органа, локалне самоуправе и јавних служби[39] свакако не стоји као примарни, јер се продуктивност у том смислу може постићи и без прикупљања биометријских података, односно уз обичне податке о носиоцу у електронском облику, о чему сведочи пракса европских држава које имају изузетно развијен e-governement без икаквих биометријских докумената. Биометријски подаци су у том погледу сувишни и њихово прикупљање нема смисла. Уз то, грађани треба да користе услуге електронске управе без универзалног идентификатора (у Србији то је ЈМБГ), који би омогућио укршање различитих база података.[40] Наиме, уз помоћ локалних идентифика-

---

[33] Предлог закона је био објављен на сајту владе Србије на адреси: http://www.parlament.sr.gov.u/.

[34] *Образложења предлога Закона о личној карти*, страна 11, пасус 5. – У трећем делу наше студије у коме се анализирају имплементације широм света се види да електронске личне карте на обавезујућој основи поседује мали број земаља у свету, а још мањи број поседује електронске личне карте са биометријским подацима, те да их најразвијеније земље света уопште не поседују, ни у каквом облику (*прим. О.С*).

[35] Исто.

[36] Исто, 12, пасус 4.

[37] Исто, пасус 5.

[38] Исто.

[39] Исто, пасус 6.

[40] *LSEIP*, стр. 262.

тора који су различити грађани могу у различитим секторима (здравствени, школски, банкарски) да обављају аутономне радње, што би онемогућило унакрсно повезивање различитих база и профилисање корисника. Нажалост, у Србији још увек постоји пракса да се ЈМБГ користи у многим институцијама као идентификатор у бази, што је проблем за себе који би тек требало изменити прецизном законском регулативом. Паноптички систем идентификације какав се очигледно предлаже у Србији, фактички би онемогућио чување приватности и аутономије грађана у електронским трансакцијама.[41] С тим у вези, одличан контра-пример је четворогодишња e-government стратешка иницијатива француске владе,[42] коју предлагачи закона вероватно нису имали у виду (као ни решења држава каква је Словенија – без електронских личних карти, Финска и и Норвешка – електронске личне карте без биометрије и на добровољној основи, Естонија – електронске личне карте без биометрије). Све ово говори да предлог закона о личној карти није добро промишљен и да не остварује људска права како је наведено,[43] већ их урушава, поготово право на приватност и дигнитет личности, да уноси немир међу грађане својом волунтаристичком позадином, а да потенцијално доноси и безбедносне ризике. Уз чињеницу да предлог закона није садржао прецизне нормативе за случајеве злоупотребе и остале случајеве важне по безбедност података, јасно је да је урађен крајње неозбиљно и површно – укратко, за предлог закона о личној карти у Републици Србији важи комплетна критика која се односи на све некритички имплементиране биометријске системе идентификације.

Међутим, и поред очигледних мањкавости, упозорења једног дела академске јавности и појединих епископија СПЦ, као и директног отпора опозиционих странака, предлог закона је у неизмењеном облику прошао парламентарну процедуру.[44]

4.3.2 Парадокс неадекватног Закона о заштити личних података

Можда највећи парадокс представља чињеница да у Србији пре спорног закона није донет *адекватан* Закон о заштити личних података, тачније није

[41] Исто, 272.

[42] Исто, 273.

[43] *Образложења предлога Закона о личној карти*, пасус 7.

[44] За закон је гласало 120 посланика, док њих 9 није гласало, али су својим присуство омогућили кворум како би закон прошао. За закон су гласали сви присутни посланици ДСС-а, Г17+, и поједини посланици из редова СПО, СПС, НС, СЛПЗ. Против закона су отворено били једино сви посланици СРС, који нису присуствовали гласању. Гласању такође нису присуствовали ни посланици ДС, али је председник Борис Тадић је ставио свој потпис на закон. Занимљиво је да је Триво Инђић, један од саветника председника Србије, јавно изразио негативан став према том пројекту уочи потписивања Закона (на напред наведеном стручном скупу у организацији ДИС-а), али да то није имало утицаја на одлуку председника Тадића да потпише поменути акт.

новелиран постојећи, поготово с обзиром на декларисану политичку конвергенцију владајуће коалиције ка земљама западне демократије (у англофонским земљама то је тзв. *Data Protection Act*), чиме је инверзија законског поступка потпуна. Бесмислено је (а и неозбиљно) доносити *Закон о личној карти* без претходног доношења *адекватног* закона о заштити личних података, који би прецизно обухватио *нове* видове криминалних активности и строго *прецизирао* казнене одредбе и санкционије које би уследиле у оквиру идентификационе политике коју држава спроводи.[45]

Не само да није донет нови Закон о заштити података, него се не примењује ни постојећи Закон о заштити података из 1998. године (у његовом делу о одредбама о правима грађана и коришћењу личних података)[46]. Прикупљање и примена личних података у појединим предузећима и јавним службама је у супротности са поменутим Законом, који предвиђа да се подаци који нису прописани законом могу прикупљати само добровољно и то на основу писмене сагласности грађанина. С тим у вези, крајње је неодређена и опасна конструкција из члана 28. којим се предвиђају услови под којима организације, правна и физичка лица могу имати приступ подацима. Овакви се случајеви морају експлицитно и прецизно нормирати, у смислу конкретних институција и њихових законских ингренеција над базом података, уз стриктне санцкије за неовлашћени приступ. Мора постојати и могућност да појединац зна ко све има или тражи приступ његовим личним подацима.[47]

У Закону о личној карти се, између осталог, предвиђа се да заштитне елементе карте прописује министар,[48] (без икакве независне контроле), иако би то морао да ради неки стручни орган задужен за безбедност података.

Нажалост, волунтаристички пројекти конвалидирани парламентарном процедуром охрабрују и планове приватног сектора, који такође иде некритичком путањом, па не чуди чињеница да у Републици Србији влада потпуни хаос по овом питању. У неколико случајева се узимају биометријски отисци приликом провере идентитета у фирмама, иако радници о томе претходно нису дали своју сагласност, нити су детаљно обавештени, што је директан атак на право на приватност.[49] Још већи проблем је чињеница да руководства тих фирми углавном немају представу о томе шта су права њихових радника из корпуса личноправних овлашћења.[50]

---

[45] Примера ради, чак се и у жестоко критикованом предлогу британске влада ово питање регулисало тако што су прецизирани нови видови криминала и казне за њихове извршиоце. Видети: *LSEIP*, стр. 25.

[46] *Закон о заштити података*, објављен у Службеном листу СРЈ бр. 24 од маја 1998.г. и у броју 26 од исте године фактички постоји, али пракса показује да се он у многим случајевима не примењује.

[47] Исто, стр. 27.

[48] *Предлог закона о личној карти,* члан 8, ст. 2.

[49] Kurir, „Nezakonito uzimanje ličnih podataka u novosadskoj firmi“, 3. 09. 2006.

[50] Исто.

Следујући сличној волунтаристичкој пракси, све више јавних предузећа и организација иде ка пројектима које нарушавају приватност личности. Такав је случај, рецимо, са београдским и новосадским ГСП-ом, који већ планирају увођење новог система идентификације коришћењем комбинације камера, RFID карти и GPS[51] уређаја у аутобусима, са којим ће *у сваком тренутку* у централи ГСП-а имати на располагању прецизан списак свих путника (*именом* и *презименом*) у сваком аутобусу који је на линији.[52]

Ови и слични приступи увођења биометријске идентификације грађана и њима сродних пројеката у Србији су изазвали додатне протесте појединих епархија СПЦ, неколико невладиних организација и одређеног броја академских грађана.

4.4 Стручни скупови и јавне дебате после усвајања Закона о личној карти

Република Србија је јединствен пример у Европи и по инвертованој процедури када је јавна дебата по питању биометријског система идентификације у питању. Тако је и права и континуирана јавна дебата уследила тек након усвајања закона, показујући нерасположење стручне јавности и грађана према овом пројекту и начину његове реализације.

4.4.1 Округли сто у галерији САНУ

Остаће забележено да се јавне дебате са представницима власти пре доношења закона по питању употребе биометријских система идентификације нису водиле у Републици Србији, неким далекоисточним и готово свим блискоисточним земљама. Наиме, први случај да су на једном стручном скупу мишљења и ставове супротставили представници власти и опоненти овог биометријског система десио се *после* изгласавања закона у Парламенту Србије. Та иницијатива је потекла не од стране власти, већ од дела невладиног сектора.

Закон о личној карти је 14. јула 2006. усвојен у Парламенту Србије – да иронија случаја буде већа, истог дана је Савет Европе донео одлуку да се националним законодавствима не могу прописивати стандарди за личне

---

[51] GPS је развила и још увек над њиме има потпуну контролу америчка армија. Погледати о томе: *RSS,* стр. 13.

[52] *Press*, „Veliko oko“, 10. novembar 2006. – У питању је изјава Жељка Ђукановића, директора Дирекције за јавни превоз. Иако би интерактивно праћење *броја* путника у аутобусима помогло за планирање саобраћаја, просто је невероватно да се предлаже могућност увида у прецизан списак путника са њиховим *именима* и *презименима*, у сваком тренутку, с обзиром да то нема апсолутно никаквог утицаја на повећање продуктивности, а представља еклатантно угрожавање права на приватност. Списак путника које ГСП у сваком тренутку вожње сваког возила жели да има сме бити *искључиво* анониман, а у случају да ГСП не одустане од таквог пројекта, треба тражити заштиту од надлежног суда.

карте те да су препоруке тог тела потпуно необавезујуће, што је била додатна потврда тврдњи да биометријске личне карте нису део међународних обавеза. Непосредно пред потписивање парламентарно усвојеног закона од стране председника Бориса Тадића, *Друштво за информатику Србије* је 18. јула 2006. године организовало округли сто у Галерији САНУ, под називом „Да ли електронска карта угрожава приватност грађана". На том округлом столу су усвојене препоруке са којима су се сложили сви учесници скупа, осим једног.[53] Договорено је да се мишљење проследи председнику, влади, Народној скупштини и Министарству унутрашњих послова Републике Србије. Друштво за информатику Србије је дало свој коментар овог скупа,[54] као и сопствене констатације о овој проблематици.[55]

Значај овог скупа је управо у чињеници што је први окупио представнике власти, академских грађана, Цркве и НВО сектора (тј. представнике свих структура у српском друштву које су на позитиван или негативан начин реаговале на биометријски пројекат) ради разрешења ове проблематике. Документ који је упућен са скупа је значајан из разлога што је њиме први пут у јавности стављен нагласак на потребу доношења адекватног закона о заштити података о личности (и личних података), као и што је дао сугестију за добровољно прихватање биметријских личних карти без дискриминације. Овај скуп је значајан и зато што је на њему први пут неко из структура власти отворено критиковао овај пројекат, пре свега из правног аспекта – у питању је генерални инспектор МУП-а, Владимир Божовић.[56]

У неким медијима је нелојално пренета изјава појединих учесника овог скупа, пре свега ђакона Радоша Младеновића, коме је импутиран непосто-

[53] Учесници скупа су били: Драган Максимовић, начелник Управе за информационе технологије и системе МУП-а Србије; Владимир Божовић, генерални инспектор МУП; Протођакон Радош Младеновић, уредник Жичког благовесника; мр Ратимир Дракулић, ФОН; мр Зоран Савић, CoreBioId и NetSet (фирма ангажована као један од подизвођача на пројекту увођења електронских личних карти у Србији); др Триво Инђић, социолог; Александар Трифони, криптолог и Оливер Суботић. Модератор округлог стола и предлагач заједничке платформе скупа био је председник Друштва за информатику Србије, информатички стручњак Никола Марковић. Од заједничке платформе са скупа једини се оградио Драган Максимовић.

[54] „Учесници округлог стола упозоравају, да је суштина проблема са новим личним картама много дубља од информатичких аспеката и указују да постоје информације о пропустима у процедури набавке опреме пре 3 године и да Закон о личним картама покреће пре свега одређена суштинска етичка, морална, филозофска и политичка питања о односу државе и грађана и положају грађана пред опасностима од глобализма и тоталитаризма у савременом свету.
Имајући у виду све изнете чињенице, са скупа је сугерирано свим надлежним органима, да са дужном пажњом размотре изнета мишљења и препоруке, и уз консултације са компетентним институцијама, предложе измене и допуне Закона о личним картама, како би он био у складу са интересима грађана Србије да заштите своју приватност и слободе." Цитат је преузет са сајта Друштва за информатику Србије, на адреси http://www.dis.org.yu/predstojece.htm.

[55] Констатације ДИС-а су објављене у критичком апарату поглавља 4.6 наше студије.

[56] Божовић је пројекат биометријског система идентификације у Републици Србији аргументовано оспорио пре свега из правног и процедуралног аспекта, наводећи притом и нелогичност куповине тако скупе опреме у време када су била потребна велика средства за Фонд за КиМ.

јећи цитат, док главни део његовог излагања (који се односио на тоталитарност концепта централне базе података и закључке Жичког скупа) није ни споменут.[57] То је једина сенка над овим еминентним скупом, чији су закључци у целости објављени у последњем делу књиге.

4.4.2 Стручни скупови у Краљеву и Вршцу

Стручни скуп у Краљеву је одржан 30. 09-1. 10. 2006. године, у Дому владике Николаја, у организацији епархије жичке и са благословом епископа Хрисостома.[58] Учесници скупа су подржали закључке Жичког симпосиона и отворили нове теме. У обраћању јавности са тог скупа наведене су правне и процедуралне мањкавости доношења спорног закона. Као новина је истакнут проблем формирања централне базе здравствених података, као и потенцијалног креирања централне базе школских података, о ђацима и њиховим родитељима. Због ширине закључака овог скупа, исти су у целости објављени у последњем делу књиге.

Стручни скуп у Вршцу је одржан 4. новембра 2006. године, у организацији епархије банатске и са благословом епископа банатског Никанора, у конгресној сали виле „Брег“.[59] На том стручном скупу је учествовао и један стручњак који се залаже за увођење овог система. Значај скупа у Вршцу је у неподељеном мишљењу (како противника тако и пропонената овог система) да је *принцип добровољности* најбоље решење, као и у навођењу неких нових аспеката проблема.[60] Скуп није донео формално обраћање јавности.

---

[57] *Danas* је пренео ауторски текст новинара Ј. Чолак, који наводи да је ђакон Радош Младеновић *најавио* „крваве демонстрације“ (са наводницима), иако реч „крваво“ нигде није фигурирала у његовом излагању. Са друге стране, ђакон Младеновић је говорио превасходно о могућности да *неке* верске заједнице, које *не морају* бити православне, могу организовати јавне верске протесте, за које пракса показује да су далеко жилавији од обичних. Но и то је била само успутна изјава, док је срж излагања ђакона Младеновића која се односила на етичке аспекте целог проблема, тоталитарне премисе концепта централне базе биометријских података и закључке Жичког симпосиона прећутана. С обзиром да смо узели активно учешће на скупу, можемо посведочити о томе, уз напомену да постоји и аудио запис. Нелојално пренета изјава ђакона Младеновића се налази у тексту J. Čolak, „Pretnja religijskim demonstracijama `krvavijim od političkih`“, *Danas,* 20. 07. 2006, на адреси: http://www.danas.co.yu/20060720/hronika2.html. Реакција ђакона Младеновића на ту информацију се може чути на сајту радија *Светигора,* на адреси http://www.svetigora.com/node/320.

[58] Учесници скупа су били проф. др Слободан Антонић (Философски факултет Универзитета у Београду); проф. др Љиљана Чолић (Филолошки факултет Универзитета у Београду); проф. др Светозар Радишић, војни аналитичар и публициста; Александар Трифони, криптолог; протођакон Радош Младеновић, главни и одговорни уредник „Жичког благовесника“; Владимир Димитријевић, члан редакције „Жичког благовесника“; Александар Павић, политиколог и адвокат Драгољуб Ђорђевић, су-оснивачи Н.В.О. „За живот без жига“; Ана Јевремовић, удружење грађана „Српски сабор Двери“; Слађан Мијаљевић, удружење грађана „Истина“; Бранко Радун, политиколог, „Нова српска политичка мисао“ и Оливер Суботић.

[59] На скупу су учешће узели Александар Павић, Слободан Антонић, Светозар Радишић, Владимир Димитријевић, Слађан Мијаљевић, Данило Тврдишић, Никола Марковић, Зоран Савић и Оливер Суботић.

[60] С тим у вези, председник удружења Истина, Слађан Мијаљевић, је први који је направио

4.4.3 Округли сто у Interkontinental-у

У оквиру међународне конференције под називом „Smart e-government 2006, Elektronski identitet i servisi e-Uprave“, одржане 25-26. октобра 2006. у хотелу *Interkontinental* у Београду, одржан је округли сто под називом „Elektronski identitet u e-Upravi i zaštita privatnosti“. На том округлом столу су, на позив организатора,[61] учествовали и неки од критичара биометријског система идентификације у Србији.[62] У дебати са гостима из Естоније, Белгије и САД је утврђено да је концепт електронске управе у потпуности могуће спровести без биометријских података, о чему сведоче искуства поменутих земаља, а било је речи и о (не)поузданости електронских система за гласање широм света. Организатори овог скупа су први пропоненти биометријског система идентификације у Републици Србији који су показали добру вољу за отвореном и аргументованом јавном дебатом. Овај округли сто је од стране Јавног сервиса РТС нелојално медијски покривен, у смислу прећуткивања ставова критички оријентисаних грађана.[63]

4.5 Званична реакција Српске православне цркве

Појединачно, епархије СПЦ су се почеле оглашавати по овом питању готово одмах после спорне куповине опреме и најава имплементације система. Предњачила је епархија жичка, чија је улога у овом погледу историјска, с обзиром да је прва званична реакције једне институције дошла на њену иницијативу, а не од академских кругова или пак невладиног сектора као што је то случај у земљама западне демократије. Ова епархија је учинила много на обавештавању јавности о суштини спорног пројекта, организацијом стручних скупова, обављивањем стручних студија и ставова Синодâ помесних цркава.

Сабор архијереја СПЦ је реаговао после доношења закона, тачније на јесењем заседању 2006. године, када је на иницијативу епископа жичког и после његовог излагања на Сабору то питање темељно размотрено и доне-

корелацију између натписа на карти који су и на енглеском језику (*name, date of birth*..) са SOFA споразумом, који омогућава слободан пролаз јединица НАТО кроз Србију, а чији текст још увек није познат јавности Србије.

[61] Један од организатора скупа била је компанија *NetSet*, подизвођач биометријског пројекта у Републици Србији, чији су представници упутили позив критичарима биометријског концепта да узму учешће у округлом столу.

[62] Александар Трифони, Светозар Радишић, Александар Павић и Оливер Суботић.

[63] У уторак, 21. новембра 2006. у 22:45, овај јавни медијски сервис је емитовао емисију са насловом „Smart-паметно електронско пословање“, у којој су пренете искључиво детаљне изјаве пропонената биометријских система идентификације, представника владе Србије и заступника корпорација које продају smart карте, док ниједна изјава противника биометријског система није пренета (осим констатације на крају прилога да су на округлом столу учествовали и противници пројекта биометријског система идентификације грађана у Србији)

та одлука да се Синод СПЦ обрати властима ради „спречавања ступања закона о личној карти у дело“.[64]

4.6 Критичке реакције НВО сектора после усвајања Закона

После усвајања Закона о биометријским документима у Републици Србији, неколико НВО су биле посебно ангажоване на пољу захтева за преиспитивањем тог решења.

НВО *Српски сабор Двери* је организовала више јавних трибина по том питању, као и највећи протестни скуп.[65] Ова НВО је непосредно по усвајању закона прихватила тачке *Жичкої симпосиона* као своју платформу, а на пољу критичке анализе овог пројекта полазила је пре свега из геополитичког аспекта.[66]

Организација *Transparentnost Srbija* је наставила да преноси критичке извештаје штампаних медија који су се односили на корупцију у вези са спорном куповином опреме и начином доношења закона, али и извештаје са стручних скупова.[67]

Највише стручних извештаја, медијских изјава и ажурних информација дала је НВО *За живот без жига*. Значај ове организације је огроман. Њени чланови су покренули први Интернет сајт посвећен искључиво овој проблематици, који се дневно ажурирао и стајао раме уз раме по квалитету садржаја у односу на сличне светске организације које се боре за електронска права и слободе. Чланови ове организације су учествовали на готово свим трибинама, стручним скуповима и дебатама по овом питању.[68] Ова организација је, такође, као свој званичан став прихватила закључке Жичког симпосиона.

---

[64] Документ је, уз обраћање епископа Хрисостома Сабору поводом те проблематике, објављен у часопису *Жички благовесник,* у новембарском броју 2006. године, на стр. 64 и 65.

[65] Машински факултет, 14. децембар 2006, протестни скуп под називом „За живот без Великог Брата“, на коме су се пред око 700 људи обратили јеромонах Николај (старешина манастира св. Петке), политиколог Александар Павић (испрен НВО За живот без жига), Владимир Божовић (генерални секретар МУП-а), проф. др Коста Чавошки (Правни факултет БУ), проф. др Александар Липковски (Математички факултет БУ), проф. др Светозар Радишић (стручњак за стратешко ратовање), Никола Марковић (председник Друштва за информатику Србије), Александар Трифони (војни криптолог), Милош Кнежевић (геополитиколог и публициста), Слађан Мијаљевић (НВО Истина) и Данило Тврдишић (члан редакције часописа Двери српске).

[66] Превасходно у излагањима економисте Данила Тврдишића, члана тог удружења.

[67] Примера ради, пренос текста о наведеном округлом столу у Галерији САНУ, преузет од Вечерњих новости, на адреси: http://www.transparentnost.org.yu/ts_mediji/stampa/2006/07jul/20072006.html и пренос текста о наведеном стручном симпосиону у Краљеву, преузет од Политике, на адреси http://www.transparentnost.org.yu/ts_mediji/stampa/2006/10oktobar/03102006.html.

[68] Најзапаженија излагања међу члановима ове НВО имао је политиколог Александар Павић, који је први у Србији указао на парламентарна сведочења припадника британских обавештајних служби против централизованих база биометријских података и указао да Србија не треба да следује Западу у свему, а погово не у ономе против чега се на Западу боре сви слободољубиви грађани, већ да Србија има прилику да сама постави стандард у заштити приватности и личности и постане нека врста слободне информационе оазе.

После доношења Закона о личној карти, свој званичан, критички интониран став из правно-техничког аспекта дало је и *Друштво за информатику Србије*.[69]

Директор *Центра за развој Интернета*, Слободан Марковић је, пред саму најаву конкретног пуштања у рад биометријског система, поновио забринутост због великих правно-техничких и безбедносних пропуста.[70]

Најпознатије НВО које својим статутом предвиђају борбу за грађанска права и слободе нису се оглашавале по овом питању, чиме су показале да нису на нивоу светских организација исте провенијенције.

