



REPUBLIKA SLOVENIJA
MINISTRSTVO ZA NOTRANJE ZADEVE

POLICIJA

Generalna policijska uprava
Uprava kriminalistične policije



"Co-funded by the Prevention of and
Fight against Crime Programme of
the European Union"

Presoja vplivov na zasebnost pri obdelavi podatkov o potnikih »PNR«



*Oddelek za ocenjevanje
varnostnih tveganj*

CKOD UKP GPU

Ljubljana, februar 2015

Republika Slovenija

Ministrstvo za notranje zadeve

POLICIJA

Generalna policijska uprava

Uprava kriminalistične policije

Štefanova 2, 1501 Ljubljana

T: +386 1 428 40 00

F: +386 1 428 47 33

gp.policija@policija.si

Dokument:

Presoja vplivov na zasebnost pri obdelavi podatkov o potnikih »PNR«

Šifra: 500-164/2013/65 (2241-01)

Datum: 25. 2. 2015

Avtor:

Robert Berginc, mag. prav., vodja oddelka

Pri pripravi dokumenta sodeloval:

Andrej Mejak, kriminalistični inšpektor specialist

Opomba:

1. Dne 5. 5. 2015 izvedeni popravki osnovnega dokumenta po podanem prvem pisnem mnenju IP RS (št. 0712-1/2015/725, z 12.3.2015) in po izvedenih študijskih obiskih v Franciji in Madžarski,
2. Dne juliju 2015 izvedeni popravki osnovnega dokumenta po podanem drugem pisnem mnenju IP RS (št. 0712-15/2015/2, z 5. 6. 2015) in po izvedenem študijskem obisku API centra v Amsterdamu.

STVARNO KAZALO

1	UVOD	6
2	OCENA UČINKA UPORABE PODATKOV PNR	8
2.1	Ocena stanja za področje hujše kriminalitete	8
2.2	Utemeljitev potrebe po uporabi in hrambi podatkov.....	14
2.3	Primerjalno pravni zakonodajni vidik obdelave podatkov	25
2.3.1	PNR pravna ureditev v Franciji.....	26
2.3.2	PNR pravna ureditev v Madžarski.....	26
2.4	Vsebina in način obdelave ter operativna uporaba podatkov	27
2.4.1	Splošno o uporabi podatkov.....	27
2.4.1.1	Delovanje SI PNR dvotirnega sistema.....	29
2.4.2	Zbiranje podatkov.....	31
2.4.2.1	Vsebina zbranih podatkov	31
2.4.2.2	Neselektivno zbiranje podatkov	33
2.4.3	Proces obdelave in uporabe podatkov	35
2.4.4	Delovni proces pri obdelavi podatkov.....	42
3	ANALIZA TVEGANJ V ZVEZI S POSEGI V USTAVNE PRAVICE.....	44
3.1	SWOT analiza za podatke PNR	44
3.1.1	Priložnosti.....	45
3.1.2	Prednosti.....	45
3.1.3	Nevarnosti.....	45
3.2	Tveganja povezana z obdelavo podatkov PNR in upravljanje z njimi	46
3.2.1	Tveganja glede neustreznosti zakonodaje	46
3.2.2	Tveganja glede zbiranja podatkov.....	48
3.2.3	Tveganja glede zavarovanja podatkov.....	51
3.2.4	Tveganja glede uporabe podatkov	53
3.2.5	Tveganja glede hrambe podatkov	55

4	TEST SORAZMERNOSTI ZARADI KOLIZIJE ČLOVEKOVIH PRAVIC	56
4.1	Ustavno pravni vidik zadevnih človekovih pravic	57
4.1.1	Varnost.....	58
4.1.2	Zasebnost in varstvo podatkov	59
4.2	Ustavna dopustnost cilja.....	60
4.3	Test primernosti in učinkovitosti	60
4.4	Test nujnosti.....	62
4.5	Test sorazmernosti v ožjem smislu	64
5	PREDLOG PRAVNE UREDITVE UPORABE PODATKOV PNR.....	67
6	ZAKLJUČEK	67
7	VIRI IN LITERATURA	69
	Publikacije in prispevki	69
	Pravni viri.....	70
	Judikati.....	70
	Razvojno usmerjevalni dokumenti.....	70

„Zakone potrebujemo predvsem takrat, kadar grmijo topovi [...]. Vsak boj države – zoper terorizem ali kateregakoli drugega sovražnika – se izvaja v skladu s pravili in pravom. Vedno obstaja pravo, ki ga mora država spoštovati. Ni ‚črnih lukenj‘. [...] Razlog za utemeljitev tega pristopa ni le praktična posledica politične in normativne resničnosti. Njegove korenine segajo veliko globlje. Je izraz razlike med demokratično državo, ki se bojuje za svoj obstoj, in bojem teroristov, ki ji nasprotujejo. Država se bojuje v imenu prava in v imenu spoštovanja prava. Teroristi se bojujejo zoper pravo in ga pri tem kršijo. Vojna zoper terorizem je tudi vojna prava proti tistim, ki mu nasprotujejo“.