4.7 Реакције критички оријентисаних штампаних медија

Штампани медији су о овој проблематици писали на различите начине и поклањали неједнаку пажњу. Критичке текстове (у неколико бројева) после доношења закона су доносили *Православље*,[71] наставивши са редовним

---

[69] Констатације *Друштва за информатику Србије* (ДИС) о личним картама са биометријским подацима су следеће: 1.Закон о личним картама се у погледу гарантовања уставног права на приватност мора ускладити са начелима за заштиту приватности исказаним у Уставу Србије и директивама ЕУ. Такође пре његове примене неопходно је усвојити нови Закон о заштити података о личности. 2. Примена Закона о личним картама са чипом носи у себи велике ризике у заштити података и опасности од њихове неовлашћене употребе. 3.Средства и методе биометријске идентификације за сада нису са становишта заштите података довољно технички поуздана. Она посебно нису поуздана за борбу против тероризма и криминала, а зашто се наводно и уводе. Зато је неопходно дозволити опционо увођење нових личних карата и дозволити грађанима да не прихвате личну карту са чипом. 4. ДИС подржава увођење е-управе али и указује да за развој е-управе није неопходна биометријска идентификација. Треба подстицати развој е-управе али као вид трансформације управе у сервис грађана који је под непосредном контролом независних тела грађана. Увођење свих база података и апликација и њихово евентуално умрежавање мора да буде критички разматрано са становишта заштите приватности грађана и регулисано законом и контролисано од стране независног органа. 5. ДИС се залаже за примену информационих и комуникационих технологија за подизање квалитета личног живота грађана, заштиту личних права и приватност и никако као технологија за успостављање контроле над грађанима и сузбијање личних права и слобода.

[70] Internodium, blog на адреси: http://www.internodium.org/node/2774. – Слободан Марковић у том тексту, између осталог, наводи: „...Веома забрињава и чињеница да је аспектима приватности и заштите електронских података грађана посвећена неадекватна пажња.То је евидентно како из самог текста закона којим се регулише издавање нових личних докумената, тако из непостојања политичке воље за усвајање закона о заштити података о личности, у складу са европским нормама. Напокон, изјава министра Јочића 'да ће увођење електронске личне карте допринети борби против организованог криминала и тероризма, унапређењу рада државних органа и тачном утврђивању бирачких спискова' апсолутно нема везе са реалношћу. Што се тиче фалсификовања електронских докумената, једино питање је -- са колико нула се то пише. Што се тиче унапређивања рада државних органа, електронске личне карте ће допринети том процесу евентуално једино тако што ће грађане спасити памћења ЈМБГ-а. Што се тиче бирачких спискова, ситуација је потпуно јасна већ годинама -- нити једна влада од 5. октобра до данас није хтела да умрежи системе за вођење бирачких спискова по општинама у јединствени систем...“

[71] „Тражимо алтернативни модел идентификације“, *Православље* бр. 950; „За добровољно узимање електронских личних карти“, *Православље* бр.952; „Црква је бранилац цивилизацијских вредности“, *Православље* бр.953 – Уредништво ових новина се од почетка проблематике залагало за отворену и аргументовану критику пројекта.

критичким текстовима, затим НИН[72] и *Политика*,[73] док су се са интернет текстовима на ову тематику истакли сајтови *Nova srpska politička misao*[74]и *Видовдан*[75] Пренос критичких текстова страних часописа по питању електронских пасоша и централних база података, као и домаће стручне скупове, често је преносио *Danas.*[76] Остали реномирани часописи и интернет сајтови су поклањали знатно мање простора овој теми.[77] Велики одјек су имали и интервјуи са српским информатичким стручњацима, који су излагали критички став према овој проблематици.[78] Новинске агенције су само де-

---

[72] Зора Латиновић, „Чиповање Србије“, НИН 2899; „Приватност на извол’те“, НИН 2900; Интервју са Владимиром Божовићем, генералним инспектором МУП-а Србије (у оквиру antrfilea претходног текста); Јован Јањић „Жиг апокалипсе“, НИН 2901.

[73] Милан Galовић, „Чип задире у приватност“, *Политика*, 10. 6. 2006; Родољуб Шабић , „Опасност злоупотребе“, *Политика*, 10. 08. 2006; Милан Галовић, „ЕУ не тражи чип“, *Политика*, 19. 06. 2006.

[74] На сајту часописа *Нова српска политичка мисао* је током парламентарне дебате, у оквиру рубрике *Полемике*, објављено је неколико квалитетних критичких текстова под посебном темом „Polemika o elektronskim ličnim kartama“ (на адреси: http://www.nspm.org.yu/polemike.htm, под опцијом „Svi tekstovi“): Slobodan Antonić, „U potrazi za srpskim Toroom“; Vasilije Mišković, „Digitalno "žigosanje" građana Srbije“; Aleksandar Pavić, „Vuk na ovcu svoje pravo ima - pogotovu ako je žigosana“. На истом сајту је објављена и наша полемика са Дарком Велимировићем о томе да ли је отпор према увођењу биометријског система идентификације у Србији мотивисан лудизмом или критичким приступом својственим сваком озбиљном интелектуалцу.

[75] Сајт се налази на адреси: www.vidovdan.org. Током парламентарне дебате о предлогу закона о личној карти, на сајту је отворена и до тренутка писања студије активна секција везана искључиво за проблематику биометријских система идентификације. Поред тога сајт је објавио више текстова из ове области и премијерно објавио текст Петра Макаре, под називом: „`Pametna karta` za glupe Srbe“ на адреси: http://www.vidovdan.org/article592.html.

[76] N. M, „Okrugli sto DIS o elektronskoj ličnoj karti i privatnosti građana“, *Danas,* 26. 07. 2006, на адреси: http://www.danas.co.yu/20060726/commedia2.html; AP, „Biometrijski pasoši veliko bacanje para“, *Danas,* 08. 08. 2006, на адреси: http://www.danas.co.yu/20060808/evropa1.html; V. R. , „Hakeri mogu da kloniraju čipove sa ličnim podacima“, *Danas,* 09. 08. 2006, на адреси: http://www.danas.co.yu/20060809/commedia1.html; „Oštri protesti aktivista za građanske slobode“, *Danas,* 23. 08. 2006, на адреси: http://www.danas.co.yu/20060823/evropa1.html; J. Tasić, „Protiv Velikog brata“, 16. 12. 2006, *Danas,* на адреси: http://www.danas.co.yu/20061216/hronika2.html#1. – *Danas* је у највећем броју случајева лојално и критички преносио текстове, вести и догађаје везане за проблематику биометријских система идентификације. Једини крајње нелојално написан текст, према нашим сазнањима, био је „Pretnja religijskim demonstracijama `krvavijim od političkih`“, аутора J. Čolak, на адреси: http://www.danas.co.yu/20060720/hronika2.html.

[77] Zoran Stanojević, „Svi Srbi u jedan folder“, *Vreme* 812; Gordan Brkić, „Stiže biometrijska omča za Srbe?“, *Dnevnik*.

[78] Такав је интервју са Дејаном Николићем, директором београдске канцеларије фирме „F-Secure“, који је први поставио сасвим сувисло питање скривеног малициозног кода (у облику тзв. *root-kit*-а) у софтверу система и рањивости самих полицијских читача. Николић у својим чланцима за конкретан случај Србије наводи да је GPRS систем преноса података, исти који се користи за приступ Интернету у мрежи мобилне телефоније, са безбедносне стране изузетно нестабилан и подложан како циљаним тако и спорадичном компромитовању безбедности корисника. Николић у својим радовима наводи да иако већина напада од стране постојећих облика малициозног кода тренутно иде путем MMS и SMS порука као и *blue-tooth* конекцијом, питање је само избора и умећа нападача да се пребаце на канале комуникације којим би могли да компромитују комуникацију читача података са централном базом. Са друге стране, Николић за конкретан случај Србије наводи да читачи користе оперативни систем *Windows CE*, што је, према овом информатичком стручњаку, са

лом отпратиле догађаје везане за биометријску полемику,[79] али су углавном преносиле наводе МУП-а.[80]

Било је, нажалост, и чланака у којима се ова тематика неозбиљно обрађивала, попут оних у таблоидним[81] или пак бесплатним новинама.[82] Са друге стране, истине ради, треба рећи да су и ти чланци, упркос сензационализму, имали своју улогу у време када је владала огромна медијска блокада свих активности критички оријентисаних грађана, јер су били једни од ретких неконформистичких извора који су давали довољан публицитет тој теми, о којој, по свему судећи, није било ни мало опортуно писати.[83]

безбедносне стране вероватно најбољи избор оперативног система, јер је исти познат по најмањем броју сигурносних пропуста на тржишту и концепцији једноставност, што не иде на руку творцима вируса или малициозног кода са специфичним задацима. Николић даље наводи да је чешка хакерска група *29a* показала да је и то могуће својим експерименталним вирусом *WinCE4.Duts*, проблем настаје у томе што модеран малициозни код коме је намена крађа података и идентитета, не захтева експлоатацију пропуста на локалном компјутеру. На жалост, дневне новине су углавном некомплетно преносиле изјаве овог информатичког стручњака, често стављајући и неодговарајући наслов (с обзиром на право уредника да то учини у складу са својим мишљењем), који је читаоце могао да доведе до забуне и наведе на погрешне закључке. Погледати с тим у вези текст: Sr. Kraljević, „Virus napao ličnu kartu?“, *Вечерње новости*, 5. 09. 2006.

[79] Miloš Milišić, „Podaci za Velikog Brata“, SINA.

[80] Танјуг и ВЕТА су углавном преносили изјаве МУП-а Србије, без преноса медијских извештаја српских организација које су опоненти биометријског система идентификације.

[81] Таблоиди су махом писали да чипови на новим српским личним картама омогућавају перманентно праћење позиције имаоца, што није тачно, јер није у питању бесконтактна технологија. Оно што је могуће је стварање трагова где је појединац и у које време идентификован, на основу чега се може дати само упрошћена шема кретања. Међутим, такве изјаве нису зачуђујуће, с обзиром да српски МУП није желео на време да отвори јавну дебату, после које би јавност имала реалну слику о целом пројекту. Са друге стране, таблоиди су, парадоксално, били једни од ретких штампаних медија који су редовно преносили округле столове и протестне скупове на ову тему. У тренуцима потпуне медијске изопштености критичких ставова, таблоиди су (иако често са дезинформацијама) били једини пут којим су грађани могли да схвате да није све онако како се званично представља. Погледати: A. ME. , „Žigosanje“, Kurir, 09. 06. 2006, на адреси: http://www.kurir-info.co.yu/Arhiva/2006/jun/09/V-09-09062006.shtmlM. M. , „Čipovanje“, Kurir, 16. 12. 2006, на адреси: http://www.kurir-info.co.yu/Arhiva/2006/decembar/16/V-09-16122006.shtml; A. Dragović , „Za život bez žiga“, Press, 13. 12. 2006, на адреси: http://www.pressonline.co.yu/vest.jsp?id=190.

[82] O. Đurić, „Strah od čipa u ličnoj karti“, 24 sata, 9. 11. 2006. – Овај чланак је пун грешака, непрецизности и дезинформација. Новинар наводи да иза једне тврдње стоје *Друштво за информатику Србије* и Галерија САНУ, иако је прва организација била само организатор скупа, док је друго локалитет на коме је скуп одржан. У чланку пише да су „неки појединци“ изјавили како су централне базе поклон за терористе и организовани криминал, а то је део сведочења баронесе Стеле Ремингтон (MI5) и баронесе Дафни Парк (MI6) пред британским парламентом поводом истог питања. Највећу дезинформацију тим поводом у спорном тексту је дао у својој изјави Божо Прелевић, бивши коминистар полиције, тврдећи да су таква упозорења „размишљања малог Перице“, јер су по њему ти подаци постали доступни странцима од тренутка продаје мобилне телефонија и банки, те је (према њему) такве податке много лакше добити преко обичног рачуна за телефон или пак платног списка. То је очит пример мешања атрибутивних и биографских са биометријским подацима, што није појединачан случај у нашој јавности. Нажалост, ово није једини текст са великим бројем дезинформација о овој проблематици.

[83] У том конетксту вреди истаћи таблоид *Kurir*, који је поред мане типично таблоидног начина покривања ове теме у великој мери значајан за пробијање медијске блокаде.

4.8 Критички извештаји електронских медија

За разлику од штампаних медија, електронски медији су мање пажње поклањали овој проблематици, иако је она била тема неколико критичких телевизијских прилога, чак и на јавном медијском сервису РТС.[84] Нажалост, у највећем броју случајева, електронски медији су се ограничили на преношење МУП-ових материјала, док су критички ставови налазили несразмерно мало места. То посебно чуди за телевизије које претендују на аналитичко-критички приступ и које се декларишу као независне и антитоталитарне (В92).[85]

Од радио-станица, једино се *Радио Светигора* активно укључио у критичко преиспитивање концепта биометријских система идентификације у Републици Србији.[86]

4.9 Критичке реакције владиних службеника

Од владиних службеника, прва критичка реакција је дошла од стране генералног инспектора МУП-а Владимира Божовића, на округлом столу одржаном у Галерији САНУ,[87] који је указао на незаконитост самог поступка набавке опреме за нове личне карте, непримереност тренутка њене куповине

---

[84] „Сигнали“, ТВНС1, 8. 8. 2006, у 21:00; „Црвена линија“, РТС2, 26. 10. 2006, у 21:35; ТВ Мост, 21.12. 2006, у 21:00; „Danas“, FOX , 04. 01. 2007, у 19:00.

[85] Иако је донекле синоним за истраживачко новинарство међу електронским медијима, телевизија В92 није ни у једној својој емисији нити на свом сајту дала ниједан критички став по овом питању после усвајања закона, уколико се не рачунају коментари гледалаца. У blog-овима на сајту В92 (попут blog-а Милана Лукића, „Alo, Crkva... “, на адреси: http://blog.b92.net/node/1206) критички ставови Цркве и грађана су отворено исмевани. Са друге стране, ова телевизија која се 90-тих година истицала борбом против тоталитарног режима је (парадоксално) предњачила у учесталости преношења званичних ставова МУП-а по овом и сличним питањима, као и ставовима пробиометријски настројених личности. Једини критички текст под називом „Različito o elektronskim l.k.“, на адреси http://www.b92.net/info/vesti/index.php?yyyy=2006&mm=07&dd=18&nav_category=12&nav_id=205134, није аналитичког типа, већ представља селективни пренос округлог стола у организацији *Друштва за информатику Србије* (пренете изјаве само три учесника скупа, без преноса расправе о суштинској проблематици).
На веома посећеном форуму сајта ове телевизије борцима против некритичког имплементирања овог концепта импутирани су *непостојећи* цитати, док су покушаји оповргавања тих фалсификата завршавали десетогодишњом забраном приступа форуму, што очигледно говори о индиректном учешћу администратора у пробиометријском табору. Погледати о томе тему на форуму В92 под називом „Pravoslavni fundamentalisti i nove tehnologije“, која се се налази на адреси: http://forum.b92.net/index.php?showtopic=29150 и која је у време писања ове студије погледана је преко 20 хиљада пута. Погледати наш одговор на импутиране фалсификате на том форуму и на покушај спречавања њиховог разобличавања, у тексту под називом „Forumom protiv istine“ на на сајту *Нове српске политичке мисли*, на адреси http://www.nspm.org.yu/prenosimo2006/2006_subotic1.htm.

[86] Радио Светигора је допринос дао објављивањем неколико интервјуа по овом питању. Примера ради, разговор са политичким аналитичарем Бранком Радуном, поводом стручном скупа у Краљеву, на адреси: http://www.svetigora.com/node/734; разговор са политикологом Александром Павићем на адреси: http://www.svetigora.com/node/513; разговор са пуковником Светозаром Радишићем, поводом протеста на Машинском факулету, на адреси; http://www.svetigora.com/node/1323;

[87] Погледати о томе у поглављу 4.4.1 наше студије.

(поготово у односу на расположива средства у Фонду за КиМ) као и чињеницу да је његов захтев за покретање истраге о процедуралним и правним пропустима остао без одговора унутар самог МУП-а. Божовић је објавио и неколико реакција путем штампаних медија[88] и учествовао на великом протестном скупу на Машинском факултету, децембра месеца 2006. године.

Друга званична реакција је уследила од стране Родољуба Шабића, повереника за информације.[89]

Трећа (и најблажа) реакција, у смислу тражења оптималног решења, дошла је од стране Чедомира Шуљагића, помоћника министра науке и заштите животне средине.[90]

Безбедност система је оспорена од стране неких бивших службеника државне безбедности,[91] који су потврдили могућност упада страних служби у нашу базу података.

4.10 Реакције пробиометријских интелектуалних кругова

У вези са пројектом биометријског система идентификације постојала је и негативна реакција дела јавности на критику тог пројекта, поготово уколико је критика била у било ком погледу долазила од стране СПЦ.

Први напад је био усмерен на закључке Жичког симпосиона, али не због неке грешке која се у њима налази (до данас се није појавила ни једна институција нити личност која би аргументовано и таксативно оспорила наводе из тачака овог симпосиона – *прим. аут*), колико због чињенице да је Црква та која је реаговала и нагађања мотивације зашто је реаговала.[92] Слична реакција је уследила од стране интелектуалаца познатих по антицрквеном ставу, којима могућност злоупотребе биометријских технологија није била толико битна, колико је за њих била скандалозна чињеница да су први стручни извештаји дошли на иницијативу епархија СПЦ.[93] Заједничка

---

[88] НИН, 2900, 27. 07. 2006, antrfile „Размишљам о грађанској непослушности“.

[89] Родољуб Шабић , „Опасност злоупотребе“. Текст се налази и на сајту НУНС-а, на адреси: http://www.nuns.org.yu/aktivnosti/view.jsp?articleId=6561.

[90] У оквиру текста „Још увек без заштите“ у НИН-у од 19. 10. 2006. на стр. 37 у antrfile-у Шуљагић говори о томе да још нема адекватног *Закона о заштити личних података*, те да о теми биометријских база података треба водити озбиљне разговоре и имплементирати велики степен контроле.

[91] Изјава Божидара Спасића је пренета у листу Курир, од. 17 јула, на стр. 4.

[92] Жарко Корађ, „Pravoslavlje i čipovi“, http://www.nezavisne.com/dnevne/stav/st07182006-01.php. – Текст је, научно гледано, нелојано и претенциозно написан. Од укупно 11 тачака Жичког симпосиона издвојена су само два, док су кључни чланови који се односе на проблем приватности и безбедности података, као и поређења са светском праксом апсолутно прећутани. Жарко Корађ је иначе био један од потпредседника владе када је биометријски систем купљен уз кршење законских процедура.

[93] Теофил Панчић, „Nečastiva lična karta“, Pobjeda, 29. jul. – Панчић у овом тексту не спори могућност злоупотребе биометријских система идентификације, поготово у нашој земљи, али цео текст не усмерава ка критичким опсервацијама на ту тему, већ ка креирању ироничног става због чињенице да је СПЦ прва реаговала, оспоравајући и саму могућност да Црква брани приватност личности.

нит таквим реакцијама је и исмевање или пак наглашавање једне од тачака Жичког симпосиона, која је указивала да продавац система (*Motorola*) има одвојене уговоре са америчким обавештајним службама.[94] На Интернету је такође објављено неколико текстова реактивне природе због чињенице да је Црква прва реаговала на ово питање.[95] То, нажалост, говори да у српском друштву постоје интелектуални кругови који не желе да отворено критикују биометријски концепт само због тога што је Црква прва реаговала и што у томе виде „мешање у политику", не разумевајући заправо природу и позадину њене реакције.[96] Са друге стране, нико од тих интелектуалаца није упутио критику НВО сектору, академским установама и припадницима аналитичког новинарства, зато што нису реаговали пре Цркве.

Од критике нису изузети ни научни радници који су храбро и отворено иступили против овог концепта онако како се он намеће грађанима Србије. Треба, додуше, знати да су и у свету (а не само у Србији) многе научне раднике оптуживали да се критичким односом према биометријским техноло-

---

[94] Критичари закључака Жичког симпосиона су у томе видели или параноју и ксенофобију (подсмешљиво се позивајући на дела Душана Ковачевића) или политички интерес (у смислу утицаја руских обавештајних служби). У оба случаја је у питању класична необавештеност, јер је о тим уговорима са наведеном фирмом својевремено писала светска, али и домаћа стручна штампа, док стручни кругови управо из антлосаксонског света предњаче у могућностима контроле које такви системи пружају обавештајним структурама сопствених земаља. Погледати такав уговор у вести под називом „3D Biometrija", објављену у часопису *Svet kompjutera* 4/2005, на страни 6.

[95] Dušan Darijević, „Žig zveri, paranoja i nešto treće", на адреси http://www.tackacacka.org/ser/vesti/septembar_2006/zigzveri.htm. – У тексту се види антицрквено расположење, јер аутор првенствено наглашава да Црква тиме не треба да се бави, наводећи уз текст једну илустрацију из времена (западне) Инквизиције. Аутор се ниједног тренутка не пита зашто нису реаговале НВО или институције које би по природи ствари требале то да ураде. Са друге стране, аутор отворено признаје правне, процедуралне и безбедносне пропусте овог пројекта, иако не разуме зашто се томе поклања толика пажња.

[96] Многи од њих су се питали зашто се „појединци из Цркве" мешају у ову проблематику? Тачно је да је Црква пре свега литургијски организам, али то не значи да хришћани нису друштвено одговорни, напротив. Чини нам се да се СПЦ огласила овим поводом (и то у сва три структурална чина: епископском, свештеничком и лаичком, а потом и саборно) из више разлога.
Први је, као што то наша студија и показује, због чињенице да пројекат биометријских идентификационих система повезаних са централизованом базом података носи у себи тоталитарне премисе, а Црква се *per se* опире сваком тоталитаризму, јер он утиче на изражавање слободе, као највећег Божијег дара човеку. Други разлог је у чињеници да је овај пројекат узбуркао духове у једном броју верника, који су га директно повезали са Јовановим Откровењем. У томе је било доста претеривања и непотребног страха, чему су наруку ишли таблоиди са текстовима који су носили разне дезинформације које чињенично ипак не стоје. Такви коментари само су правили немир међу верницима и дали могућност антицрквеним круговима да уносе даље смутње. Са друге стране, иако је јасна штетност таквог става, очито је да су овакви пројекти ипак нека врста претече супертоталитаризма о коме говори Св Јован Богослов, те да консеквентном и некритичком применом водећих трендова у информационим технологијама (интеграција и минијатуризација) у једном временском тренутку се заиста можемо наћи у таквом окружењу. Генерално, то се да видети и из синодских докумената Украјинске, Руске, Јеладске цркве као и протата Свете Горе. И на крају, Црква је прва реаговала по овом питању због чињеница да нису реаговали они који по природи ствари то први треба да ураде, а то су најутицајније НВО на овим просторима и академске установе, које су до данас остале неме.

гијама пребацују на политички терен[97] и да им је ту једина мотивација. Зачуђују, међутим, плитки ставови неких интелектуалаца који људе који траже критички однос према биометријским системима идентификације називали лудистима, не схватајући да постоји доктринарна и практична разлика између некритичког модернизма и критичке имплементације информационих технологија.[98]

4.11 Пробиометријска публикација МУП-а

Публикација МУП-а Србије, под називом „Elektronski identitet građana i mogućnosti njegove primene,[99] јавности је приказана после усвајања Закона о личној карти. Написана је далеко озбиљније од претходних саопштења МУП-а пуних дезинформација. Међутим, и она садржи велики број недоречености, омашки и проблематичних ставова, на које ћемо се укратко осврнути.

На почетку наведеног проспекта (на десет страна) се понавља позната аргументација за увођење биометријских система идентификације везана за борбу против криминала, тероризма и злоупотребе идентитета, коју употребљавају апсолутно све владе које уводе овај систем и која је била присутна и у образложењу закона.[100] Наводи се пример случајева крађе идентитета у Америци,[101] али се не наводи да је томе узрок превасходно проширена употреба *Social Security Number*-а, којим се базе лако укрштају и на основу тога и добијају подаци за жељену особу. Даље се наводи да се биометријски идентитет не може фалсификовати,[102] што се може узети само условно а никако ултимативно, јер експерименталне студије показују на који начин је (иако не лако) могуће преварити систем.[103] У проспекту се даље наводи да ће овај систем смањити број злоупотреба,[104] док наша студија показује

[97] Edgar A. Whitley, „Mistaken identity“.

[98] Погледати о томе нашу полемику са Дарком Велимировићем, на сајту „Нове српске политичке мисли (Дарко Велимировић : „Лудизам у Србији“, http://www.nspm.org.yu/koment2006/2006_velim_ludizam.htm; реакција: Оливер Суботић, „Ко је овде луд(иста)?“, http://www.nspm.org.yu/koment2006/2006_subotic_ludizm.htm; одговор на реакцију: Д.В. „О римским гускама, трешњама и још нечему (одговор О.Суботићу) “, http://www.nspm.org.yu/koment2006/2006_velim_guske.htm; „Komentar na odgovor Darka Velimirovića“, на http://www.nspm.org.yu/koment2006/2006_oliver22velim.htm.).

[99] Sunčica Nešić, Vojkan Nikolić, нав. дело.

[100] Критику тог става погледати у поглављима 2.3 и 2.6 наше студије.

[101] Sunčica Nešić, Vojkan Nikolić, нав. дело, стр. 1.

[102] Исто.

[103] Погледати поглавље 2.3 наше студије. – Чак и да је тако како стоји у проспекту МУП-а Србије, особа која жели лажни идентитет може преко корумпираног службеника приликом самог аплицирања за карту оставити потпуно другачије атрибутивне и биографске податке, уз задржавање аутентичне биометрије, чиме пред државом практично добија други идентитет иако биометрија остаје аутентична. Стога је велика мана наведеног проспекта терминолошка недореченост у одређеним случајевима.

[104] Sunčica Nešić, Vojkan Nikolić, нав. дело, 2.

да ће се тај број повећати, како од стране системских радника тако и од нелојалних корисника, те да се могу појавити и нови видови криминала. Чињеница да не постоји адекватан закон о заштити података о личности наш став само потврђује.

Из проспекта се даље закључује да аутори ултимативно повезују концепт електронске управе са физичким идентитетом одређеним уз помоћ биометријског идентификационог документа, који се види као један од неопходних хардверских елемената PKI архитектуре.[105] Међутим, пракса сведочи да велики број земаља за e-government не користи електронске личне карте, а у случајевима где се користе за ту сврху, оне су најчешће без биометрије, једнонаменске и често на добровољној основи.[106] У проспекту се наводи да биометријска smart карта потпуно испуњава услове за e-government,[107] потпуно превиђајући чињеницу да их испуњава и *превише*, јер носи податке (биометријске) који су апсолутно сувишни за такву употребу.

Приметно је да се о концепту вишенаменског документа се у наведеном проспекту говори крајње афирмативно,[108] иако реномиране светске академске институције (попут Лондонске школе економије и политичких наука) у својим студијама јасно показују да је то тоталитаран концепт који има потенцијал да у будућим итерацијама потпуно оголи појединца пред државом, дајући потенцију за унакрсно повезивање разнорнодних база података које су у позадини а самим тим и профилисање грађана.[109]

За биометријске личне карте је потпуно ирелевантан аргумент под називом „међународна примењивост“, [110] јер личне карте се користе на националном а не међународном нивоу (осим у специјалним случајевима, попут путовања кроз Шенген зону *уколико* ималац личне карте жели да је користи као путнички документ – ни тада микрочип није ултимативан, а опционо решење се заснива на бесконтактној, а не контактној технологији) и релевантан је само за путничка документа (што се, истине ради, у наставку текста и даје као пример). ICAO 9303 спецификација се у проспекту прво наводи у реалном контексту (у вези са машински читљивим путничким исправама),[111] док се на крају, у оквиру поднаслова „Наши нови електронски документи“ експлицитно наводи да су *сви* документи (а то per se значи и лична карта) урађени према овом стандарду, што може довести у велику забуну, јер се не даје прецизан податак о томе шта који документ у складу са том

[105] Исто, 3.

[106] Погледати поглавље 2.9 наше студије.

[107] Sunčica Nešić, Vojkan Nikolić, нав. дело.

[108] Исто.

[109] *LSEIP*, стр. 262.

[110] Sunčica Nešić, Vojkan Nikolić, нав. дело, 3.

[111] Исто, 4

спецификацијом испуњава (биометријске личне карте у Србији су рађене у контактној технологији, док поменута спецификација предвиђа бесконтактну). Уз то, поменута спецификација се *уопште* не односи на личне карте (нити пак постоји иједно међународно тело које би прописивало нешто слично националним законодавствима).[112]

Споран је аргумент да су smart карте најраспрострањенија технологија за утврђивање идентитета на свету,[113] осим уколико се не узимају искључиво земље Далеког и Блиског истока. Иако не негирамо да то може бити будуће стање, садашње не говори у прилог те тврдње.[114]

У проспекту се наводе и естетске предности нових докумената, што је аргумент који свакако стоји, као и издржљивост на физичка оштећења. Међутим, ако та издржљивост важи за карту, не важи за сам чип – обична лична карта има валидност и уколико је незнатно оштећена, док оштећења чипа на е-карти аутоматски доводе до престанка његове функције. [115]

Следујући селективном приступу, наводи се да је у Финској електронски ID истовремено и банкарска карта,[116] али није доследно наведено на ком режиму се карте издају у тој земљи (добровољном) и које информације обухватају (без биометрије).[117]

Није јасно који је то „поједностављен поступак у случају квара“, с обзиром да у односу на старе личне карте ништа није имало да се поједностављује у том погледу (нису биле подложне квару нити паду система као нове).[118] Такође није јасно зашто је уопште потребна централна база биометријских података грађана уколико ће идентификација на полицијским пунктовима бити 1:1.[119] То и јесте разлог да се не сложимо са констатацијом да се овим системом обезбеђује тајност, тј. поверљивост и интегритет података, како то стоји у проспекту,[120] пре свега због постојања централне биометријске базе података, која је увек подложна упадима, било споља или изнутра.[121]

Потпуна је бесмислица да је технолошки услов за издавање електронских пасоша као секундарног документа постојање електронске личне карте као примарног,[122] о чему сведочи пракса европских земаља које немају

---

[112] О овој проблематици погледати поглавља 3.2 и 3.2.1 наше студије.

[113] Исто, 6.

[114] Погледати поглавље 3 наше студије.

[115] Sunčica Nešić, Vojkan Nikolić, нав. дело, 6.

[116] Исто.

[117] Погледати поглавље 3.1.2.3 наше студије.

[118] Sunčica Nešić, Vojkan Nikolić, нав. дело, 6.

[119] Исто, 7.

[120] Исто.

[121] Погледати о томе поглавље 2.4 наше студије.

[122] Sunčica Nešić, Vojkan Nikolić, нав. дело, 6.

електронске личне карте, а већ су развиле су електронски пасош.[123] То је једна од крупнијих грешки у наведеном проспекту.

Даље се наводи да су сви документи израђени према директивама међународних тела,[124] не наводећи притом да не постоји ниједно међународно тело које има ингеренције да било којој земљи наметне тип примарног идентификационог документа (личне карте), чиме читалац опет може бити доведен у заблуду.

У закључку овог документа се, између осталог, наводи и чињеница да ће грађани моћи „да купују производе електронским путем без страха од могућих злоупотреба“.[125] С обзиром на насловљеност темата, да ли то значи „и без приватности“ (јер наведени проспект отворено пропагира паноптички систем помоћу вишенаменског идентификационог документа)? На који начин ће бити сачувана приватност грађана код финансијских трансакција, које у већини случајева треба да буду анонимне? На то питање се одговор у овом проспекту не даје. Наводи се само да ће предузећа омогућити радницима обављање послова на удаљеним местима, потпуно сигурна да само они могу приступити одређеним подацима, мада је и то споран закључак, с обзиром да нико не може гарантовати присуство још особа приликом аутентификације идентитета.

Завршна реченица је до те мере идеалистички интонирана да вреди да буде пренета у целини:

> „Брзо ће доћи дан када ће питање поузданог утврђивања идентитета коначно заузети другоразредни значај, али не као неважно, већ стога што ће тај поступак постати јаван и сигуран, тако да ће кривична дела злоупотребе идентитета постати прошлост“.

Овакве изјаве приличе само пропагандном материјалу корпорација које се баве продајом биометријске опреме за идентификацију, али не и стручном проспекту једног озбиљног министарства. Чак ни највећи оптимисти не тврде да ће злоупотреба друштвеног идентитета постати прошлост (чак и британски *Cabinet Office* у закључку своје студије каже да крађа идентитета никада неће моћи у потпуности да се спречи),[126] поготово не коришћењем биометријских технологија идентификације.

Све у свему, ова публикација (као незванични претендент на место најозбиљније студије српског МУП-а по овом питању), иако представља видан напредак у односу на првобитна саопштења односног министарства и даје

[123] Погледати поглавље 3 наше студије у делу који се односи на електронске пасоше.

[124] Sunčica Nešić, Vojkan Nikolić, нав. дело, 8.

[125] Исто, 10.

[126] Cabinet Office UK, нав. дело, стр. 3.

озбиљнији приступ овој проблематици, према нашем мишљењу има доста недостатака, погрешних премиса и ставова, уз очигледан пробиометријски (некритички) став, не може да издржи темељну критику.

4.12 Уредба владе Србије – опционалност микрочипа на обрасцу

Током завршних радова на овој студији (11. јануара 2007) изненада се појавила изјава министра Драгана Јочића коју су пренели сви штампани и електронски медији, да ће у обрасцима за нове личне карте чип бити опционог типа тј. да ће се узимати на потпуно добровољној бази, као и да ће пуштање у погон целог система бити одложено из техничких разлога.[127] У званичном саопштењу на владином сајту стајало је да ће влада тим поводом донети уредбу којом ће Закон практично бити прецизиран.[128] У истом саопштењу је, међутим, стајало да ће се биометријски подаци ипак узимати и није експлицитно наведен став према концепту централне базе података, што је кључни проблем у овом питању. Међутим, и поред тог крупног недостатка, ово саопштење је један од најбитнијих догађаја када су биометриски системи идентификације у Србији у питању, које показује значај борбе грађана који су критички приступали овој проблематици. Највећи број дневних новина је по инерцији само пренео комплетну вест новинске БЕТА, док су, према нашим сазнањима, три дневна листа и два недељника дала критичке текстове непосредно после тог догађаја,[129] а један таблоид пре-

[127] Новинска агенција БЕТА, „Lične karte ipak bez čipa“, 11. 01. 2007. http://www.beta.co.yu/default.asp?m=Vesti%20dana,ves&j=sr&h=Home,sr&prikaz=1566951. У саопштењу ове новинске агенције, између осталог, стоји: „Одредба закона да образац личне карте садржи простор за контактни микроконтролер - чип, изазвала је приликом усвајања закона полемику да ли ће чип са личним подацима моћи да се очита на даљину и да ли ће тиме бити угрожена приватност“. Навод из овог саопштења је у великој мери дезинформација, јер највећи број стручних критика овог пројекта није садржало тврдњу да је могуће даљински пратити имаоца личне карте, управо због чињенице да је у питању контактна технологија. Критички став је био пре свега усмерен на угрожавање права на приватност због скупљања великог броја података од стране управе, превасходно у контексту централне базе података, чија је безбедност такође оспоравана. Микрочип је био споран због начелне нетранспарентности података на њему и иманентности феномена „информационе грудве снега“, као и због чињенице да његова конструкција није била довољно позната јавности. Једна од замерки концепту са микрочипом било је и питање следеће итерације система.

[128] Сајт Владе Србије, „Биометријски чипови неће бити обавезан део нових личних карата“, на адреси http://www.srbija.sr.gov.yu/vesti/vest.php?id=62527.

[129] У питању је чланак Миленка Пешића под називом „Чип није обавезан“, објављен у Политици, у коме аутор критички приступа теми, уз наводе А.Павића и Ђ. Р. Младеновића (чланак се налази на адреси http://www.politika.co.yu/detaljno.php?nid=16941) и текст С. Стаменића, „Lične karte ipak bez čipa“, објављен у новинама Danas, у коме поред критичког приступа аутор консултује по том питању и повереника за информације Родољуба Шабића, (чланак се налази на адреси: http://www.danas.co.yu/20070112/dogadjajdana1.html#0). Оба текста објављена су 12. 1. 2006. Чланци: S. Stamenić, „Utvrditi odgovornost za kupovinu opreme koja godinama stoji po magacinima“, Danas (на адреси http://www.danas.co.yu/20070113/dogadjajdana1.html#2) и Ср. Краљевић, „Чип изгубио битку“, Вечерње новости (на адреси http://www.novosti.co.yu/code/navigate.php?Id=4&status=jedna&vest=98627&datum=2007-01-13), објављени су 13. 01. 2007. Од недељника, критичке

нео и реакције политичарâ.[130] Вест је, у ауторском чланку у Политици, поздравио и Родољуб Шабић, повереник за информације Републике Србије.[131]

Ова вест је имала великог одјека и у светским медијима – тиражни амерички часопис *World Net Daily* је пренео вест о томе како је у Србији грађански сектор успео да примора владу да чип на електронској карти буде опционог типа, правећи паралелу са истом борбом у САД.[132]

Критичари овог пројекта углавном су поздравили изјаву министра Јочића, као знак добре воље владе да изађе у сусрет реалним потребама грађана уз очување њихових права, али су захтевали даље вођење јавних расправа по овом питању, пре свега по питању концепта централне базе података и ЈМБГ-а, као наслеђа тоталитарне комунистичке прошлости.[133]

Уредба Владе Србије је донета у складу са изјавом министра и односи се на опционалност чипа на обрасцу личне карте.[134] Ово је веома битно, јер

текстове су објавили НИН (Јован Јањић, „Грађани без жига“, НИН 2925) и *Vreme* (Zoran Majdin, „Nečastivi u čipu“, Vreme 837). Новинар НИН-а је поздравио уредбу Владе, наводећи закључке стручних скупова у Србији, реакцију СПЦ и критичке текстове FIDIS конзорцијума, док је новинар недељника *Vreme* критиковао власт због неспособности имплементирања система, правдајући донекле предложено решење и не видећи велики проблем у концепту централне базе података, наводећи успут дезинформацију да постојеће полемике нису критиковале концепт додатних података који су се захтевали од грађана (сви наведни стручни скупови одржани на ту тему имали су замерку и на тај аспект).

[130] M. M. - AG, „Lične karte bez čipova!“, Kurir, 12. 1. 2007. на адреси: http://www.kurir-info.co.yu/arhiva/2007/januar/12/V-07-12012007.shtml. – У тексту је пренета и подршка генералног инспектора МУП-а, Владимира Божовића, министру Јочићу на овом потезу и пренет је став СПЦ. У тексту „Veliki brat“ истог таблоида од 15. 01. 2007. наводе се и ставови политичара о добровољности чипа, који су подељени и, што је најзанимљивије, не могу се разврстати према политичкој припадности.

[131] Текст повереника за информације, Родољуб Шабића, „Чип за приговор савести“, објављен у Политици од 13. 01. 2007. због важности и критичких опсервација је пренет у потпуности у последњем делу књиге.

[132] WorldNetDaily, „Public revolt quashes biometric ID chips“, (наднаслов: Life with Big Brother), 27. 01. 2007. Чланак је преузет са адресе: http://wnd.com/news/article.asp?article_id=53945. – Чланак је написан као паралела ситуацији у САД, где се води борба против Real ID Act регулативе. Србија је узета као пример државе у којој је притисак грађана био довољно јак да убеди владу у опционалност чипа на карти. Колико нам је познато, ово је први критички чланак великог публицитета који је објављен на Западу, а тиче се критике биометријског система у Србији. У суштини, текст је прилично добро написан, осим што на неколико места постоје терминолошке омашке и приступ карактеристичан за дневну штампу. То је приметно код навода изјавâ критичарâ овог концепта у Србији, које су у једном делу засигурно преузете из српске штампе. Занимљиво је да се преноси и став аутора ове студије у вези са електронском управом, преузет вероватно из неког одраније објављених интервјуа, мада није наведена кључна замерка коју је смо увек истицали, а то је концепт паноптичког система базираног на вишенаменским документима, јединственом идентификатору и централној бази као тоталитарном супстрату (*прим – О.С*).

[133] Миленко Пешић, нав. чланак.

[134] Владина Уредба о упису података у образац личне карте од 11. јануара под бројем 05 Број: 110-320/2007, на адреси: http://www.srbija.sr.gov.yu/vesti/dokumenti_pregled.php?id=62625 у свом првом члану предвиђа да „Подаци из члана 7. и члана 8. став 1. Закона о личној карти („Службени гласник РС”, број 62/06) уписују се у образац личне карте и у машински читљиву зону на том обрасцу. Само на основу изричите сагласности лица коме се издаје лична карта, у образац личне

се тиме спутава концепт потенцијалног паноптичког система који би могао бити реализован уз употребу вишенаменског документа са јединственим и фиксираним идентификатором (ЈМБГ), а ка коме би овај пројекат вероватно гравитирао у будућности да је остао на обавезујућем виду (узевши у обзир неке од некритичких изјава службеника МУП-а).

Битно је и у смислу да је Влада показала интересовање за потребе и замерке грађана, академске јавности и Цркве, што отвара простор да се будуће иницијативе за изградњу информационог друштва темеље на критичким приступима, у којима ће активно учеше узети наведене структуре друштва, а не само политичке и интересне групације.

Међутим, велики део проблема још увек није решен: проблематичност централне базе биометријских података и сам концепт (удвојеног) ЈМБГ-а са једне стране, а непостојање адекватног закона о заштити података о личности и потреба за независним стручним телом које би пратило рад система са друге, су ставке које се морају узети у критичко разматрање у будућности.

4.13 Србија – уместо закључка

Уместо закључне речи, наводимо наше мишљење о предлогу Закона о личној карти (у парламентарној процедури прихваћеног у неизмењеном облику), које је на захтев Синода СПЦ предато 5. јула 2006. године. Иако је садашња студија по обиму и детаљности неупоредиво већа од оне која је служила као основ за доношење напред наведеног мишљења, закључне тачке обе студије по питању биометријског пројекта у Србији задржавамо готово идентичним. Наравно, места где је у оригиналном документу стајало „Предлог закона“ (с обзиром да је исти тада тек био у парламентарној процедури) у нашој студији ће бити замењено са „Закон“ (с обзиром да је предлог закона прошао парламентарну процедуру у неизмењеном облику). Мање исправке стилског карактера нису посебно назначене, а додатне напомене, коментари, дораде и допуне су посебно назначене у угластим заградама.

> Пре било какве анализе Закона о личној карти, веома је битно нагласити чињеницу да он не би ни постојао да претходно [2003. године] није купљена скупа опрема за биометријску идентификацију и то на **незаконит начин.** Приликом куповине опреме прекршени су Закон о буџетском систему и Закон о јавним набавкама, а уговор о куповини опреме је поред тога садржао и штетне клаузуле по државу. Ово су потврдили и надлежни органи и институције Републике Ср-

карте може да се угради чип који у том случају садржи и податак о пребивалишту и адреси стана лица коме се издаје лична карта.”

бије, најављујући подизање кривичних пријава, што су пренела сва средства информисања. Дакле, пре било какве анализе првенствено је потребно истаћи да Закон о личној карти [у овом облику] постоји да би се оправдала нелегална куповина скупе опреме купљене за време бившег [ДОС] режима.

Друга чињеница коју треба нагласити пре конкретне анализе закона је да је Србија **јединствен пример у свету** да је прво купљена опрема за биометријску идентификацију, да је после куповине тестирана а тек после три године покренута парламентарна процедура. Пракса и логика налажу да целокупан процес буде обрнут, уз додатне напомене да се таква опрема никада не узима само из једне понуде и да се никада не узима пре детаљног тестирања. Наведене чињенице говоре да је у правном смислу пројекат крајње волунтаристичког облика. [Наведено потврђује и чињеница да је права јавна дебата зачета тек после усвајања спорног закона у Парламенту, иако савремена правна начела и елементарна логика налажу да то буде на самом почетку].

Закон о личној карти подразумева узимање **биометријских података** од грађана и стварање **централне базе** биометријских података: дигитализованих отисака прстију *свих* грађана [уз посебне информације потребне за аутоматску обраду], дигитализоване слике лица са фацијалним особеностима и дигитализованим [тј. својеручним] потписом који [могуће] обухвата и динамику), што се види из *члана 8, ст.1*, *члана 10, ст.5* и *чл. 28.*

Закон је проблематичан из правног, безбедносног и етичког аспекта. Додатно може унети конфузију и раздор међу православне хришћане због сличности са симболиком Откровења, што потенцијално отвара и верски проблем.

Поред већ наведеног кршења системских закона и процедура, пројекат увођења биометријског начина идентификације грађана је проблематичан у **правном** смислу, јер се сакупљањем толиког броја осетљивих података директно нарушава право на приватност. Држава огромним кораком проширује количину [ЈМБГ родитеља, рецимо] и тип информација [биометрија у електронском облику] које скупља о грађанима, а да о томе није дата масовна грађанска сагласност. Држава не скупља само податке *о* грађанима, већ у централизовану базу података смешта интимне делове саме личности, који чине њен идентитет. Тиме се нарушавају не само државни закони, већ и међународни акти који се односе на приватност, што показују и студије светски признатих институција и организација [мисле се пре свега на студију LSE – *прим. О.С.*]. Из тог разлога у неким земљама су судски оборени слични пројекти идентификације грађана. Такође, то је разлог да су против оваквих пројеката [у свету] устале најпознатије организације које се боре за људска права, као и престижне академске установе и угледни професори. Проблем у правном смислу представља и чињеница да ће нова лична карта у себи агрегирати податке које њен носилац неће моћи да види, осим преко захтева службеном лицу, што отвара простор за тајне криптоване архиве [имплицирајући феномен „информационе грудве снега“ и неовлашћеног проширивања функционалности електронског дела личне карте].

У **информационо-безбедносном** смислу, Закон о личној карти је вишеструко

споран. Први проблем је сам концепт централ(изова)не базе података, за коју светски признати стручњаци за безбедност и бивши чланови обавештајних агенција тврде да представља поклон за криминалце којима су такви подаци потребни, а који ће лако наћи начин да их прекопирају [или модификују]. У наведену базу података би се сместили биометријски подаци који су по природи веома осетљиви и непромењиви до краја живота. Уколико се човеку једном украду биометријски подаци из такве базе, он је практично покраден за цео живот. Као сведочанство томе треба рећи да су само у последњих неколико година документоване крађе информација о милионима грађана чији су подаци били у најстроже чуваним базама. Поред криминалних група, централна база биометријских података ће бити веома примамљива и за западне обавештајне службе (пре свега CIA), са којима фирма која је продала Србији систем за биометријску идентификацију има посебне уговоре [иако је овај аргумент током парламентарне и стручне дебате исмејан од стране пропонената биометријског система идентификације у Србији, он је базиран *искључиво* на јавно доступним информацијама о уговорима у чланцима из домаћих и страних стручних часописа]. Апсолутно *нико* не може гарантовати да неће бити тзв. „цурења података“ у том смислу, што је пракса више пута показала. Посебан проблем представља чињеница да у Србији још увек не постоји прецизна и адекватна легислатива по питању [оваквих] електронских база података у државним службама [јер постојећа легислатива из 1998. није адекватна]. То отвара широке могућности за продају делова базе трећим лицима од стране корумпираних службеника [и потпуно нове видове криминала]. Пошто је [биометријска] база централизована, најосетљивији подаци о свакој личности се могу веома брзо извући, што до сада није био случај, јер база нити је била централизована нити је садржала биометријске податке [реч је о електронској бази података коју је МУП до сада водио, која у себи није укључивала биометријске податке – *прим. О.С*]. Закон о личној карти (*чл. 8 ст. 2*) предвиђа да заштитне елементе карте прописује министар, иако би то морао да ради неки стручни орган задужен за безбедност података [и надзор рада и коришћења система], што додатно говори о неозбиљности целокупног предлога и пројекта.

У **етичком** смислу пројекат је проблематичан јер многе људе подсећа на својеврсан електронски конц-логор, због опсега информација које се узимају и начина идентификације особа. Посебан проблем је што мислећи људи широм света осећају да је ово само увертира у много тоталитарније концепт државног надзора, који се у будућности може спровести интеграцијом свих личних докумената у једном [што је први следећи корак уколико се буде инсистирало на вишенаменском концепту докумената] и ликвидацијом папирног новца (чиме би се у једном временском тренутку потпуно укинула анонимност токова новца).

У **верском** смислу, приметно је према написима из дневне штампе да Закон о личној карти уноси немир међу хришћане свих деноминација, јер их подсећа на лагано остваривање прогноза о тоталитарном режиму описаном у Јовановом

Откровењу. То може довести до велике подвојености међу православним хришћанима који би имали различит став по овом питању. Најгоре од свега је што злонамерни људи могу покушати са уношењем раскола.

У **образложењу** предлога Закона о личној карти је наведено доста тога нетачног или спорног.

На *стр. 11* (*пасус 5*) стоји да је интегрисан аутоматизован систем уз помоћ електронских картица заживео у многим државама. Пуна истина је да електронске личне карте на обавезујућој основи поседује мали број земаља у свету, а још мањи број поседује електронске личне карте са биометријским подацима. Личне карте какве се предлажу предлогом Закона (биометријске smart карте) поседује свега неколико земаља у свету, и то углавном далекоисточних [и блискоисточних]. Најразвијеније земље света их не поседују, чак ни у најосновнијем облику [осим у секторском погледу, када не представљају идентификациони документ].

Није истина да овакве карте помажу у борби против тероризма, као што се наводи у образложењу предлога (исти пасус). То потврђују светски признати стручњаци за безбедност и шпијунажу, па чак и неки предлагачи сличних закона, попут британског министра унутрашњих послова [који је потврдио да оне не би помогле спречавању терористичког напада у Лондону 2005. године].

Није истина да се оваквим документима врши усклађивање са европским и светским стандардима (*стр. 12, пасус 4*). Највећи број земаља ЕУ не поседује овакве личне карте, а неке их не поседују уопште [нити постоји било које наддржавно тело које има ингеренције да формира и наметне стандард за личне карте било којој земљи]. Оне нису услов за улазак у ЕУ, о чему сведочи пример Словеније која их пре уласка није увела и која поседује обичне пластифициране карте са механизмима који омогућавају виши ниво заштите документа од фалсификовања, а без smart чипа са биометријским подацима.

Фалсификовање докумената (*стр 12, пасус 5*) је омогућено пре свега због чињенице да *Motorola* ради сличне системе за америчку војску и централнообавештајну агенцију, а одговара америчком националном законодавству. Могућност злоупотреба (*стр 12, пасус 5*) није смањена, него, напротив, повећана због чињенице да се прикупља огроман број осетљивих података и смешта у централизовану дигиталну базу, из које се подаци могу тренутно копирати и укрштати.

Разлог у виду модернизације рада државних органа, локалне самоуправе и јавних служби (*стр 12, пасус 6*) не стоји, јер се продуктивност у том смислу може постићи и без прикупљања биометријских података, односно уз обичне податке о носиоцу у електронском облику [и уз помоћ других концепата: без електронских личних карти, а ако се користе smart карте, онда помоћу једнонаменског концепта]. Биометријски подаци су у том погледу сувишни и њихово прикупљање нема смисла [док предложено решење води ка паноптичком систему, омогућеном концептом вишенаменског документа, универзалним идентификатором и једном централном базом података, што је све заједно погубно по приватност].

Предлог закона не остварује људска права како је наведено (*стр 12, пасус 7*), већ их урушава, поготово право на приватност и дигнитет личности.

Овакве личне карте нису најпоузданије средство за идентификацију (*стр 12, пасус 8*) [уколико контекст поузданости посматрамо двосмерно, узимајући у обзир и имаоца исправе], о чему говоре и студије познатих институција које се баве овим проблемом [FIDIS то тврди поготово када је у питању бесконтактна технологија, док је контактна технологија, истини за вољу, ипак доста поузданија када је реч о чувању података, који су сигурни док карта није у читачу, али пати од проблема потенцијалног „цурења“ података приликом њеног читања, поготово у случају шема које нису јавно доступне – *прим. О.С*].

На *стр. 14*, у претпоследњем пасусу стоји да се биометријски идентитет не може фалсификовати нити копирати, што стоји само у односу на његовог имаоца, који је доживотно покраден уколико неко успе да извуче његове податке из биометријске базе државних органа.

Узевши у обзир правне, информационо-безбедоносне, етичке и верске проблеме, од државне управе је неопходно захтевати могућност алтернативе, у виду слободног избора замене старих докумената [ово је суштински, нанешто другачији начин, решено Уредбом о опционалности чипа на обрасцу – *прим. О.С*] односно давања биометријских података на добровољној основи [што тек треба разматрати]. У случају негативног одговора државне управе на апел грађана за приговор савести, због очите незаконитости пројекта [од самог почетка] упутно је његово оспоравање на нивоу Врховне судске инстанце [најупутније на нивоу Уставног суда, чији је рад за време писања студије био блокиран, што је био случај и после доношења Закона о личној карти].

Оно што би могло да се овом незнатно измењеном и допуњеном првобитном закључку урађеном на захтев Синода СПЦ, јесте да је доношењем новог Устава отворен широк простор за оцену уставности закона и његовог усаглашавања са највишим државним законским актом. Уз то, треба рећи да реакција владе у виду Уредбе која је уследила током завршавања наше студије даје охрабрење да ће критички приступ овој проблематици у Србији бити реалност, те да ће Србија постати пример земље у којој су се грађани ипак питали за решење које им одговара, а управа се оријентисала према препорукама стручне јавности. Уколико у Републици Србији по питању имплементације овог система кључну реч буду имали грађани и научни радници, то ће бити пример како је могуће од једног крајње волунтаристичког пројекта који је конвергирао типичном етатизму доћи до критичке имплементације урађене уз поштовање грађанских и академских права и слобода.

Закључци и препоруке

1. Биометријске системе идентификације превасходно треба проучавати у контексту њихових друштвених импликација, а не само кроз питања техничке изводљивости и примењивости. То подразумева мултидисциплинаран приступ који пре свега обухвата етичке, информатичке, правне и социолошке дисциплине. Сваки редукционизам и свођење ове проблематике на само један од наведених аспеката не доноси добре резултати и води ка погрешним закључцима који могу имати далекосежне последице.

2. Имплементација биометријских система идентификације на бази политичког волунтаризма, без критичког става и ван академске расправе је недопустива. Политичке структуре најчешће имају мало знања из ове области и ослањају се углавном на проспекте биометријских корпорација, притом често улазећи и у конфликт интереса. Ниједно слободно друштво не сме дозволити да се питања идентификационог менаџмента решавају превасходно у политичким и/или интересним круговима, већ иницијатива и предложена решења првенствено морају долазити од стране стручних и научних институција из релевантних области. Поред стручних и научних препорука, потребно је уважити и став грађана – уколико не постоји шира подршка грађана биометријском систему идентификације, исти не треба ни имплементирати.

3. Дневна штампа у великом броју случајева површном обрадом ове проблематике, дезинформацијама и сензационалистичким приступом отежава напор научних радника и стручњака да ову тему приближе грађанима на адекватан начин, зарад стварања што објективније представе. Стога су јавни стручни скупови, округли столови и расправе од виталног значаја по овом питању. Они морају бити одржани пре било какве имплементације биометријских система идентификације на ширем плану, јер у супротном губе свој смисао и постају формално покриће за пројекте базиране на некритичком и политички вођеном приступу.

4. Аутоматска обрада биометријских података представља једну од кључних особина савремених биометријских система идентификације. Рудиментарне методе биометријске идентификације јесу историјске претече ових система, али се не могу се са њима поистоветити управо због недо-

статка аутоматске обраде података. Поистовећивање биометријских података на електронским и неелектронским носиоцима није правилно због разлика у детаљности, брзини обраде, опсега тренутног преузимања података и могућностима директног укрштања. Иако се сматра да су савремени аутоматизовани биометријски системи непогрешиви, то теорија и пракса демантују и недвосмислено их категоризују у пробабилистички корпус.

5. Не сме се допустити укидање концепта анонимности у случајевима где га је могуће очувати. У случајевима где је биометрија сувишна, као код имплементирања електронске управе, не треба је ни инкорпорирати јер се тиме биометријски систем идентификације уводи на нелојалан начин. Технологија сама по себи не сме бити циљ, већ искључиво средство и мора бити одмеравана општеприхваћеним етичким постулатима. У случају колизије технолошких решења и правно-цивилизацијских норми, предност увек треба да је на страни ових других, што је принцип који треба применити и на биометријске системе идентификације.

6. Захтеви научних кругова да се уведе мораторијумом над широм применом биометријских система идентификације све док се темељно не испитају постојећи правно-технички механизми безбедног коришћења је реалан и сврсисходан. Но пре тога је потребно извршити темељно истраживање о томе да ли биометријски системи идентификације уопште мењају природу политике у конкретном друштву, да ли нарушавају однос између државе и појединца и да ли конкретна имплементација отвара тоталитарне премисе за будућност. Приступи који су нисходни и крећу од техничке имплементације идентификационог решења без уважавања темељних постулата на којима свако друштво почива воде ка лаганом преобликовању и урушавању његових освновних етичких норми.

7. Проблеми различите природе који искрсавају приликом некритичке имплементације биометријских система идентификације не могу се решавати саморегулативним методама. Проблемима етичког, безбедносног и правног карактера мора се темељно и критички приступати и они се морају решити пре конкретне имплементације система. У случајевима доказане незаконитости пројекта не сме се допустити принцип конвалидације.

8. Увек треба давати предност решењима на добровољној основи, уколико је то могуће. У том случају је обавезно строго и прецизно санкционисање потенцијалне дискриминације. Приметно је да политичке структуре углавном форсирају употребу биометријских система идентификације на ширем плану у ултимативном и инвазивном погледу, правдајући се најчешће борбом против тероризма и организованог криминала, као и модернизацијом управе. Такви аргументи немају реално упориште и не могу издржати темељну критику.

9. Било каква имплементација у приватном сектору мора бити у складу са законским нормама о заштити личних података и података о личности. Уколико те норме не постоје, биометријске системе идентификације треба забранити у приватном сектору пре доношења прецизне легислативе која би их регулисала. С тим у вези, закони о заштити података о личности и личних података морају бити прецизно нормирани, посебно у делу који се односи на прецизирање нових видова криминалних активности и њихово конкретно санкционисање.

10. Концепт централне базе биометријских и њима придружених података има потенцијал за актуелизацију информационо контролисаног друштва. Иако у перцепцији просечног грађанина проблематичан може бити само уређај на коме се биометрија налази (smart картица или нешто друго), у етичком, правном и информационом смислу највећи проблем представља централна база биометријских података, која временом може да прерасте у тоталитарни паноптички супстрат уколико постоји могућност укрштања са осталим базама. Укрштање разнородних база податка је могуће на више начина, али у пракси се своди на коришћење универзалног алфанумеричког идентификатора. Због повећања концентрације моћи полицијског апарата, рањивости централне базе споља и изнутра и њене потентности за развој информационо контролисаног друштва, принцип централ(изов)ане базе биометријских и (укрштањем) придружених података представља насртај на концепт слободног друштва и треба га недвосмислено оспорити.

11. Будуће итерације некритичких имплементација биометријских система идентификације очито конвергирају ка друштву тоталног надзора и контроли свих трансакција. Наиме, проблематични аспект tokena, тј. уређаја на коме је смештена биометрија, није везан за његову садашњу имплементацију у виду једнонаменских smart карти, већ за концепт вишенаменског документа и евентуалну будућу имплементацију у виду биочипа (имплантата), што је огромном броју људи данас апсолутно неприхватљиво. Концепт биочипа је посебно неприхватљив у срединама са већински хришћанским становништвом, због конотација које такав развој догађаја доноси у поређењу са Јовановим Откровењем и чињеницом да би неслагања по том питању интересне групе могле да искористе за увођење раскола међу неистомишљенике и немира међу вернике.

12. Историјски гледано, у слободним земљама је притисак политичких структура за некритичку имплементацију биометријских система идентификације довео до реакција академских институција и научних кругова, мислеће јавности и НВО сектора који се бори за очување права на приватност. У земљама са већински православним становништвом активан отпор некритичкој имплементацији биометријских система дала је и Православна

Црква. Највећи отпор је приметан у земљама обичајног права, док је најмањи отпор приметан код блискоисточних и далекоисточних земаља. Постоје случајеви земаља где су некритички концепти оборени на судским инстанцама, одбијени у парламентарним заседањима, повучени под притиском јавности или пак компромитовани безбедносним пропустима. Постоје и примери земаља са високим нивоом грађанске свести и економских стандарда у којима се овакви системи користе на добровољној основи.

13. Да би се имплементације биометријских система у свету реално сагледале, потребно је познавати историјску позадину сваке земље и њен социолошки миље, те извлачити закључак за сваки појединачни случај. Уз то, потребно је правити разлику између различитих имплементација, типа документа, постојању односно непостојању централне базе података, интероперабилности и опсегу биометријских података који се предлаже за узимање. Апсолутно је неприхватљиво извлачење једнозначних закључака на основну различитих типова имплементације.

14. Државни пројекат биометријског система идентификације грађана у Републици Србији, јавности представљен 2003. и озакоњен 2006. године, представља класичну матрицу примењеног волунтаризма у области идентификационог менаџмента, у којој се биометријски систем за идентификацију купује и инсталира пре било какве јавне и парламентарне дебате, уз кршење системских закона приликом куповине опреме, да би потом уследила својеврсна конвалидација спорног уговора. Република Србија је тиме постала парадигма некритичког увођења биометријског система идентификације у свету и пример политички вођеног пројекта који је у колизији са свим наведеним тачкама из закључка ове студије. Са друге стране, антиномија случаја Републике Србије се огледа у историјској потврди да грађански отпор потпомогнут угледним институцијама може довести до накнадног преусмеравања сличног пројекта на добровољну основу (у одређеној мери), чиме наша земља спада у малобројни круг слободних земаља таквог искуства, али не у потпуности – због задржаног концепта јединственог (сада удвојеног) идентификатора и централне базе биометријских података.

15. У случају како Републике Србије тако и остатка слободног света, од примарног је значаја принципијелно очување темељних слобода на којима савремено друштво стоји, уз активно укључивање релевантних научних и стручних институција у плодну дебату која би дала финалне смернице за критичку имплементацију, уз обавезно уважавање става шире јавности. Приступи базирани на политичком волунтаризму и некритичком модернизму воде искључиво ка нимало светлој етатистичкој будућности.

Додатак А

Критички гласови из света

Роџер Кларк

Електронска идентификациона документа: обећања и опасности

(закључно поглавље)

...Ова последња секција* идентификује одређене карактеристике у дизајну које би требало да буду усвојене од стране оних који примењују чип технологију у идентификационе сврхе:

– идентификовани трагови трансакције морају бити ограничени на околности у којима су оправдани због непостојања алтернатива;

– да би се постигла равнотежа међу сукобљеним интересима, мора се много више примењивати псеудонимност, нарочито кроз заштићене индексе;

– аутентификација идентитета мора се користити **само** тамо где је формално потребна и мора се много више примењивати довољна (обична) аутентификација;

– **мора** се користити више једнонаменских идентификатора, а не један вишенаменски;

– веома важна последица принципа „више идентификатора“ је одржавање раздвојености између примене у оквиру вишефункционалних чипова, да би се утврдила целовитост примене и заштита против неауторизованог одавања података и идентификатора;

– још једна битна примена принципа „више идентификатора“ је увођење „role ids“-а и „person ids“-а, да би се показала чињеница да особа врши више улога у исто време или да више особа обавља исту организациону функцију.

---

* Превод текста је преузет из часописа *Жички благовесник* (званичног гласила епархије жичке), специјално издање под називом „Хроника најављеног слободоубиства“, јул 2006, стр. 48. Оригинални текст: Roger Clarke, „Chip-Based ID: Promise and Peril“, верзија од 27. септембра 1997, налази се на адреси: http://www.anu.edu.au/people/Roger.Clarke/DV/IDCards97.html. – Проф. др Роџер Кларк је један од највећих светских стручњака из области информационе инфраструктуре, електронске приватности и електронског пословања. Активан је у области информационих технологија више од 35 година. Редовни је професор на Аустралијском националном универзитету (Одсек за компјутерске науке) и гостујући професор на више светских факултета. Један је од покретача Аустралијске фондације за приватност (*Australian Privacy Foundation*) која слави 20 година постојања. На адреси http://www.anu.edu.au/people/Roger.Clarke/ је постављено преко 1000 његових чланака из различитих информационих области, док је његов академски профил доступан на адреси: http://www.anu.edu.au/people/Roger.Clarke/AcademicCV.pdf.

Други опсег потреба повезан је са омогућавањем појединцу да има озбиљну контролу над процесима који укључују картице базиране на чиповима:

– власништво картице мора бити у рукама личности, а не државе;

– дизајн идентификационих шема базираних на чиповима **мора бити јасан појединцу**;

– издавање и конфигурација картице **морају** бити плод конкуренције више фирми, укључујући и корпорације приватног сектора, у сарадњи са представни цима јавних интереса;

– приватни кључеви који се различито користе за шифровање поруке и за електронске потписе могу бити смештени у истој картици, али се **не сме дозволити развијање централне базе приватних кључева**;

– **контрола биометрије особе мора бити у рукама особе, а не државе**. Према томе, **не сме се дозволити смештање биометрије у јединствену државну базу података**.

Ове карактеристике дизајна стварају додатне изазове за организације које планирају употребу чипова као основу за идентификациону шему. Али оне представљају основу по којој организације могу легитимно остварити своје циљеве, док грађани могу бити уверени да шеме неће претерано угрозити њихову приватност.

Џулијан Ешбурн

Развејавање популарних митова о биометријској технологији
(извод)

1. Биометрија доказује да сте ви она особа која тврдите да јесте.* *Нетачно*. Биометрија не ради ништа слично, она једноставно пружа већу поузданост подударности индивидуе са претходно дефинисаним идентификационим профилом. Друга је ствар да ли је тај профил тачан или да ли је накнадно измењен.

2. Тест биометријске идентификације је непогрешив. *Нетачно*. Технологија је увек подложна грешкама, а биометријска технологија не представља никакав изузетак. Штавише, још увек не постоји опште разумевање за сијасет разлога за могуће неуспехе у процесима биометријског проверавања идентитета.

3. Биометрија доприноси приватности. *Нетачно*. Сама по себи, биометрија нити повећава нити угрожава приватност. Ради се о начину њене употребе у контексту дефинисане техничке архитектуре и оперативног процеса.

4. Биометријски подаци не могу да буду украдени. *Нетачно*. Биометријски подаци се врло лако могу украсти. Главно питање је за које све сврхе се они могу користити у случају крађе.

5. Биометрија не може да открије личне информације. *Нетачно*. Личне информације се могу извући из самих биометријских података, као и из података који су са њима повезани. Ово друго је потенцијално комплекснији проблем, с обзиром на могућност да се са тим подацима манипулисало или да су проширени без знања или одобрења личности на коју се односе.

6. Електронски чипови су по својој природи безбедни. *Нетачно*. Чип је обичан механизам за складиштење података. Релативна безбедност тих података зависи од комбинације технолошке контроле и оперативног процеса.

---

* Оригинални текст под насловом *The Societal Implications of the Wide Scale Introduction of Biometrics and Identity Management*) представљен је на конференцији Euroscience Open Forum ESOF 2006, одржаној у Минхену, јула 2006. године. Тај материјал је коришћен у нашој студији као једна од референци. Џулијан Ешбурн (Julian Ashbourn) је председник Међународне биометријске фондације (*International Biometric Foundation*) и аутор више књига, студија и чланака из области инентификационог менаџмента и биометријских система идентификације. Први је направио биометријски софтвер за 32-битну *Windows* платформу. Живи и ради у Енглеској.

7. Складиштени биометријски подаци нису подложни манипулацији. *Нетачно*. Складиштени биометријски подаци могу бити предмет разних врста манипулације.

8. Модерна технологија за базе података је сама по себи безбедна. *Нетачно*. Безбедност складиштених података зависи од многих чинилаца али, сама по себи, база података не мора аутоматски да буде и безбедна. Штавише, може постати веома небезбедна као последица неадекватне контроле, непромишљеног повезивања са другим изворима података, лоше политике и неразумевања основа ИТ технологије и праксе уопште.

Превод: Александар Павић

FIDIS

Будимпештанска декларација о машински читљивим путним исправама

Abstract. Због тога што нису увеле одговарајућу безбедносну архитектуру, европске владе су фактички приморале грађане да прихвате нове међународне Машински читљиве путне исправе (*Machine Readable Travel Documents* - MRTD) које драматично смањују њихову безбедност и приватност, а повећавају ризике крађе идентитета.* Једноставно речено, садашње увођење Европског (биометријског) пасоша ради се уз помоћ технологија и стандарда који су лоше прилагођени својој намени. У овој декларацији, истраживачи у домену идентитета и идентификационог менаџмента (уз подршку једногласне иницијативе изнете током скупа Мреже FIDIS (*Future of Identity in the Information Society*) одржаног септембра 2006. у Будимпешти, сажели су своје налазе засноване на анализи MRTD-а и препоручили конкретне мере које заинтересовани у владама и индустрији треба да примене како би ублажили постојеће проблеме.

Увод

Мада су већ сада подложне већ добро познатим сценаријима злоупотребе идентификационих докумената, нови MRTD-ови подложни су додатним претњама, међу којима подвлачимо следеће:

– Насупрот традиционалним идентификационим документима, подаци са европских MRTD-ова су даљински, транспарентно и не-интерактивно читљиви (са становишта носиоца документа) са раздаљине од 2 до 10 метара. Ове слабости су појачане мерама контроле приступа које су подложне заобилажењу или хаковању (носећи ризик сталне, непримећене аутентификације података на MRTD од стране ауторизованих и неауторизованих трећих лица, омогућавајући праћење људи који носе пасоше, на пример у својству туриста у страним земљама).

* Оригинални документ под називом „Budapest Declaration on Machine Readable Travel Documents (MRTDs)“ се налази на адреси http://www.fidis.net/fileadmin/fidis/press/budapest_declaration_on_MRTD.en.20061106.pdf . – FIDIS је стручно тело које има подршку ЕУ. Његов конзорцијум чини десет европских универзитета, три института, више установа истраживачког карактера и представници највећих светских информационих компанија.

– Употреба биометријских података на идентификационим документима је подложна експлоатацији од стране јавних и приватних сектора за додатне сврхе – што представља кршење европских принципа приватности. Штавише, сама биометрија је заснована на вероватноћама, што значи да су лажно-позитивне и негативне аутентификације неминовне и потенцијално могу да утичу на свакодневни живот многих европских грађана. На основу међународних техничких (ICAO – Међународна организација за цивилни авио-саобраћај) стандарда дефинисаних у документу 9303 и пратећи Правило ЕС 2252/2004 [5] европског законодавства, увођење Европског пасоша (тзв. „epass“) као међународног MRTD-а почело је 2005. Овај позициони папир је заснован на анализи правних основа за увођење MRTD-а, технологије која се употребљава и спровођењу мера заштите података и безбедности. Ова анализа је урађена од стране FIDIS-а и документована у FIDIS-овој „Студији о идентификационим исправама“. Такође је, у састављању овог позиционог папира, коришћен и следећи материјал: – Заштитни профили за механизме биометријске верификације и MRTD, укључујући и Основну контролу приступа (BAC – „Basic Access Control“), одобрени од стране немачког Савезног уреда за информативну безбедност (BSI), Техничко упутство V1.0 за Проширену контролу приступа („Extended Access Control“), издато од стране немачког Савезног уреда за информативну безбедност (BSI) у августу 2006.

Сажетак налаза

Ни широј јавности ни заинтересованим стручњацима није представљен никакав кохерентан, интегрисан концепт безбедности за MRTD. Јавно доступни документи, као што су Заштитни профили и Техничка упутства покривају само делове таквог једног безбедносног концепта. BAC је на почетку представљен као једна ефектна мера контроле приступа, док је у нешто скорије време EAC представљен као ојачана верзија истог. Међутим, обе мере су једноставно недовољне (као мере контроле приступа на располагању самом имаоцу документа) у многим ситуацијама. Већи број теоријски и научно доказаних претњи и концептуалних слабости MRTD-ова већ је објављен. Оне још увек нису обухваћене Заштитним профилима, техничким упутсвима и стандардима или постојећим применама.

Међу најзначајнијим претњама су следеће:

– За сада нема могућности да се биометријски подаци у садашњим MRTD-овима ставе ван снаге и, пошто биометријске ознаке ималаца, као што су отисци прстију и црте лица, не могу лако да се промене, „украдени“ биометријски подаци се могу злоупотребљавати у дужем временском року;

– Неадекватан менаџмент кључа преко BAC-а: кључ за приступ подацима на RFID (Радио фреквентна идентификација) чипу складишти се на самом пасошу и могу га очитавати и људи и машински скенери. То значи да свако ко је имао физички приступ пасошу и, нпр. направио оптичку копију, потенцијално може да сачува инфорације о кључу и употреби их за приступ подацима на RFID чипу.

– Прислушкивање комуникација између RFID чипа и читача, као и употреба бруталне силе напада на сам BAC, употребљавајући његове доказане криптографске слабости ради приступу подацима;

– Клонирање RFID чипова у MRTD-овима;

– Злоупотреба могућности даљинског очитавања RFID чипова у пасошима, нпр. за потребе људско-осетљивог активирања „паметних бомби“. Комбинација ових претњи и слабости доноси знатне ризике по безбедност и приватност европских грађана. Ово је посебно релевантно с обзиром на широку географску примену и дуг животни век (до 10 година) постојећих MRTD-ова.

Препоруке заинтересованим странама у Европи

На основу ових налаза, припремили смо један број препорука за заинтересоване стране у Европи (политичаре, индустрију и истраживачке институције) у домену MRTD-ова:

1. Пошто су MRTD-ови са уграђеним слабостима већ уведени и пошто ће неминовно бити коришћени у будућности, препоручујемо следеће мере за хитну примену, ради смањења ризика провале безбедности и крађе идентитета. Ове препоруке укључују и резервне процедуре и технологије које захтевају развој и споразум на међународном нивоу (нпр. на нивоу ICAO):

а. Организациону примену и спровођење принципа јасно одређене сврхе, поготову када је реч о биометријским подацима који се употребљавају у MRTD-овима (у овом случају, та јасно дефинисана сврха била би аутентификација за међународне путнике). Употреба MRTD-ова не би требало да буде проширена на аутентификацију у приватном сектору.

б. Грађане би требало обавестити о ризицима везаним за поседовање нових MRTD-ова, као и о мерама безбедности које они сами могу предузети (на пример, избегавање давања докумената приватним организацијама као што су хотели, итд.).

в. Доступне, али још увек непримењене мере безбедности, као што су Фарадејеви кавези, морају одмах да буду интегрисане у постојеће MRTD-ове од стране држава-чланица ЕУ.

г. Потребне су организационе процедуре које би се носиле са случаје-

вима неуспеле биометријске аутентификације заснованим у урођеним биометријским проблемима као што су стопа лажних одбијања (“false rejection rates“ - FRR) и грешке при самом упису података.

д. Потребне су организационе и техничке процедуре ради спречавања злоупотребе личних података из MRTD-ова.

ђ. Потребне су организационе и техничке процедуре у вези са крађама идентитета кроз употребу података из MRTD-ова, или кроз употребу самих MRTD-ова.

2. Средњерочно гледано (у следеће три године), потребно је развити и обзнанити један нов, убедљив и интегрисан концепт безбедности MRTD-ова и сродних система, који у виду нарочито мора да има следеће:

а. Дефиницију неопходних нивоа безбедности.

б. Заштиту личних података европских грађана.

в. Мултилатералне и организационе безбедносне обзире у вези издавања MRTD-ова, који имају у виду различите оператере у различитим државама, као и саме кориснике MRTD-ова.

г. Ризике и претње који се помаљају из комбинације разних технологија које се примењују у контексту MRTD-ова, као што су RFID, биометрија, као и безбедносне стране папирних докумената.

д. На основу дефинисаних нивоа безбедности и ризик-анализе, потребно је применити поновну, свеобухватну процену и ново пројектовање техничких решења која су усвојена за постојеће MRTD-ове, посебно када је реч о RFID-у и биометрији. Треба испитати да ли су ове технологије уопште и потребне, или да ли су безбедније технологије, које боље чувају приватност, довољне.

ђ. Начини на које примена датих технологија може бити побољшана (нпр. кроз биометрију путем коришћења процеса поређења података на самој картици, или сензора на самој картици) треба такође да буду испитани.

е. Концепт безбедности треба да буде предмет јавне дебате од стране стручњака за безбедност и приватност на нивоу Европе.

3. Техничке и организационе мере које буду развијене треба да буду стандардизоване (на нивоу ICAO), уведене у следећој генерацији MRTD-ова и подложне глобалној ревизији.

Превод : Александар Павић

Кевин Хагерти

Једна генерација је све што им треба

До времена када мој четворогодишњи син буде обложен омекшалом кожом старости, њему ће вероватно изгледати сасвим уобичајена чињеница да ће скоро свако кога буде познавао имати трајно уграђен микрочип.* Аутоматски пратећи његово кретање у реалном времену, чип ће га повезивати са базама података које ће надзирати и снимати његове најситније навике у понашању. Већина људи гледа на такву могућност са осећајем ужаснуте неверице, одбацујући је као фантазију из научне фантастике. Међутим, технологија већ постоји. Већ годинама друштва за заштиту животиња уграђују у све кућне љубимце који напуштају њихове просторије један мали идентификациони микрочип. Исто тако, милиони потрошачких производа сада се прате преко минијатурних радио-таласних идентификационих (RFID) чипова који омогућују сателитима да одреде њихову тачну локацију.

Један одабран број људи је већ „чипован“ са уређајима који аутоматски отварају врата, пале светла и извршавају друга скромна чудеса. Један од познатијих међу њима јесте истраживач са енглеског Ридинг универзитета (*Reading University*) Кевин Ворвик (*Kevin Warwick*); Ворвик је водећи заговарач скоро неограничених могућности употребе таквих чипова.

Међу корисницима су и муштерије Баха бич клуба (*Baja Beach Club*) у Барселони, од којих су многи платили око 150 америчких долара за привилегију да им буде уграђен микрочип који им омогућава да заобиђу дугачке редове на улазу у клуб и купују пића путем скенирања.

Ови појединци су авангарда напора да се ова технологија што више прошири. Од сада ће микрочипови постајати постепено све мањи и све неприметнији и лакши за постављање. Према томе, свака реална препрека масовном „чиповању“ грађана Запада није више технолошка већ културна. Она се заснива на нагонској реакцији против могућности личног обележавања које појединца претвара у обичан делић масовног инвентара људске расе.

---

*Оригинални текст је објављен 12. децембра 2006. године у часопису *Toronto Star*.

Можда се ми данас чврсто држимо таквих убеђења али се обзири могу, и вероватно хоће мењати. Начин на који ће се такав невероватан преображај погледа на свет вероватно десити јасан је свакоме ко прати све што је везано за питања приватности у последњих четврт века. Неће бити куцања на врата у 3 сата ујутру од стране специјалаца који су дошли да нам на силу уграде чипове у тела. Процес ће бити суптилнији и надовезујући, обложен необоривом терминологијом прогреса и друштвеног напретка, опонашајући процесе који су већ допринели експанзији у употреби надзорних камера и у корпорацијском тржишту личних података. Биће употребљен читав низ већ проверених стратегија како би се ова технологија грађанима приближила. То ће ићи упоредо са растућим притисцима на већ прокажене друштвене групе и подстрецима остатку становништва да се чипује.

Све почиње у далеким земљама. После испробавања технологије на заморчићима, људским и животињским, прво широко распростањено уграђивање чипова у људе десиће се на обронцима западног света.

Такав развој ствари већ ће имати важност сам по себи, али ће његов међународни одјек лежати у прилици да се глобално гледалиште упозна са том технологијом и навикне на помисао да је чиповање једна могућа будућност. Све већи број разних хипотетичких сценарија за чиповање такође ће бити представљен путем забавних медија, што ће даље допринети процесу тог упознавања.

На Западу ће чипови прво бити уграђивани у чланове обележених група. Педофили су главни кандидати за ту почаст, мада би могло да започне и са терористима, нарко-дилерима или једноставно криминалцима који су на најлошијем гласу баш те године. Биће давана обећања кратког даха да ће та технологија бити примењена само на „најгоре од најгорих“, а заправо ће врло брзо уследити свеобухватно чиповање свих затвореника, укључујући и оних који издржавају условне казне.

Чак ће и они који су само оптужени бити чиповани, што ће бити правдано тиме да ће то спречити њихово бежање од правде. Многи ће затвореници ово радо прихватити, пошто ће само чиповани имати могућности превременог, условног пуштања на слободу, одласка кући за викенд или кажњавања друштвено-корисним радом. Унутар затворског система развиће се нови речник који ће разликовати нечиповане од чипованих.

Мада ће употреба чипова бити правдана напорима да се смање преваре и друга кривична дела, криминалци ће скоро тренутно развити начине да симулирају кодове са туђих чипова и да манипулишу тим подацима.

Релативна малобројност затворске популације значиће, међутим, да ће затвори бити тек кратак предах на једном дужем путу. Комерцијални успех зависи од способности налажења начина да се чипује шире становништво,

то јест сви они који поштују законе. Зато ће се циљати на још неке обележене групе. То ће несумњиво подразумевати надзор над примаоцима социјалне помоћи, што ће се правдати напорима да се смање злоупотребе, повећа ефикасност и спречи могућност примања „незаслужених“ бенефиција.

Једном када електронска трговина постане довољно напредна, примаоци социјалне помоћи ће исту примати у виду електронске допуне својих микрочипова, што ће имати призвук праведности, обезбеђујући да корисници могу да купују само производе које је одобрила влада, и то од одобрених продаваца, смањујући ту увек узнемиравајућу могућност да ће сиромашан свет можда користити ограничена средства која су му дата на располагање за куповину алкохолних пића или дувана.

Борци за грађанске слободе ће покушати да покрену дебату на ту тему. Њихова настојања да се чиповање забрани биће ометена природним тешкоћама у анимирању саосећања јавности према криминалцима и примаоцима помоћи – групама за које би већина хтела да буду под још већом контролом. Дакако, нижи степен саосећања јавности према таквим групама заправо објашњава зашто ће присилно чиповање бити првенствено усмерено на оне који су већ на неки начин обележени.

Тада ће се у причу умешати и званични органи које се баве заштитом приватности. Поседујући мандат за оцену законитости таквих иницијатива, комесари за приватност и скупштински одбори произвешће масе извештаја који ће бити представљени на читавом архипелагу међународних скупова. Успорени дугим процесима истраживања и роковима за издавање, њихови налази ће бити изнети већ дуго нако што широка примена чиповања буде постала већ готова ствар. Налази истраживања о ефикасности таквих технологија биће разнородни и отворени различитим тумачењима.

Званичници ће на сав глас пружати уверавања индустрији чипова да се они не противе самом чиповању, које је великом брзином постало растућа пословна грана. Уместо тога, они ће само настојати да се та технологија употребљава на равноправан начин, и да подаци на чиповима не буду подложни злоупотреби. Предлагаће се нове мере заштите.

Послодавци ће почети да траже микрочиповање као услов за запошљавање. Предводник ће бити америчка војска, која ће захтевати чиповање свих војника као начин побољшавања команде и контроле на терену, као и идентификације људских остатака. Од кувара до командоса, свих милион и више припадника америчких оружаних снага добиће уграђене чипове уместо досадашњих металних плочица.

Убрзо ће следити и огромни сектор безбедности. Од чувара, полицајаца и затворских чувара ће се очекивати да имају уграђени чип, што ће такође бити случај са свима који раде на осетљивим пословима.

Први знаци овог последњег већ су видљиви. Током 2004. уред мексичког државног правобраниоца почео је са уграђивањем чипова у запослене ради ограничавања приступа обезбеђеним зонама. Категорија „осетљивог занимања“ биће проширена до тачке када ће свако чији посао захтева кључеве, лозинке, безбедносну проверу или идентификациону значку морати да исте замени уграђеним чипом.

Судије које буду одлучивале о уставности оваквих мера закључиће да је чиповање у оквирима закона. Танка маска „добровољности“ иза које ће се већина оваквих програма крити омогућиће судству да тврди како појединци нису приморавани да ту технологију прихвате против своје воље.

У ситуацијама када чипови буду очигледно наметани људима, судови ће пресудити да то представља несумњиво кршење њиховог права на приватност. Међутим, они ће се тада позвати на небулозни и историјски променљиви стандард „разумности“ да би прогласили обавезно чиповање као нужно кршење права на приватност у контексту захтева за ефикасношћу државних органа и неодложном потребом да се повећа безбедност у светлу још увек трајућих ратова против тероризма, дроге и криминала.

На овом месту, нека нажалост већ уобичајена трагична појава модерног живота ће се десити: неко мало дете, вероватно нека врло фотогенична беба, биће убијено или на ужасан начин малтретирано. То ће се десити у једном од медијских центара западног света, омогућујући непрестано извештавање, без предаха. Произвођачи чипова препознаће у овоме прилику коју су годинама чекали. Пошто ће до тада већина „бубица“ у њиховим производима бити „испеглана“, већина грађанства са њима већ упозната а сами производи већ релативно јефтини, произвођачи ће се удружити са полицијом ради покретања гласне јавне кампање у циљу подстицања родитеља да чипују своју децу „како би себи обезбедили мирну савест“.

Биће нуђене посебне погодности. Уграђивање ће бити бесплатно, под условом да се породица пријави за услуге надзора. Пуни љубави али забринути, родитељи ће бити умирени могућношћу повезивања чиповања своје деце са другим функцијама на њиховим PDA ручним рачунарима, како би могли да уживо посматрају своју децу, било кад и са било ког места.

Паралелно са овим развојем ствари пласираће се иницијативе са призвуком практичности, ради подстицања све мање групе нечипованих да прихвате сада већ уобичајени поступак чиповања. Прво ће таква „практична“ чиповања бити намењена највишим слојевима западног друштва, омогућавајући елити да се несметано креће физичким и међународним коридорима моћи. Таква пракса ће се ширити како користи од чиповања буду постајале све баналније. На пример, чиповани појединци ће се све лакше кретати кроз царину.

На крају ће услов коришћења система јавног превоза бити омогућавање службеницима да надзиру ваш чип. Компаније ће нудити попусте појединцима који плаћају путем свој уграђеног чипа, уз услов, штампан ситним словима, да продавац добије право приступа великој колични ваших личних података. Ови „попусти“ представљаће уствари казнену ценовну политику према нечипованим појединцима како би их подстакли да се повинују сталном надзору. Корпорације ће тражити личне податке како би могле да праве све детаљније профиле купаца за потребе маркетинга, а и како би исте личне податке продале другим институцијама.

Тада ће већ све главне организације тражити начине да искористе све могућности које нуди једна скоро универзално чипована популација. Употреба чипова ће бити све разноврснија, као и попусти који се нуде. Свака нова генерација кућних технологија биће прављена тако да може све ефикасније да суделује са чиповима уграђеним у тело.

Налажење рачунара или уређаја који ће функционисати на старомодни, „ручни“ начин биће све теже и скупље. Пацијенти у болницама и на кућној нези биће већ рутински чиповани, што ће омогућити медицинском особљу – или, тачније, далеким рачунарима – да надзиру њихове биолошке функције у реалном времену.

Нестрпљиви да смање здравствене трошкове већином физички неактивног грађанства, власти ће понудити пореске олакшице појединицима који редовно вежбају. Лични чипови биће даљински надзирани ради потврде да је пулс у складу са прописаним програмом вежбања. До тог времена, за многе појединце, појам „чиповања“ ће се вртети око тога које функције у уграђеном чипу евентуално треба активирати. Свака могућност евентуалног уклањања чипа биће све мање одржива, пошто ће ношење чипа бити предуслов за учешће у најбитнијој динамици савременог живота, попут куповине, гласања и вожње.

Они који још увек одолевају биће све уморнији од сталних шаљивих етикетирања да су „лудисти“, као и суптилних оптужби да можда имају нешто да сакрију. Већ фрустрирани сталним призорима суседа који пролазе мимо њих у „чипованим“ редовима док они чекају, разним непрактичностима и трошковима којима су „нечиповани“ изложени, и они ће на крају изабрати пут најмањег отпора и дати да им се угради чип.

Дакле, у року од једне генерације, она културолошка одбојност за коју многи сматрају да је нагонска реакција на могућност да наша тела буду обележена попут затвореника у концентрационом логору, вероватно ће се изгубити.

У годинама које долазе, неки од најмоћнијих институционалних чинилаца у друштву почеће да делују у циљу подстицања, принуђивања па чак и присиљавања следеће генерације да прихвати уградњу чипова.

Сада је, дакле, време да се размисли о беспримерним опасностима овог сценарија, од којих је најозбиљнија међу њима везана за могућност да чак и релативно стабилна модерна друштва могу, у доба општих страховања, да прихвате варљива обећања. Како би се предрасуде једног Џоа Мекартија, Едгара Хувера (дугогодишњег директора америчке Федералне службе за истраживања, FBI) или јужњачких Кју-клукс-клановаца – а сви су у неком тренутку били дубоко интегрисани у амерички политички естаблишмент – одразиле у једном таквом свету? Шта би један Хитлер, Мао или Милошевић постигли да су њихови грађани били чиповани, кодирани и даљински надзирани?

Ускоро ћемо бити бомбардовани хорским сведочанствима која говоре о свим врлинама микрочиповања, праћеним умирујућим уверавањима о демократским традицијама, владавини права и правима на приватност. Нажалост, историја показује да ствари могу да брзо крену у катастрофалном правцу, и да се то дешава са узнемирујућом редовношћу. А међународни уговори, законитост или демократски назори се традиционално нису показали претерано способним да спрече нечију усредсређену безобзирност.

„То се овде не може десити“ постала је тиха лабудова песма оних који су нестали. Зато је најбоље да размишљамо о оваквим анти-утопијским могућностима пре него што понудимо нежне ручице наших синова и ћерки на чиповање. И, мада не можемо да предвидимо све предности које из ове технологије могу да произађу, њене негативне могућности су скоро и превише застрашујуће да би се о њима чак и размишљало.

превод Александар Павић

Додатак Б

Критички гласови из Србије

Жички апел

1. Биометријске личне карте као обавезујући документ на националном нивоу су уведене у неколико држава света, углавном далекоисточних.* У Европској унији велика већина земаља нема такве личне карте, оне нису услов за улазак у Европску унију нити њихово увођење доприноси бржем уласку. Очигледан пример је Словенија, која пре уласка у ЕУ није увела такве карте (иако је постојала могућност), већ обичне пластичне са вишим нивоом заштите.

2. Сабор Светог Синода у сталном сазиву православне цркве у Грчкој, Свети Синод Руске православне цркве, Свети Синод Украјинске православне цркве (Московске патријаршије), Протат Свете горе Атоске, Епископија Жичка упозоравају да се иза целог пројекта нових идентификационих докумената крије најтежи тоталитаризам потпуно супротан хришћанском разумевању света и живота, и погубан за људско достојанство и слободу као најдрагоценији дар Бога људима. „А Дух (Свети) је Господ, а где је Дух Господњи онде је слобода“ (2 Кор. 3,17). Управо зато, због светости слободе, никаквог Божијег благослова нема на овоме пројекту и православни га не могу подржати.

3. Земље које су планирале или планирају да уводе биометријске личне карте суочене су са отпором мислеће јавности и друштвене заједнице уопште. У Великој Британији је покушај увођења биометријских личних карти довео до вишемесечних дебата у парламенту и бурних реакција академских грађана, док је у Канади од стране званичне парламентарне комисије одбачен на неодређено време, као скуп, неоправдан и потенцијално опасан.

4. Светски стручни органи, какав је Заједнички комитет за људска права британске владе, процењују да је пројекат увођења биометријских личних карти на националном нивоу потенцијално у колизији са европском Конвенцијом о људским правима, а званичне студије о изводљивости показују да такве личне карте не гарантују стопроцентну поузданост и аутентичност. Судови неких земаља (Јапан и Тајван) су реаговали са пресудама да пројекат биометријских личних карти крши права грађана и одредбе Устава, у складу са чиме су донети и суспензивни акти.

5. У Србији је пројекат набавке опреме за израду биометријских личних карти постао актуелан крајем 2003. године, када је тадашњи министар

---

* Тачке Жичког апела, донете на основу Жичког симпосиона, су преузете из часописа Жички благовесник, јул 2006, стр. 1. Детаљније о симпосиону у поглављу 4.2.1 наше студије.

полиције објавио да је купљена модерна и скупа опрема од америчке фирме Motorola. Та куповина није прошла ни обавезан тендерски протокол ни законско додељивање новца из републичког буџета, због чега је 2004. године реаговао министар финансија са најавом подизања кривичних пријава. Србија је јединствен пример да је прво купљена опрема за биометријску идентификацију грађана, а после тога (тачније после три године) покренута скупштинска процедура за предлог закона о биометријским личним картама, због чега је себе сврстала у ред тоталитарних држава са волунтаристичким правним уређењем.

6. Америчка фирма која је МУП-у Србије продала систем за биометријску идентификацију грађана има посебне уговоре са америчком војском и централнообавештајном службом (CIA), те нико не може да гарантује да не постоји могућност одлива података страним службама. Такође је основано претпоставити да поменуте службе веома лако могу креирати лажне личне карте за своје потребе, које ће од стране нашег рачунарског система бити препознате као потпуно валидне. Индикативна је чињеница да у Америци државна управа није ни покушала са увођењем биометријских личних карти међу својим становништвом, јер би то сигурно довело до великог отпора јавности.

7. Није тражена масовна сагласност грађана Србије за проширивање базе података коју ће држава о њима водити нити су организоване јавне дебате и дискусије по том питању.

8. Пројекат директно угрожава приватност грађана као једно од фундаменталних личних права данашњице и отвара простор за електронски криптоване тајне архиве.

9. Бирократски апарат добија могућност готово тренутног манипулисања огромним бројем података преко централизоване базе и продаје делова базе трећим лицима.

10. Злонамерни упади споља или намерно исправљање централизоване базе изнутра носе огромну опасност по интегритет личности које су њима обухваћене.

11. Усвајање овог пројекта у будућности води ка много тоталитарнијим концептима интеграције свих докумената у један, чиме би се избрисала анонимност токова новца и отворио пут тоталном надзору државе над појединцем. Минијатуризација целог система се полако спроводи у свету, у виду поткожних чипова, због чега хришћани свих конфесија изражавају оправдан страх од најаве тоталитарног режима описаног у Јовановом Откривењу (уп. гл. 13, ст. 16-18). Синоди неких Православних цркава су дали званична саопштења, јер злонамерни људи могу искористити овакве пројекте за уношење раздора и немира међу хришћане.

Да ли електронска карта угрожава приватност грађана?

(закључци и препоруке округлог стола у Галерији САНУ)

1. Предлаже се хитно доношење Закона о заштити приватности који би био сагласан са одговарујућим директивама ЕУ и међународним конвенцијама, или примена постојећег савезног Закона о заштити података о личности из 1998 године, а који предвиђа: да се лични подаци могу прикупљати, користити и обрађивати само на основу закона или уз личну сагласност грађана.* На округлом столу је изнето мишљење да су поједине одредбе Закона о личној карти (члан 28 ставови 2 и 3) супротни међународно прихваченим начелима заштите приватности и чак у супротности са постојећим Законом о заштити података, а кога свакако треба допунити или заменити са новим Законом о заштити приватности.

2. Након усвајања Закона о заштити приватности, неопходно је на основу одредби из тог закона извршити измене и допуне Закона о личним картама који је Народна скупштина изгласала 14 јула 2006. Такође, у Закон о личним картама треба унети и да грађани који не желе личну карту са чипом и биометријским подацима могу да задрже стари формат личне карте.

3. Констатовано је да постоје опасности, да као и код других база података, дође до злоупотребе и напада на податке у бази података о издатим личним картама. Зато се препоручује стално усавршавање мера заштите и увођење одређених видова парламентарне контроле над организацијом, коришћењем и заштитом базе података о издатим личним картама.

4. Основни проблеми и разлике у мишљењима у вези са издавањем нових личних карата нису у основи информатичке природе. Изражене су извесне сумње и дилеме, али и дати задовољавајући стручни одговори у односу на безбедност примена чип технологија. Објашњено је, да МУП планира употребу „контактних чип картица“ које спадају у најбезбедније медије за чување личних података, дигиталних сертификата, електронских потписа и др. Истовремено, на скупу је указано, да они који желе да користе тековине савременог информационог друштва, учествују у електронском пословању, употребљавају апликације електронске управе, ипак морају да имају одговарајућу електронску идентификацију.

---

* Округли сто је организовало Друштво за информатику Србије. Текст преузет са сајта те организације, на Интернет адреси: http://www.dis.org.yu/. Деатаљније о скупу у поглављу 4.4.1 наше студије.

Поред препорука скупа, учесници су упозорили на многе проблеме који прате ову проблематику. Учесници округлог стола упозоравају, да је суштина проблема са новим личним картама много дубља од информатичких аспеката и указују да постоје информације о пропустима у процедури набавке опреме пре 3 године и да Закон о личним картама покреће пре свега одређена суштинска етичка, морална, филозофска и политичка питања о односу државе и грађана и положају грађана пред опасностима од глобализма и тоталитаризма у савременом свету.

Имајући у виду све изнете чињенице, са скупа је сугерирано свим надлежним органима, да са дужном пажњом размотре изнета мишљења и препоруке, и уз консултације са компетентним институцијама, предложе измене и допуне Закона о личним картама, како би он био у складу са интересима грађана Србије да заштите своју приватност и слободе.

Декларација стручног скупа у Краљеву

Са скупа о изазовима нових информационих технологија, одржаног у Дому Светог Николаја Жичког у Краљеву, обраћамо се јавности Србије сматрајући да још увек није касно да се, помоћу друштвеног дијалога, зауставе негативне тенденције које воде кршењу права на приватност под видом увођења нових информационих технологија у државну управу.* Понављајући закључке Жичког симпосиона, одржаног 26. марта 2005, а упућеног у виду Апела Скупштини Републике Србије јула 2006. године, подсећамо на следеће чињенице:

1. Нови Закон о личним картама донет је без јавне расправе, уз кршење низа светских и европских конвенција о људским правима, Устава Републике Србије, Закона о заштити личних података, као и тендерских правила за набавку опреме за биометријска лична документа;

2. Опрема за личне карте коштаће презадужену Србију око 100 милиона евра;

3. Стварање централне базе биометријских података о свим грађанима Србије води ка могућностима опасних злоупотреба, које могу имати кобне последице по личну и колективну безбедност;

4. Кршење права на приватност наставља се стварањем централне базе података о свим здравственим осигураницима у Републици Србији, као и централне базе података Министарства просвете, где ће се сабирати огроман број података о свим просветарима, ђацима и њиховим родитељима. И ове базе података настају без минимума јавне сагласности.

После научног скупа чији ће резултати бити обнародовани у зборнику радова, обраћамо се јавности позивајући грађане да:

1. Учествују у борби за основно људско право на приватност захтевајући од власти своје државе и својих легитимних представника у парламенту пуну информацију о свим аспектима закона који се тичу приватности грађана, укључујући се у јавне расправе по овом питању;

---

* Преузето из новине *Православље*, бр. 950, званичног гласила Српске патријаршије. Текст под називом „Тражимо алтернативни модел идентификације“ налази се на адреси: http://www.pravoslavlje.org.yu/broj/950/tekst/trazimo-alternativni-model-identifikacije/. Детаљније о скупу у поглављу 4.4.2 наше студије.

2. Прате све демократске иницијативе које бране право на приватност почев од иницијативе за оцену уставности новоуведених закона и уредаба у тој области до законодавних иницијатива за измене и допуне Закона о личној карти;

3. Придруже се акцији прикупљања потписа за измене и допуне Закона о личној карти, заснованих на праву приговора савести оних грађана који, не желећи биометријске личне карте, траже алтернативни модел идентификације.

Верујући да ће покретање дијалога у овој области имати повољан утицај на демократске процесе у Републици Србији, спречавајући тенденције ка тоталитаризму, од кога смо толико постарадали у XX веку, обраћамо се представницима власти тражећи од њих да изађу у сусрет грађанским иницијативама чији је циљ заштита права на приватност. Зато учесници скупа указују на:

1. Опасност од скупљања и чувања података о личном животу људи, посебно о религиозном и политичком избору, здрављу, познанствима, путовањима и слично;

2. Неоправданост даљинског препознавања човека без његовог знања, нарочито на местима где није дужан да се представи;

3. Право грађанина да зна каква се информација налази у његовом „електронском досијеу“ и могућност уклањања података који су изгубили актуелност. Листа података који се сабирају и чувају мора бити јасно дефинисана и опште позната;

4. Неопходност разраде електронских система идентификације и евидентирања грађана под контролом јавности, са јасним тумачењем мотива и објашњењем значења симбола који се у том процесу користе;

5. Неопходност јасног и подробног дефинисања списка установа које имају приступ базама података, усвајања мера за заштиту личних информација, уз појачавање одговорности за незаконито коришћење истих;

6. Средства препознавања човека не смеју да штете његовом здрављу, понижавају његову част и достојанство;

7. Не смеју се користити средства препознавања неодвојива од људског тела.

Слободан Антонић

У потрази за српским Тороом

Главни разлог за страх јесте нетранспарентност. Ви са собом морате да носите документ у коме уопште не знате шта пише. Али, зар не верујете сопственој држави? Наравно да не верујемо!

„То од нас тражи ЕУ". „Сви у Европи то већ имају". Са ове две реченице у Србију можете увести било коју глупост. Рецимо, да деца не смеју да седну на клацкалицу без заштитног шлема за главу. Или да, пре но што узберете воћку, морате дрвету да убризгате анестетик.

Последњи пример су нове личне карте. Тврдило се да су електронске личне карте услов за укидање виза Србији и да већ све земље у окружењу то имају. Онда су неке религиозне групе и радикали показали да ништа од тога није тачно. Нико не везује укидање виза Србији са стављањем чипа на личне карте, а земље у окружењу имају пластификоване, али не и електронске исказнице.

Сада се, међутим, вели да је ово сјајна прилика да Србија буде прва у модернизацији и да се само мрачне и ретроградне снаге боје овог унапређења – као што су се некада бојале железнице или радија. Полако, господо, ствари нису баш тако једноставне. Да су електронске личне карте толико сјајна и непроблематична ствар, како нам се сада представља, не би се чекало на Србију да их прва уведе. Железница и радио су се тицали добре воље појединаца, а овде држава уводи обавезу сваког ко је старији од 16 година да са собом носи чип, из кога, опет, само полицајац или неки државни службеник може да ишчита одређене податке. И то онда више није страшило само за религиозне групе и радикале, то је нешто што диже косу на глави и сваком искреном либералу.

Главни разлог за страх јесте нетранспарентност. Ви са собом морате да носите документ у коме уопште не знате шта пише. Али, зар не верујете сопственој држави? Наравно да не верујемо! Прво, свако од нас је био сведок грешака администрације. Те грешке су макар биле белодане, и човек је некако могао да тражи да се исправе. Како сада да знате да се у вашем чипу неће поткрасти нека грешка – рецимо, податак да сте вишеструки убица? Треба

---

* Текст је преузет из Политике, 13. 06. 2006. Проф. др Слободан Антонић је ванредни професор на Филозофском факултету у Београду и политички аналитичар.

ли да вас десет полицајаца, који су вас легитимисали, измалтретира да бисте тек онда схватили да нешто са вашом личном картом није реду?

Али, такви подаци неће ни стајати на чипу. Неће? Како то можемо да знамо? Зато што ће тако писати у закону? Ма хајдете, молим вас! Можда садашња власт искрено верује да ће се држати закона и на чип стављати само оно чега већ има у постојећим личним картама. Али, свако коме памћење досеже даље од прекјуче зна да нема ствари коју овде власт није злоупотребила – само ако је то могла. Српска историја је пуна пустолова, частољубаца, грабежљиваца и неурастеника, који су се домогли државне власти и од ње направили злочин. Шта нам јамчи да буквално већ сутра неко од таквих неће поново завладати Србијом? Погледајте само све оне политичке десперадосе који, испуњени мржњом и манијом величине, стоје на улазу у наше политичке установе и отворено прете својим „гвозденим метлама"? Па зар мислите да ће се они моћи уздржати?

И да нам неће, необуздани јавношћу и транспарентношћу, у чип ставити и нешто више од ЈМБГ и отиска прста – нешто што ће нам бескрајно отежати и затровати сваки додир са државом и администрацијом?

Ако неко о томе има било каквих илузија, то је његова ствар. Али, не може све остале терати да учествују у његовим илузијама. Ко воли такве, „модерне" личне карте нека их слободно узме. Али, нека не тера и оне који их се плаше да их морају имати. Ако и за одлазак у војску постоји алтернатива, не видим зашто се и овде она не би могла дозволити? Зато што је неко, пре три године, без тендера и закона набавио опрему вредну 100 милиона долара, па је сада полицији жао да толика опрема стоји неискоришћена? Нека стоји, то је мања штета од страха грађана да је поново на помолу тоталитарна држава – само овога пута технички много напреднија и моћнија.

А ако се у садашњем облику овај закон ипак усвоји, неће нам преостати ништа друго до да се сетимо старог либералног хероја Дејвида Тороа. Он је сматрао да је лична слобода толико неприкосновена, да је боље отићи у затвор него ли се покорити закону који је угрожава. И отишао је у затвор. Тако је настао појам грађанске непослушности. Овдашњи квазилиберали често су махали тим појмом. Али, наравно, у затвор нису одлазили. Сада је ред на истинске либерале. Неко мора да оде у затвор да би ово друштво схватило суштину либерализма. Ко ће бити српски Дејвид Торо?

Родољуб Шабић

Чип за приговор савести

Министарство унутрашњих послова најавило је да примена новог Закона о личној карти неће почети крајем јануара, како је то законом предвиђено, као и да ће уредбом владе обавеза грађана да имају личне карте снабдевене електронским чиповима бити претворена у факултативну, односно да ће такву личну карту имати само онај ко то жели.* Вероватно ће сама идеја да се уредбом владе интервенише у одредбу закона бити суочена с многим примедбама формално-правне природе. Лично, делим мишљење да, са становишта нормалне хијерархије правних аката, оваква идеја не може поднети критику, али, искрено, немам жељу да се таквој критици придружим. Јер, мислим да ће најављени потез МУП-а, бар за одређено време, отклонити неке оптерећујуће дилеме и многе људе учинити мирнијим.

У прилог томе говори ми и то што сам о једној необичној теми у последњих месец или два, више пута разговарао с различитим људима из стручних удружења, НВО, цркве. Тема је био приговор савести. Вероватно делује необично то да приговор савести означавам као „необичну" тему, јер тешко да заслужује тај епитет. Приговор савести је у међународним релацијама прихваћен правни стандард који подразумева право да се због религијских, етичких, моралних, филозофских и других сличних разлога одбије извршавање одређене законске обавезе. То право је прихваћено у великом броју земаља света и одавно није нешто необично.

И наш Устав познаје приговор савести. У члану 45. стоји да „лице није дужно да противно својој вољи или убеђењима испуњава војну или другу обавезу (која укључује употребу оружја). Лице које се позове на приговор савести може бити позвано да испуни обавезу (без обавезе да носи оружје), у складу са законом". „Изостављање", односно стављање речи које говоре о оружју у заграду, илуструје „необичну" садржину поменутих разговора. Наиме, људи са којима сам разговарао размишљали су о праву на приговор савести у једном контексту битно другачијем од стандардног – о позивању на њега у вези с обавезом која не укључује употребу оружја и у прилог томе су истицали озбиљне разлоге.

---

* Текст је преузет из Политике, 13. 01. 2007. Родољуб Шабић је повереник за информације Републике Србије.

Непосредан повод за то је био управо почетак примене новог Закона о личној карти, пре свега, одредби чл. 7. и 8. које, поред осталог, предвиђају да се у личну карту уносе и тзв. биометријски подаци, да она садржи контактни микроконтролор (чип), те да омогућава аутоматско очитавање података. То је, још у фази предлагања закона, било повод за многобројне жестоке реакције врло различитих субјеката.

Неки људи биометријске личне карте виде као непотребан сувишан феномен који, мада није реално опасан, ипак јесте иритантан због својих „тоталитарних" карактеристика. Други у томе виде корак ка реалном успостављању тоталитарне контроле. Неки, опет, препознају прву фазу у претпостављеном трофазном процесу – отприлике, прво један чипом снабдевен документ, потом један једини документ, наравно са чипом и на крају само чип, као документ који се не носи у џепу или новчанику, већ у телу, под кожом. А одатле за неког није далеко ни до застрашујућег, апокалиптичног виђења будућности какво је оно из, у последње време, често помињаног Откровења Јовановог.

Очигледно је да наш Устав не даје нимало простора за истицање приговора савести у односу на законом предвиђену обавезу, осим кад та обавеза укључује употребу оружја. И чињеница да су, у време доношења закона, све критике практично игнорисане, говорила је да ни политичка констелација не иде у прилог тако нечем. Ипак и поред тога, сва је прилика да и без измене закона, онај ко не жели да има личну карту снабдевену чипом, неће ни морати да је има. Да ли је то први наговештај ширења простора за примену приговора савести? То је, наравно, неизвесно али је извесно да ће, бар за аналитичаре, поред осталог, бити занимљиво и питање ко или шта је утицао на то да МУП повуче овај потез. На једну од могућих претпоставки с тим у вези могао би да указује и прилично видан ангажман представника СПЦ. Реална или не, оваква претпоставка је, у вези с приговором савести, сигурно асоцијативна. Бар мене, иако преферирам аргументе правне природе, подсећа на то да је и процес чији резултат је актуелна, призната садржина приговора савести, својевремено, покренут мотивима религијске природе.

Многи од оних који не виде проблем биометријске личне карте у контексту остварења неке црне или сиве, орвеловске или библијске, футуристичке пројекције – виде га, међутим, као реалан проблем садашњости. Лични документи снабдевени електронским чиповима подразумевају стварање база података које су далеко богатије и комплексније од досадашњих, класичних. То потенцира могућност власти да скоро тренутно употребљава огромну количину информација о грађанима, али самим тим и да их, она или субјект коме их је уступила, злоупотребљава. Наравно, злоупотреба информација, њихова незаконита употреба или интервенција у њихову садр-

жину, не мора бити вршена од стране власти, већ може бити и последица злонамерних упада споља. Такође, није могуће отклонити сумње у погледу тога да електронски чип у личној карти може бити (зло)употребљаван за лоцирање или праћење.

Било би нецелисходно, у било којој области, одређи се користи коју доноси коришћење напредних технологија, али би било неодговорно заборавити на ризике које оно, такође, доноси. Баш зато је важно да се време, које ће бити обезбеђено „контроверзним" потезом МУП-а, искористи за то да се у отвореној комуникацији власти и стручне јавности отклони што више дилема, а евентуалне злоупотребе новог идентификационог система искључе или бар сведу на минимум.

С тим у вези је незаобилазна чињеница да је, мада је Уставом зајамчено, право грађана на заштиту података о личности код нас више теоријско него стварно. Увођење нових личних карата, с чипом или без чипа, у сваком случају више него озбиљно, упозорава на то да би један од апсолутних приоритета будућег сазива Народне скупштине морало да буде доношење новог Закона о заштити података о личности.

Библиографија

Примарна литература

Књиге, студије и стручни извештаји

1. Ashbourn, Julian, *The Societal Implications of the Wide Scale Introduction of Biometrics and Identity Management*, Background paper for the Euroscience Open Forum ESOF 2006, Минхен 2006. Студија је преузета са адресе: www.statewatch.org/news/2006/jul/biometrics-and-identity-management.pdf.

2. Ball, Kirstie, David Lyon, David Murakami Wood, Clive Norris, Charles Raab, *A Report on the Surveillance Society,* Full Report, 2006. Извештај је преузет са адресе: http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/.

3. Brands, S., *Rethinking Public Key Infrastructures and Digital Certificates; Building in Privacy*, MIT Press, 2000.

4. Cabinet Office UK, *Identity fraud: A Study*, Лондон 2002. Студија је преузета са адресе: http://www.identitycards.gov.uk/downloads/id_fraud-report.pdf.

5. Dessimoz, Damien, Christophe Champod, Jonas Richiardi, Andrzej Drygajlo, *Multimodal Biometrics for Identity Document State-of-the-Art*, Research Report, PFS 341– 08.05, Version 2.0, 2006. Студија је преузета са адресе: http://www.europeanbiometrics.info/images/resources/90_264_file.pdf.

6. EPIC, *Annual report 2004–2005*, Извештај је преузет са адресе: http://www.epic.org/epic/annual_reports/2004.pdf.

7. FIDIS, *D3.2: A study on PKI and biometrics*. Студија је преузета са адресе: http://www.fidis.net/fidis-del/period-2-20052006/d32/.

8. FIDIS*, D3.6*: *Study on ID Documents*. Студија је преузета са адресе: http://www.fidis.net/fidis-del/period-2-20052006/d36/.

9. Froomkin, A. Michael, *The Uneasy Case for National ID Cards*, Draft, University of Miami School of Law, март 2004. Студија је преузета са адресе: http://personal.law.miami.edu/~froomkin/articles/ID1.pdf

10. House of Commons Science and Technology Committee, *Identity Card Technologies: Scientific Advice, Risk and Evidence*, Sixth Report of Session 2005-06, Лондон 2006. Студија је преузета са адресе: http://www.publications.parliament.uk/pa/cm200506/cmselect/cmsctech/1032/1032.pdf.

11. Heydt-Benjamin, Thomas S, Daniel V. Bailey, Kevin Fu, Ari Juels, and Tom O'Hare, *RFID Payment Card Vulnerabilities Technical Report*, 2006. Извештај је преузет са адресе: http://www.nytimes.com/packages/pdf/business/20061023_card/techreport.pdf

12. Hayes, Ben, *Construction of EU's Big Brother database*, Statewatch, 2005. Анализа је преузета са адресе: http://www.statewatch.org/news/2005/may/sisII-analysis-may05.pdf.

13. London School of Economics and Political Science, *The Identity Project, An assessment of the UK Identity Cards Bill and its implications*, Version 1.09, Лондон, 2005. Студија је преузета са адресе: http://www.csrc.lse.ac.uk/idcard/identityreport.pdf.

14.London School of Economics and Political Science, *Research Status Report*, Лондон, 2006. Студија је преузета са адресе http://www.csrc.lse.ac.uk/idcard/statusreport.pdf.

15. Privacy International, *PHR2004 report:- People's Republic of China*. Студија је преузета са адресе: http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-83511.

16. Privacy International, *PHR2004 report: Malaysia.* Студија је преузета саадресе:http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-83539.

17. Privacy International & EPIC, *PHR Privacy and Human rights Report 2005*. Студија је преузета са адресе: http://www.privacyinternational.org/article.shtml?%20cmd[347]=x-347-542783&als[theme]=Privacy%20and%20Human%20Rights.

18. Schmitz, Patrice-Emmanuel, Roberto Tavano, Juliet Lodge, Ronald Huijgens & al., *Biometrics in Europe - Trend Report 2006*, Брисел 2006. Студија је преузета са адресе: http://www.europeanbiometrics.info/images/resources/112_165_file.pdf.

19. Standing Committee on Citizenship and Immigration, *A national identity card for Canada?,* 2003. Извештај је преузет са адресе: http://cmte.parl.gc.ca/Content/HOC/committee/372/cimm/reports/rp1085068/cimmrp06/cimmrp06-e.pdf.

20. Станковић, Обрен, Владимир Водинелић, *Увод у грађанско право*, НОМОС, Београд 1996, стр. 120.

21. Twight, Charlotte, *Limited Government, Ave Atque Vale*, Independent Review, Volume X, No. 4, Spring 2006, Oakland, CA, USA. Рад је преузет са адресе: http://www.independent.org/pdf/tir/tir_10_4_01_twight.pdf.

22. Whitley, Edgar A., Ian R. Hosein, Ian O. Angell, Simon Davies, *Reflections on the academic policy analysis proces and UK Identity Card scheme*, Department of Information Systems LSE, Лондон 2006. Студија је преузета са адресе: http://is2.lse.ac.uk/wp/pdf/wp147.pdf.

23. Зизиулас, Јован, *Догматске теме*, Беседа, Нови Сад, 2001.

Документи, правна акта и званична саопштења

1. Council od the European Union, Directive …/…/EC Of the European Parliament and of the Council, *9010/1/06*, Press Release, Брисел, 18. септембар 2006. Документ је преузет са адресе: http://www.statewatch.org/news/2006/dec/eu-driving-licences-proposal-9010-rev1-06.pdf

2. Council od the European Union, *15801/0*6, Press Release, 2768th Council Meeting, Justice and Home Affairs. Документ је преузет са адресе: http://www.statewatch.org/news/2006/dec/jha-dec-prel.pdf.

3. Department of State, *Federal Register Vol. 70, No. 33*, 18. 02. 2005. Документ је преузет са адресе: http://a257.g.akamaitech.net/7/257/2422/01jan20051800/edocket.access.gpo.gov/2005/05-3080.htm.

4. FIDIS, *Budapest Declaration on Machine Readable Travel Documents (MRTDs)*, 08. 11. 2006. Документ је преузет са адресе: http://www.fidis.net/fileadmin/fidis/press/budapest_declaration_on_MRTD.en.20061106.pdf.

5. House of Commons, „Home Affairs - Minutes of Evidence“, 11. 12. 2003. Документ је преузет са адресе: http://www.publications.parliament.uk/pa/cm200304/cmselect/cmhaff/130/3121101.htm

6. ICAO, *Doc 9303*. Документ је преузет са адресе: http://www.icao.int/mrtd/publications/doc.cfm.

7. IDABC, „Flemish project addresses privacy shortcomings of Belgian e-ID card“, 12. 10. 2005. Саопштење преузето са адресе: http://ec.europa.eu/idabc/en/document/4983/332.121

8. MUP Republike Hrvatske, Закона о особној исказници, на адреси: http://www.mup.hr/91.aspx.

9. МУП Републике Србије, „Саопштење 01.broj: 32/05“, 1. 03. 2005. Саопштење је преузето са адресе http://www.mup.sr.gov.yu/domino%5Carhiva.nsf/1mart05mup.

10. МУП Републике Србије, „Veliki korak u modernizaciji rada policije“, 4.12.2003 – KZN. Саопштење је преузето са адресе: http://www.mup.sr. gov.yu/domino%5Carh.nsf/4122003.

11. OHR Political Department, „BiH Citizen Identity Card“, Саопштење је преузето са адресе: http://www.ohr.int/ohr-dept/pol/spu/lprojects/default.asp?content_id=5844.

12. Парламент Републике Словеније, *Zakon o osebni izkaznici,* ZOIzk-UPB1. Документ је преузет са адресе http://www.uradni-list.si/1/ulonline.jsp?urlid=2005100&dhid=78815

13. Парламент Републике Србије, *Закон о личној карти*. Документ је преузет са адресе: http://www.parlament.sr.gov.yu/content/cir/akta/akta_detalji.asp?Id=372&t=Z.

14. Privacy International, „Canadian parliamentary report ridicules id cards as pointless, costly and dangerous“, Media release, 08. 10. 2003. Извештај је преузет са адресе: http://www.privacyinternational.org/article.shtml?%20cmd[347]=x-347-183137&als[theme]=ID%20Around%20the%20World.

15. Privacy International, „French report highly critical of new French ID Card project“. Извештај је преузет са адресе: http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-247752&als[theme]=ID%20Around%20the%20World.

16. Privacy International, „Japanese Court Rules ID System Unconstitutional“. Извештај је преузет са адресе: http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-228843&als[theme]=ID%20Around%20the%20World.

17. Privacy International, „Taiwan Constitutional Court places fingerprinting plan on hold“, 22. 06. 2005. Вест је преузета са адресе: http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-249615.

18. Privacy International, „UK Government narrowly wins ID card bill“, 30. 03. 2006. Извештај је преузет са адресе: http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-531723.

19. Privacy International „US State of Georgia passes law banning fingerprints in licenses“, 08. 04. 2005. Вест је преузета са адресе: http://www.privacyinternational.org/article.shtml?%20cmd[347]=x-347-180966&als[theme]=ID%20Around%20the%20World.

20. SFOR, *Transcript - Press Conference 25. 2. 2002*, Coalition Press Information Center. Документ је преузет са адресе: http://www.nato.int/sfor/trans/2003/t030225a.htm.

21. Statewatch, „EU: Biometrics - from visas to passports to ID cards“, 2005. Извештај је преузет са адресе: http://www.statewatch.org/news/2005/jul/09eu-passports-id-cards.htm.

22. Statewatch, „EU: Fingerprinting of children - the debate goes on“, 2005. Извештај је преузет са адресе: http://www.statewatch.org/news/2006/aug/02eu-fingerprinting-children.htm.

23. Statewatch, „EU states will be free to fingerprint children from day one of their life as soon as it is technologically possible“, 2006. Извештај је преузет са адресе: http://www.statewatch.org/news/2006/jul/08fingerprinting-children.htm.

24. The Maine Senat Democrats, „Joint Resolution Memorializing the President of the United States and the Congress of the United States to Repeal the Real ID of 2005“. Документ је преузет са адресе: http://www.mainesenate.org/mitchell/realid.htm.

25. Влада Републике Естоније, „ID Card Issuing Statistics“. Званична статистика преузета је са адресе: http://www.id.ee/pages.php/03030102.

26. Влада Републике Србије „Биометријски чипови неће бити обавезан део нових личних карата“. Изјава је преузета са адресе http://www.srbija.sr.gov.yu/vesti/vest.php?id=62527.

27. Влада Републике Србије, „Јочић образложио Предлог закона о личној карти“. Саопштење је преузето са адресе: http://www.srbija.sr. gov.yu/vesti/vest.php?id=51662.

28. Влада Републике Србије, *Уредба о упису података у образац личне карте*, 11. 01. 2007. под бројем 05 Број: 110-320/2007. Документ је преузет са адресе: http://www.srbija.sr.gov.yu/vesti/dokumenti_pregled.php?id=62625.

29. Vlada Republike Crne Gore, *Nacrt Zakona o ličnoj karti*. Документ је преузет са адресе: http://www.gom.cg.yu/files/1103905246.doc.

30. „Жички апел“,(Закључци стручног скупа у Жичи од 25. марта 2005) *Жички Благовесник (Хроника најављеног слободоубиства)*, епархија жичка, јул 2006.

31. „Тражимо алтернативни модел идентификације“, (Закључци стручног скупа у Краљеву од 1. октобра 2006), *Православље* бр. 950.

Стручни чланци и есеји

1. Accenture Technology Labs, „The future of identity: Biometrics solutions to enhance the performance of businesses and governments“. Проспект је преузет са адресе: http://www.accenture.com/xdoc/en/services/technology/vision/future_identity.pdf.

2. Булатовић, Душан, *Smart картице и сигурност података у њима.*

3. Bunyan, Tony „While Europe sleeps“, *ECLN Essays no. 11*, 2005. Ecej je преузет са адресе: http://www.statewatch.org/news/2005/oct/ecln/essay-11.pdf.

4. Canadian Internet Policy and Public Interest Clinic, „How reliable are biometric systems?“. Чланак је преузет са адресе: http://www.cippic.ca/en/faqs-resources/biometrics/#faq_how-reliable-bio-systems.

5. Canadian Internet Policy and Public Interest Clinic, „National ID Cards“. Чланак је преузет са адресе: http://www.cippic.ca/en/faqs-resources/national-id-cards.

6. Clarke, Roger, „Authentication: A Sufficiently Rich Model to Enable e-Business“, верзија од 26. децембра 2001. Рад је преузет са адресе: http://www.anu.edu.au/people/Roger.Clarke/EC/AuthModel.html.

7. Clarke, Roger, „Biometrics and Privacy“, верзија од 15. априла 2001. Рад је преузет са адресе: http://www.anu.edu.au/people/Roger.Clarke/DV/Biometrics.html.

8. Clarke, Roger, „Biometrics' Inadequacies and Threats, and the Need for Regulation“, верзија од 15. априла 2002. године. Чланак је преузет са адресе: http://www.anu.edu.au/people/Roger.Clarke/DV/BiomThreats.html.

9. Clarke, Roger, „Biometric Insecurity“, верзија од 14. маја 2004. Чланак је преузет са адресе: http://www.anu.edu.au/people/Roger.Clarke/DV/AusCERT0405.html.

10. Clarke, Roger, „Chip-Based ID: Promise and Peril“, верзија од 27. септембра 1997. Рад је преузет са адресе: http://www.anu.edu.au/people/Roger.Clarke/DV/IDCards97.html.

11. Clarke, Roger, „Five Most Vital Privacy Issues“, верзија од 31. јула 1997. Чланак је преузет са адресе: http://www.anu.edu.au/people/Roger.Clarke/DV/VitalPriv.html.

12. Clarke, Roger, „Identification and Authentication Fundamentals“, верзија од 22. августа 2003. Чланак је преузет са адресе: http://www.anu.edu.au/people/Roger.Clarke/DV/clpc030908.html.

13. Clarke, Roger, „Message Transmission Security“, верзија од 11. маја 1998. Рад је преузет са адресе: http://www.anu.edu.au/people/Roger.Clarke/II/CryptoSecy.html.

14. Clarke, Roger, „Promises and Threats in Electronic Commerce“, верзија од 13. августа 1997. Рад је преузет са адресе: http://www.anu.edu.au/people/Roger.Clarke/EC/Quantum.html.

15. Clarke, Roger, „The Scope for Privacy-Sensitive Biometric Architecture“, верзија од 23. фебруара 2003, http://www.anu.edu.au/people/Roger.Clarke/DV/BioArch.html.

16. Clarke, Roger, „Why Biometrics Must Be Banned“, верзија од 25. августа 2003. Чланак је преузет са адресе: http://www.anu.edu.au/people/Roger.Clarke/dv/Biom030908.html.

17. Clement, Andrew, Felix Stalder, Jeff Johnson, Robert Guerra, „National Identification Schemes (NIDS) and the Fight against Terrorism: Frequently Asked Questions“, v1.2, 27. 11. 2001. Чланак је преузет са адресе: http://www.cpsr.org/issues/privacy/natidfaq.

18. Davies, Simon G., „Touching Big Brother: How biometric technology will fuse flesh and machine“, Privacy international, 1996. Чланак је преузет са адресе: http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-61904.

19. EPIC, „National ID Cards and REAL ID Act“. Рад је преузет са адресе: http://www.epic.org/privacy/id_cards/.

20. EPIC, „Your Papers, Please: From the State Drivers Licence to a National Identification Systtem“. Чланак је преузет са адресе: http://www.epic.org/privacy/id_cards/yourpapersplease.pdf.

21. EPIC, „United States Visitor and Immigrant Status Indicator Technology: (US-VISIT)“. Чланак је преузет са адресе: http://www.epic.org/privacy/us-visit/.

22. Fussell, Jim, „Group Classification on National ID Cards as a Factor in Genocide and Ethnic Cleansing“. Чланак је преузет са адресе: http://www.preventgenocide.org/prevent/removing-facilitating-factors/IDcards/.

23. Greenleaf, Graham, Roger Clarke, „Privacy Implications of Digital Signatures“, верзија од 10. марта 1997. Рад је преузет са адресе: http://www.anu.edu.au/people/Roger.Clarke/DV/DigSig.html

24. Матица српска, „Језичке недоумице“, *Језик данас*, бр. 17. Часопис је преузет са адресе: http://www.maticasrpska.org.yu/download/danas17.pdf.

25. Mason, Stephen, „Is there a need for identity cards?“. Чланак је преузет са адресе: http://www.compseconline.com/free_articles/cfs_IDcards.pdf.

26. Nešić, Sunčica, Vojkan Nikolić, „Elektronski identitet građana i mogućnosti njegove primene“, Београд 2006.

27. Rotenberg, Marc, „Real ID, Real Trouble?“, Communications of the ACM, Vol. 49, No. 3. Чланак је преузет са адресе: www.epic.org/privacy/id_cards/mr_cacm0306.pdf.

28. Toth, Bori, „Biometric ID Card Debates“, *Deloitte*, 2005. Чланак је преузет са адресе: http://www.deloitte.com/dtt/cda/doc/content/uk_ta_idcarddebates_june05.pdf.

29. Watkins, Marc, „What are biometric systems?“. Чланак је преузет са адресе: http://www.cippic.ca/en/faqs-resources/biometrics/#faq_what-are-bs.

Стручна излагања и предавања

1. van Arkel, Jan, „Common requirements for (global) interoperable eID“, излагање на конференцији Porvo9, Љубљана, 11-12. мај 2006. Сиже је преузет са адресе: http://porvoo9.gov.si/pdf/fri_17_1130_JvanArkel_Porvoo9.pdf.

2. Clarke, Roger, „Dataveillance – 15 Years On“, Privacy Issues Forum, Wellington NZ, 28. март 2003. Документ је преузет са адресе: http://www.anu.edu.au/people/Roger.Clarke/DV/dvnz03.html.

3. Clarke, Roger, „Research for eGovernment Key Issues“, предавање на форуму eGovernment Consultation Workshop 7th Framework Programme for Information Society Technologies, Брисел 26–27. октобра 2005. Ауторизовано предавање је преузето са адресе: http://www.anu.edu.au/people/Roger.Clarke/EC/eGovRes0510.html.

4. Crompton, Malcolm, „Biometrics and Privacy: The End of The World as We Know It or The White Knight of Privacy?“, ауторизовано излагање на конференцији Biometrics – Security and Authentication, Сиднеј, 20. март 2002. Документ је преузет са адресе: http://www.privacy.gov.au/news/speeches/sp80notes.pdf .

5. Gaston, Lorenzo, „cen/ts 15480 standard European Citizen Card Progress“, излагање на конференцији Porvoo9, Љубљана, 11-12. мај 2006. Сиже је преузет са адресе: http://porvoo9.gov.si/pdf/fri_14_0930_LGaston_eccmay_12.pdf.

6. Gil Bernabeu, „Global Platform Technical Activities for ID“, излагање на конференцији Porvoo9, Љубљана, 11-12. мај 2006. Сиже је преузет са адресе: http://porvoo9.gov.si/pdf/thu_13_1635_GBernabeu_GlobalPlatform_Porvoo9.pdf .

7. Grossman, Wendy M., „Identifying Risks: National Identity Cards“, ауторизована верзија предавања одржаног на Универзитету у Единбургу, 19. јануар 2005. Документ је преузет са адресе: http://www.law.ed. ac.uk/ahrb/script-ed/vol2-1/idcards.pdf.

8. Kričej, Dušan, „E-Governmentin Slovenia, Bestpractice“, излагање на конференцији Porvoo9, Љубљана, 11-12. мај 2006. Сиже је преузет са адресе: http://porvoo9.gov.si/pdf/thu_01_0915_DKricej_Porvoo9.pdf.

9. Küster, Ronald, Wolfgang P. Schulz, *Biometric Identity - Privacy, Risks and Law*, Work paper, излагање на конференцији 2nd Biennial congress on the law of the world, Пекинг, 4-10. септембар 2005. Документ је преузет са адресе: http://www.europeanbiometrics.info/images/news/24_857_file.pdf.

10. Leitold, Herbert, „European Electronic Identity Practices, Country Update of Austria“, излагање на конференцији Porvoo9, Љубљана, 11-12. мај 2006. Сиже је преузет са адресе: http://porvoo9.gov.si/pdf/thu_11a_1400_Country_update_Austria.pdf.

11. Loukidelis, David, „Privacy and Security: Seeking a Middle Path“. Ауторизовано излагање на 5th Annual CACR/Ontario IPC, Универзитет у Торонту, 28-29. октобра 2004. Документ је преузет са адресе: http://www.oipcbc.org/publications/speeches_presentations/CACRspeech102704.pdf

12. Marković, Nikola, Milan Marković, „Uvođenje i prednosti elektronskog poslovanja i elektronskog potpisa - normativno regulisanje -“, излагање на првом југословенском симпозијум о електронској трговини под називом “E-Trgovina 2001”, 29. 05. 2001, Novi Sad.

13. Mattatia, Fabrice, „European Electronic Identity Practices, Country Update of France“, излагање на конференцији Porvo9. Сиже излагања преузет са адресе http://porvoo9.gov.si/pdf/THU_11d_Country_update_France.pdf.

14. Nagaaki Ohyama, „New e-Japan strategy and unified eI Dunder discussion“. излагање на конференцији Porvoo9, Љубљана, 11-12. мај 2006. Сиже излагања је преузет са адресе: http://porvoo9.gov.si/pdf/thu_08_1130_nohyama_nicss_porvoo9.pdf.

15.Robroch, Harko, „ePassport Privacy Attack“. Излагање је преузето са адресе: www.riscure. com/2_news/200604%20CardsAsiaSing%20ePassport%20Privacy.pdf.

16. Shroff, Marie, „Trans Tasman Standardisation for Biometrics“, ауторизовано излагање у оквиру групне теме, 1. октобар 2004, Конвенциони центар, Велингтон, Нови Зеланд, стр. 1. Документ је преузет са адресе: www.privacy.org.nz/filestore/docfiles/652009.pdf.

Текстови из стручних часописа

1. Balaban, Dan, „Grand vision or grand illusion?“, *CardTechnology*, јануар 2006. Часопис преузет са адресе: http://www.cardtechnology.com/attachments/20060130hmfkesir-1-ct_jan_2006.pdf.

2. Balaban, Dan, Don Davis, Thad Rueter, Kevin Woodward, „The future of smart cards – Top 10 trends“, *CardTechnology*, март 2006. Часопис је преузет са адресе: http://www.cardtechnology.com/attachments/200604054yolcsdx-1-ct_march_2006.pdf.

3. Davis, Donald, „Will That Be Cash, Card Or Finger?“, *CardTechnology*, мај 2006. Часопис је преузет са адресе: http://www.cardtechnology.com/attachments/200605319z8l4fwd-1-ct_may_2006.pdf.

4. Diaz, Claudia, „Privacy risk scenario“, *D2.6: Identity in a Networked World – Use Cases and Scenarios*, FIDIS, август 2006. Брошура је преузета са адресе: https://prof.hti.bfh.ch/arb1/FIDIS/fidis.pdf.

5. Марковић, Милан, „Elektronski potpis u Srbiji“. Текст је преузет са адресе: http://www.emagazin.co.yu/clanak.asp?id=453.

6. Nikitović, Branko, „Digitalni serfitikati“, *PC*, бр. 129, PC Press, Beograd, 2007.

7. Nikitović, Branko, „Put do sigurnih podataka“, *PC*, бр. 128, PC Press, Beograd, 2007.

8. Scheeres, Julia, „ID Cards Are de Rigueur Worldwide“, *Wired*, 25. 09. 2001, на адреси http://www.wired.com/news/conflict/0,2100,47073,00.html.

9. Schneier, Bruce, „Fatal Flaw Weakens RFID Passports“, *Wired*, 2. 11. 2006. Чланак је преузет са адресе: http://www.wired.com/news/technology/0,69453-0.html.

10. Woodward, Kevin, „Deadline Nears For U.S. Federal Employee ID“, antrfile „Getting Good E-Passport Photos is Tougher than Imagined“, *CardTechnology*, мај 2006. Часопис је преузет са адресе: http://www.cardtechnology.com/attachments/200605319z8l4fwd-1-ct_may_2006.pdf

11. Woodward, Kevin, „Directory Holds The Key To E-Passport Authentication “, *Card Technology*, септембар 2006. Часопис је преузет са адресе: http://www.cardtechnology.com/attachments/200609198f8hr24y-1-ct_sept_2006.pdf.

12. Woodward, Kevin, „Electronic Passports: Is a Global Certification Body Necessary?“, *CardTechnolog*y, април 2006. Часопис је преузет са адресе: http://www.cardtechnology.com/attachments/20060516n1xjiwx3-1-ct_april_2006.pdf.

13. Woodward, Kevin „E-Passports Await Real-World Tests“, *CardTechnology*, март 2006. Часопис је преузет са адресе: http://www.cardtechnology.com/attachments/200604054yolcsdx-1-ct_march_2006.pdf.

14. Woodward, Kevin, „How Smart Card Chips Found Their Way Into Passports“, *CardTechnology*, јун-јул 2006. Часопис је преузет са адресе: http://www.cardtechnology.com/attachments/20060721pv67v73z-1-ct_june_2006.pdf.

15. „Smart Cards Win Some, Lose One, In U.S.“, (непотписан чланак), *Global Newswatch*, *CardTechnology*, новембар 2006. Часопис је преузет са адресе: http://www.cardtechnology.com/attachments/20061218lzr1p6co-1-ct_nov_2006.pdf.

16. „The Month: Researchers raise concern over RFID security“, (непотписан чланак), *SC Magazine*. Текст је преузет са адресе http://www.scmagazine.com.au/feature/3067,the-month-researchers-raise-concern-over-rfid-security.aspx.

Секундарна литература

Текстови из стране штампе

1. Benedictus, Leo, „A brief history of the passport“, *The Guardian*, 17. 10. 2006. Текст је преузет са адресе: http://travel.guardian.co.uk/article/2006/nov/17/travelnews.

2. Boggan, Steve, „Recall demand after cloning of new biometric passports“, *The Guardian*, 17. 11. 2006. Чланак је преузет са адресе: http://www.guardian.co.uk/idcards/story/0,,1950229,00.html.

3. Horn, Kahentinetha, „Smart Cards to be tried on Mohawks and Crees “. Чланак је преузет са адресе: http://noii-van.resist.ca/smart_cards.html, MNN Mohawk Nation News.

4. Johnston, Philip, „Millions may resist database, says poll“, *Telegraph*, 5.12.2006. Чланак је преузет са адресе: http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2006/12/04/ndata04.xml.

5. Leigh, David, Rob Evans, „Warning over privacy of 50m patient files“, *The Guardian*, 1. новембар 2006. Чланак је преузет са адресе: http://society.guardian.co.uk/health/news/0,,1936403,00.html.

6. Owen, Janette, „Where do we stand on fingerprinting pupils?“, *The Guardian*, 21. 11. 2006. Текст је преузет са адресе: http://education.guardian.co.uk/schools/teach/story/0,,1952673,00.html.

7. Peev, Gerri, „ID cards will lead to ’massive fraud’“, *The Scotsman*, 18. 10. 2005. Чланак је преузет са адресе: http://news.scotsman.com/index.cfm?id=2103982005.

8. Schneier, Bruce, „The ID Chip You Don’t Want in Your Passport“, *Washington Pos*t. Чланак је преузет са адресе: http://www.schneier.com/essay-125.html.

9. Whitley, Edgar A., „Mistaken identity“, *The Parliamentary Monitor*, јун/јул 2006. Текст је преузет са адресе: http://www.csrc.lse.ac.uk/idcard/parlmon.pdf.

10. Wintour, Patrick, „ID cards ‘will reveal details of daily life’“, *The Guardian*, 28. 06. 2005. Текст је преузет са адресе: http://www.guardian.co.uk/idcards/story/0,15642,1516115,00.html.

11. „Analyst Sees Boom In Identity And Biometric Projects“, (непознат аутор), *CardTechnology*. Вест је преузета са адресе адресе: http://www.card-technology.com/article. html?id=20060921GD6L6J83.

12. „Cracked it! “, (непотписан чланак), *The Guardian*, 17. 11. 2006. Текст је преузет са адресе: http://www.guardian.co.uk/idcards/story/0,,1950226,00.html.

13. „Public revolt quashes biometric ID chips“, *WorldNetDaily*, (непотписан чланак), 27. 01. 2007. Чланак је преузет са адресе: http://wnd.com/news/article.asp?article_id=53945.

Текстови из домаће штампе

1. Čolak, J. „Pretnja religijskim demonstracijama `krvavijim od političkih`“, Danas, 20. 07. 2006. Чланак је преузет са адресе: http://www.danas.co.yu/20060720/hronika2.html.

2. Đurić, O, „Strah od čipa u ličnoj karti“, 24 sata, 9.11.2006.

3. Korać, Žarko, „Pravoslavlje i čipovi“, 17. 07. 2006. Текст је преузет са адресе: http://www.nezavisne.com/dnevne/stav/st07182006-01.php.

4. Краљевић, Ср, „Чип изгубио битку“, Вечерње новости. Чланак је преузет са адресе: http://www.novosti.co.yu/code/navigate.php?Id=4&status=jedna&vest=98627&datum=2007-01-13, објављени су 13. 01. 2007.

5. K.P, „Nezakonit tender za opremu MUP-a“, Blic, 30.9.2004. Чланак је преузет са адресе: http://www.blic.co.yu/blic/arhiva/2004-09-30/strane/tema.htm#1.

6. Lasić, Mile, „Verska pripadnost kao znak terorista“, Danas, 8. септембар 2006. Текст је преузет са адресе: http://www.danas.co.yu/20060908/evropa1.html.

7. Макара, Петар, „`Pametna karta` za glupe Srbe“. Текст је преузет са адресе: http://www.vidovdan.org/article592.html.

8. Марковић, Никола, „Konačno! Usvojen zakon“, EBIT , бр. 36. Текст је преузет са адресе http://www.ekonomist.co.yu/magazin/ebit/36/por/por2.htm.

9. Pančić, Teofil, „Nečastiva lična karta“, Pobjeda, 29. 07. 2006.

10. Пешић, Миленко, „Чип није обавезан“, Политика. Чланак је преузет са адресе: http://www.politika.co.yu/detaljno.php?nid=16941. 12. 1. 2006.

11. R.D, „Motoroli i Arijusu isti posao? “, Danas, 10.12. 2003. Чланак је преузет са адресе: www.danas.co.yu/20031210/frontpage1.html.

12. Stamenić, S, „Lične karte ipak bez čipa“, 12. 1. 2007, Danas. Чланак је преузет са адресе: http://www.danas.co.yu/20070112/dogadjajdana1.html#0.

13. Stamenić, S, „Utvrditi odgovornost za kupovinu opreme koja godinama stoji po magacinima“, Danas, 13. 01. 2007. Чланак је преузет са адресе: http://www.danas.co.yu/20070113/dogadjajdana1.html#2.

14. Суботић, Оливер, „Forumom protiv istine“, Нова српска политичка мисао. Текст је преузет са адресе: http://www.nspm.org.yu/prenosimo2006/2006_subotic1.htm.

15. Шабић, Родољуб, „Опасност злоупотребе“, Политика, 10. 08. 2006.

16. Туба, Милан, „Какве нас све лепоте очекују када се реинтегришемо у међународну заједницу“, Правда, септембар 1994.

17. V. R., „Hakeri mogu da kloniraju čipove sa ličnim podacima“, Danas, Com_Media, 09. 08. 2006. Текст је преузет са адресе: http://www.danas.co.yu/20060809/commedia1.html.

18. Z.Ž., „Sporedni ulazi“, EBIT, бр. 29. Текст је преузет са адресе: http://www.ekonomist.co.yu/magazin/ebit/29/pra/pra2.htm.

19. „3D biometrija“, (непознати аутор), *Svet kompjutera* 4/2005, стр. 6.

20. „Inspektori Ministarstva finansija Srbije o odlivu kapitala vrednog više od milijardu evra“, *Transparentnost Srbija*, вест пренета из Вечерњих новости од 30. 09. 2004. Текст је преузет са адресе: http://www.transparentnost.org.yu/ts_mediji/stampa/2004/septembar_2004/3009-04.html

21. „Nezakonito uzimanje ličnih podataka u novosadskoj firmi“, (непознат аутор), Kurir, 3. 09. 2006.

22. „Veliko oko“, Press, 10. 11. 2006.

23. „Građani Srbije imaće uskoro elektronska dokumenta“, (преузето од Политике, Душан Телесковић, 10. 06. 2006). Текст је преузет са адресе http://www.konekta. net/sr/index.php?read=13.

Материјали новинских агенција и информативних портала

1. BETA, „Lične karte ipak bez čipa“, 11. 01. 2007. Вест је преузета са адресе: http://www.beta.co.yu/default.asp?m=Vesti%20dana,ves&j=sr&h=Home,sr&prikaz=1566951.

2. European Biometrics Portal, „Australia implement biometrics for immigration“, 22. 09. 2006. Вест је преузета са адресе: http://www.europeanbio-

metrics.info/news/newsdetail.php?Id_news=280.

3. European Biometrics Portal, „Biometric IDs to be Widely Availabe in 3 Years“, 29. 05. 2006. Анализа је преузета са адресе: http://www.europeanbiometrics.info/news/newsdetail.php?Id_news=172.

4. European Biometrics Portal, „Biometric passports introduced in Sweden and Norway“, 07. 10. 2005. Вест је преузета са адресе: http://www.europeanbiometrics.info/news/newsdetail.php?Id_news=31.

5. European Biometrics Portal, „Canada: Biometrics in favour, poll shows“, 02. 10. 2006. Резултат истраживања је преузет са адресе: http://www.europeanbiometrics.info/news/newsdetail.php?Id_news=287.

6. European Biometrics Portal, „Canada tests biometrics in immigration field trial“, 14. 06. 2006. Вест је преузета са адресе: http://www.europeanbiometrics.info/news/newsdetail.php?Id_news=191.

7. European Biometrics Portal, „Debate on Biometrics on National ID Cards“, 25. 08. 2006. Текст је преузет са адресе: http://www.europeanbiometrics.info/news/newsdetail.php?Id_news=250.

8. European Biometrics Portal, „Gemalto develops the first smart card-based e-government solution ever in the Middle East“, 21. 09. 2006. Вест је преузета са адресе: http://www.europeanbiometrics.info/news/newsdetail.php?Id_news=269.

9. European Biometrics Portal, „Greece set for ePassports“, 09. 05. 2006. Вест је преузета са адресе: http://www.europeanbiometrics.info/news/newsdetail.php?Id_news=157.

10. European Biometrics Portal, „eID card is launched in Spain“, 20. 03. 2006. Вест је преузета са адресе: http://www.europeanbiometrics.info/news/newsdetail.php?Id_news=132.

11. European Biometrics Portal, „Exploring traveller's biometric data sharing“, 02. 11. 2006. Текст је преузет са адресе: http://www.europeanbiometrics.info/news/newsdetail.php?Id_news=319

12. European Biometrics Portal, „Finnish Police take delivery of new AFIS“, 28. 04. 2006. Вест је преузета са адресе: http://www.europeanbiometrics.info/news/newsdetail.php?Id_news=152.

13. European Biometrics Portal, „New AFIS in Ireland“, 04. 12. 2006. Вест је преузета са адресе: http://www.europeanbiometrics.info/news/newsdetail.php?Id_news=351.

14. European Biometrics Portal , „New ID Biometrics in Morocco“, 05. 10. 2005. Вест је преузета са адресе: http://www.europeanbiometrics.info/news/newsdetail.php?Id_news=28.

15. European Biometrics Portal, „Opinion: Biometrics gain British citizens approval“, 24. 10. 2006. Анализа је преузета са адресе: http://www.europeanbiometrics.info/news/newsdetail.php?Id_news=308.

16. European Biometrics Portal, „Opportunity of Mega ID database questionned in UK“, 21. 12. 2006. Вест је преузета са адресе: http://www.europeanbiometrics.info/news/newsdetail.php?Id_news=359.

17. European Biometrics Portal, „Pilot project for biometric passports in Switzerland“, 05. 09. 2006. Вест је преузета са адресе: http://www.europeanbiometrics.info/news/newsdetail.php?Id_news=258.

18. European Biometrics Portal, „Swiss citizens may ‘opt-out’ of biometric passports until 2011“, 08. 09. 2005. Вест је преузета са адресе: http://www.europeanbiometrics.info/news/newsdetail.php?Id_news=21.

19. European Biometrics Portal, „UK’s debate: ID cards biometrics will not stop forgery“, 20. 2. 2006. Текст је преузет са адресе: http://www.europeanbiometrics.info/news/newsdetail.php?Id_news=113.

20. European Biometrics Portal, „UK Home Office advisor urges biometrics testing“, 23. 10. 2006. Прилог је преузет са адресе: http://www.europeanbiometrics.info/news/newsdetail.php?Id_news=311.

21. European Biometrics Portal, „UK House of Commons passes ID Cards Bill“, 18. 10. 2005. Вест је преузета са адресе: http://www.europeanbiometrics.info/news/newsdetail.php?Id_news=44.

22. European Biometrics Portal , „UK: Liberal Democrats urge citizens to renew their passports“, 25. 05. 2006. Вест је преузета са адресе: http://www.europeanbiometrics.info/news/newsdetail.php?Id_news=181.

23. European Biometrics Portal, „UK National Identity Register on its way“, 26. 09. 2006. Вест је преузета са адресе: http://www.europeanbiometrics.info/news/newsdetail.php?Id_news=282.

24. EDRI, „Campaign launched in UK to opt out of central medical database“,EDRI-gram 4.23, 6. децембар 2006. Текст је преузет са адресе: http://www.edri.org/edrigram/number4.23/uk_medical_database.

25. EDRI , „FIPR report on children’s databases - likely to harm rather than help“, EDRI-gram 4.22, 22 новембар 2006. Прилог је преузет са адресе: http://www.edri.org/edrigram/number4.22/fipr-children-database.

26. EDRI, „French campaign against biometric ID card“, EDRI-gram 3.11, 02. 06. 2005. Вест је преузета са адресе: http://www.edri.org/edrigram/number 3.11/biometrics

27. EDRI, „French minister demands compulsory biometric ID“, EDRI-gram 3.8. Вест је преузета са адресе: http://www.edri.org/edrigram/number3.8/ID

28. EDRI, „New biometric passports in Slovenia, као и Passports with biometrics for Romanians“. Вест је преузета са адресе: http://www.edri.org/edrigram/number4.9/passports.

29. EDRI, „Passports with biometrics for Romanians“. Вест је преузета са адресе: http://www.edri.org/edrigram/number4.9/passports.

30. EDRI, „Privacy Commissioners act together“, EDRI-gram4.21, 8. 11. 2006. Вест је преузета са адресе: http://www.edri.org/edrigram/number4.21/privacy.

31. EDRI, „UK DNA Database under scrutiny“, *EDRI-gram 4.21,* 8. 11. 2006. Текст је преузет са адресе: http://www.edri.org/edrigram/number4.21/uk-dan.

32. Engadget, „Dutch RFID e-passport cracked - US next?“. Вест је преузета са адресе http://www.engadget.com/2006/02/03/dutch-rfid-e-passport-cracked-us-next/.

33. Heise online, „Bundesrat gives the green light to identity number“, 07. 11. 2006. Вест је преузета са адресе: http://www.heise.de/english/newsticker/news/80622.

34. HPC wire, „Motorola Gives Serbia $21 Million For Integrated ID System“. Вест је преузета са адресе: http://www.taborcommunications.com/hpcwire/hpcwirewww/03/1010/106157.html.

35. Mikro, „Neizvesna sudbina britanskog Zakona o izdavanju biometrijskih ID kartica“, 17. 03. 2005. Вест је преузета са адресе: http://www.mikro.co.yu/ser/vesti/vesti.php?datum=2005-03-17&ID=6852.

36. Mikro, „Nemačka usvojila plan o biometrijskim pasošima“, 25. 07. 2005. Вест је преузета са адресе: http://www.mikro.co.yu/ser/vesti/vesti.php?datum=2005-07-25&ID=7234.

37. Mikro, „Počinje izdavanje RFID pasoša u SAD“, 31. 07. 2006. Вест је преузета са адресе: http://www.mikro.co.yu/ser/vesti/vesti.php?datum=2006-07-31&ID=8271.

38. Mikro, „SAD odložile uvodjenje biometrijskih pasoša“, 16. 05. 2005. Вест је преузета са адресе: http://www.mikro.co.yu/ser/vesti/vesti.php?datum=2005-06-16&ID=7140.

39. SecurelDNews, „Thailand introduces national ID with biometric technology“, 15. 04. 2005. Вест је преузета са адресе: http://www.secureidnews.com/weblog/2005/04/15/thailand-introduces-national-id-with-biometric-technology/.

40. Southeast European Times, „Nove bugarske lične karte polovinom 2007. godine“, 13. 11. 2006. Вест је преузета са адресе: http://www.setimes.com/cocoon/setimes/xhtml/sr_Latn/newsbriefs/setimes/newsbriefs/2006/11/13/nb-05

41. Statewatch, „EU: Biometrics and national ID cards back on the table“. Текст је преузет са адресе: http://www.statewatch.org/news/2006/jul/09eu-id-cards.htm.

42. Statewatch, „EU: Biometrics - from visas to passports to ID cards“, 2005. Текст је преузет са адресе: http://www.statewatch.org/news/2005/jul/09eu-passports-id-cards.htm.

43. Танјуг, „MUP-Mihajlovic: Novi informacioni sistem poboljsace sigurnost gradjana “, 11. 09. 2003. Вест је преузета са адресе: http://www.mfa.gov.yu/Srpski/Bilteni/Srpski/b120903_s.html#N25.

44. Travelbite, „Scandinavian airline first to use fingerprint scans“, 22. септембар 2006. Вест је преузета са адресе: http://www.travelbite.co.uk/newsbrief/flights/scandinavian-airline-first-use-fingerprint-scans-$452572.htm.

45. USA Today, „Joining USA, Japan to fingerprint and photograph foreign visitors“, 17. 05. 2006. Вест је преузета са адресе: http://www.usatoday.com/travel/news/2006-05-17-japan-fingerprint_x.htm?csp=34 .

46. ZDNet Australia, „Senate passes passport biometric, RFID legislation“. Вест је преузета са адресе: http://www.zdnet.com.au/news/security/soa/Senate_passes_passport_biometric_rfid_legislation/0,130061744,139180464,00.htm.

Извештаји електронских медија

1. B92, „Elektronske lične karte u Srbiji?“. Вест је преузета са адресе: http://www.b92.net/info/vesti/index.php?yyyy=2006&mm=06&dd=09&nav_id=200511.

2. BBC, „ID cards are of ’limited value’“, 29. 01. 2006. Прилог је преузет са адресе: http://news.bbc.co. uk/2/hi/uk_news/politics/4659228.stm.

3. BBC, „Pet Shop Boys protest at ID cards“. 01.03.2006. Прилог је преузет са адресе: http://news.bbc.co.uk/1/hi/uk_politics/4763874.stm.

4. BBC, „What data will ID cards store?“, 11. јул 2006. Прилог је преузет са адресе: http://news.bbc.co.uk/2/hi/uk_news/politics/4630045.stm.

5. Mikro, „Nesporazumi Evropske unije i SAD oko biometrijskih pasoša“, 06. 04. 2005. Извештај је преузет са адресе: http://www.mikro.co.yu/ser/vesti/vesti.php?datum=2005-04-06&ID=6920.

6. Mikro, „Britanski e-pasoši laki za `provaljivanje`“, 29. 11. 2006. Извештај је преузет са адресе: http://www.mikro.co.yu/ser/vesti/vesti.php?datum=2006-11-29&ID=500224.

7. Yen, Hope „Data on 2.2 Million Active Troops Stolen From VA“, ABC News. Вест је преузета са адресе: http://www.abcnews.go.com/gma/wireStory?id=2047707.

Интервјуи

1. BBC, „ID plan excessive, says watchdog“. Интервју је преузет са адресе: http://news.bbc.co.uk/2/hi/uk_news/politics/4627881.stm.

2. BBC, „Do you support ID cards?“. Анализа је преузета са адресе http://news.bbc.co.uk/1/hi/talking_point/4625971.stm.

3. Clarke, Roger, „Interview with Dr Ted Dunstone, Director, Biometix Consulting“, 16. септембар 2000. Интервју је преузет са адресе: http://www.anu.edu.au/people/Roger.Clarke/dv/BiometixIview.html

4. Jones, George, „ID cards would not have helped, says Clarke“, *Telegraph*,

09. 07. 2005. Интервју је преузет са адресе: http://www.telegraph.co.uk/news/main. jhtml? xml=/news/2005/07/09/npoll209.xml&sSheet=/news/2005/07/09/ixnewstop.html.

5. Kirkup, James, „Identity cards a 'present' to terrorists and criminals, spy heroine says", *The Scotsman– Scotland`a National Newspaper,* 21. 03. 2006, преузето са адресе: http://thescotsman.scotsman.com/uk.cfm?id=441172006.

6. Krsman, Nataša, „Siniša Macan: Pooštrićemo mjere zaštite ličnih podataka", *Nezavisne novine*, 03. 06. 2006. Интервју је преузет са адресе: http://www.nezavisne.com/revija/tekst060604-01.php.

7. Peev, Gerri, „ID cards will lead to 'massive fraud'", *The Scotsman*, 18. 10. 2005. Интервју је преузет са адресе: http://thescotsman.scotsman.com/index.cfm?id=2103982005.

8. „Архиђакон Радош Младеновић о личним картама са биометријским чиповима", (непознат аутор), *Светигора.* Интервју се налази на адреси: http://www.svetigora.com/node/320

9. „Biometric ID cards 'dangerously flawed'", (непознат аутор), *Silicon.com-Law&Policy,* 23.05.2003. Интервју је преузет са адресе: http://management.silicon.com/government/0,39024677,10004326,00.htm.

10. „Interview with Darrin Reilly, Vice President and General Manager Biometrics Business unit, Motorola Inc.", (непознат аутор), *Find Biometrics*, март 2006. Интервју је преузет са адресе: http://www.findbiometrics.com/Pages/feature_motorola_mar06.htm.

11. Латиновић, Зора, „Још увек без заштите", интервју са Чедомиром Шуљгићему оквиру наведеног текста, НИН, 19. 10. 2006.

12. Латиновић, Зора, „Приватност на извол'те", интервју са Владимиром Божовићем, у оквиру antrfilea „Размишљам о грађанској непослушности", НИН 2900.

13. „U. K. Identity Card Will Make Fraud Easier, Expert Says", (непознат аутор), *Bloomberg.com*, 26. 04.2006. Интервју је преузет са адресе: http://quote.bloomberg.com/apps/news?pid=10000102&sid=a7DltmImquye&refer=uk.

Полемике

1. Antonić, Slobodan, „U potrazi za srpskim Toroom", сајт часописа *Нова српска политичка мисао*. Текст је преузет са адресе: http://www.nspm.org.yu/polemike.htm.

2. Brands, Stefan, „The problem with the Belgian eID card", *The Identity Corner*, 7. 4. 2005. Текст је преузет са адресе: http://www.idcorner.org/?p=121.

3. Darijević, Dušan „Žig zveri, paranoja i nešto treće", на адреси http://www.tackacacka.org/ser/vesti/septembar_2006/zigzveri.htm.

4. Daugman, John, „Inquiry on Use of Scientific Evidence in Policy Formation and Assessment“.

5. LSE, „Memorandum from the London School of Economics and Political Science Identity Project Team“.

6. Суботић, Оливер, „Ко је овде луд(иста)?“, http://www.nspm.org.yu/koment2006/2006_subotic_ludizm.htm.

7. Велимировић, Дарко : „Лудизам у Србији“, http://www.nspm.org.yu/koment2006/2006_velim_ludizam.htm.

8. „Are E-Passports More Secure?“, *The Wall Street Journal*, 29. 09. 2006. Расправа између представника State Department-а Мојре Харти (Maura Harty) и правног заступника ACLU-а Берија Стајнхарда (Barry Steinhardt). Текст је преузет са адресе: http://online.wsj.com/public/article/sb115938787873075826-6abupmiajvcs1i_ubvogrwp867k_20070929.html.

Blog-ови

1. Lukić, Milan, „Alo, Crkva... “, blog на адреси http://blog.b92.net/node/1206.

2. Marković, Slobodan, „Elektronske lične karte od kraja januara“, *Internodium*, blog на адреси: http://www.internodium.org/node/2774.

Остало

1. LeaveThemKidsAlone, „10 Things You Should Know About Schools Fingerprinting Children“. Проспект је преузет са адресе: http://www.leavethemkidsalone.com/10things.htm.

2. Australian Privacy Foundation, „The Australia Card Proposal 1985–87“. Чланак је преузет са адресе: http://www.privacy.org.au/Campaigns/ID_cards/Resources.html#OzCard.

3. Australian Privacy Foundation, „The Case Against a National Identification Scheme“. Чланак је преузето са адресе: http://www.privacy.org.au/Campaigns/ID_cards/NatIDScheme.html

4. Australian Privacy Foundation, „The Korean National Education Information Systems (NEIS)“. Чланак је преузет са адресе: http://www.privacy.org.au/Campaigns/KoreaNEIS/.

5. Australian Privacy Foundation, „National ID scheme; Elsewhere in the World“. Чланак је преузет са адресе: http://www.privacy.org.au/Campaigns/ID_cards/Resources.html#NatIDSchemes.

О аутору

Оливер В. Суботић је рођен 1977. године у Новој Вароши (Србија). У родном граду је завршио Природно-математичку гимназију (1996), после које уписује студије на Одсеку за информационе технологије ФОН-а у Београду. Током тих студија је објавио више десетина чланака из области рачунарске анимације и визуелизације и постао активни стручни сарадник Више електротехничке школе на предметима Компјутерска графика и Компјутерска анимација. Упоредо са тим активностима, уписује и Православни богословски факултет у Београду (2000).

На ФОН-у је дипломирао 2004, а на Православном богословском факултету 2005. године.

Из области информационих технологија чланке је објављивао у часописима *Čip*, *Svet kompjutera*, *Računari*, *Digital Arts*, *PC*, *Digital*, а из друштвено-религијских области за часописе *Православље*, *Светиора* и *Нова српска политичка мисао*.

Објавио је две књиге:
3D Studio MAX3 – Tehnike modelinga, (2000), приручник за тродимензионално моделовање и визуелизацију;
Човек и информационе технологије: поглед из православне перспективе, (2006), зборник текстова, студија и есеја који говори о феноменима информационих технологија из аспекта православне теологије и антропологије.

Тренутно је ангажован на Православном богословском факултету као стручни сарадник на информационим делатностима у оквиру Информационо-документационог центра факултета. Ожењен је и живи у Београду.

CIP – Каталогизација у публикацији
Народна библиотека Србије, Београд

СУБОТИЋ, Оливер
Биометријски системи идентификације:
критичка студија/Оливер Суботић –
Београд : Институт за политичке студије,
2007 (Београд : Драслар партнер). – 184
стр. ; 24 cm

Тираж 500 - Биографија аутора : стр. 183.
- Напомене и библиографске референце уз
текст. – Библиографија : стр. 164-181.
ISBN 978-86-7419-120-0

а) Биометријски системи идентификације
COBISS.SR-ID 138440204

ИНСТИТУТ ЗА ПОЛИТИЧКЕ СТУДИЈЕ
ИПС
1968
БЕОГРАД