*(citat Vrhovnega sodišča v Izraelu, HCJ 769/02 [2006],
javni odbor zoper mučenje v Izraelu in drugi proti vladi Izraela
in drugim, točki 61 in 62)*

1 UVOD

Vzpostavitev in širjenje evropskega prostora, s temeljno pravico prostega pretoka blaga in ljudi, ob bonitetah, državljanom EU in nacionalnim gospodarstvom, nehote doprinaša prednosti in na široko odpira vrata tudi terorizmu in drugim oblikam mednarodno organiziranega kriminala. Slednji za razliko od politike, hitro premaguje nacionalne razlike in do popolnosti izkorišča moderno informacijsko in drugo tehnologijo, kar se odraža v mednarodni razvejanosti kriminalnih združb in njihovemu delovanju. Skratka, organiziran kriminal se povezuje in deluje na mednarodni ravni mnogo hitreje, kot to velja za organe odkrivanja oziroma organe kazenskega pregona, ki so pri svojem delu vse bolj omejeni tudi z varovanjem tistih človekovih pravic, ki kolidirajo z istovrstno pravico do varnosti. Tudi to je razlog, da ti organi vse težje dohajajo razsežnosti organiziranega kriminala. V novem času je organiziran kriminal prešel še na področje hitro rastočega evropskega gospodarstva in politike, kar pa je tudi povzročilo trenutno svetovno gospodarsko in ekonomsko krizo. Eden glavnih vzrokov za širitev organiziranega kriminala v vse pore družbenega življenja je prav zmožnost njegovega hitrega prilagajanja vsestranskim družbenim spremembam.

Terorizem je danes ena izmed najpogostejših tem dnevnih poročil, kljub temu, da obstaja že od samega obstoja človeštva. V zadnjem času se najpogostejše oblike terorizma vse bolj pogosto pojavljajo tudi v Evropi, čemer so za teroriste človeške žrtve postranskega pomena. Gre namreč za najhujše oblike povzročanja splošnega strahu in negotovosti s posledicami za življenje in zdravje ljudi ter za njihovo premoženje. Sam boj proti terorizmu je težaven, dolgotrajen, izčrpavajoč in predstavlja velik finančni zalogaj. Kljub velikim finančnim, materialnim in drugim vložkom v boj zoper terorizem, se slednjega ne da povsem izkoreniniti, kar pomeni da ostaja neprestana grožnja nacionalni varnosti in vseskozi ruši ravnovesje med svobodo in varnostjo. Terorizem navsezadnje pomeni tudi napad na človekovi pravici; svobodo in varnost, kot temeljni demokratični družbeni vrednoti, zato je boj proti tej varnostni grožnji postal prioriteta vseh demokratičnih držav.

Vse pogostejše teroristične grožnje in napadi so privedli do tega, da je širša mednarodna skupnost začela razmišljati o odločnejšem, načrtnem in bolj sistematičnem boju zoper tovrstne varnostne grožnje, ki resno in neposredno ogrožajo mednarodno in nacionalno varnost. EU je k temu pristopila resno in načrtno, saj Evropski svet poudarja, da je razvoj območja svobode, varnosti in pravice obravnava kot prednostno vprašanje, ker gre za enega od osrednjih interesov držav članic EU. V Stockholmskem programu¹ so tako določene prednostne naloge EU pri odzivanju na varnostne grožnje in določa temeljna načela pri zatiranju kriminalitete. Ugotavlja namreč, da terorizem in druge hujše oblike mednarodnega kriminala še naprej resno ogrožajo notranjo varnost EU, zaradi česar se od držav članic ter pristojnih organov, agencij in institucij zahteva jasn in celovit odziv. Dokument obvezuje pristojne organe, okrepi svoje aktivnosti skladno s sprejeto strategijo v zatiranju terorizma in drugih hujših oblik mednarodnega kriminala v EU, te pa morajo temeljiti na proaktivnem pristopu na podlagi obveščevalnih podatkov in v tesnem

1 Stockholmski program – Odprta in varna Evropa, ki služi državljanom in jih varuje, predstavlja temeljni razvojno strateški dokument za zagotavljanje mednarodne varnosti na celotnem območju EU, Uradni list C 115, 04/05/2010 str. 0001 – 0038.

medsebojnem sodelovanju pri izmenjavi informacij. Evropski svet v tem dokumentu poziva Komisijo, da za preprečevanje, odkrivanje, preiskovanje in pregon terorističnih in hudih kaznivih dejanj² predstavi predlog za vzpostavitev sistema za uporabo podatkov o letalskih potnikih (PNR – *Passenger Name Record*). Ta pristop je prepoznan, kot eno od učinkovitih orodij za boj proti organizirani kriminaliteti s čezmejnimi posledicami. S tem je prišlo do oblikovanja predloga Direktive Evropskega Parlamenta in Sveta o uporabi podatkov iz evidenc podatkov o potnikih za preprečevanje, odkrivanje, preiskovanje in pregon terorističnih in hudih kaznivih dejanj (*v nadaljevanju: Predlog Direktive PNR*)³, kjer je uporaba podatkov PNR predstavljena tudi kot mehanizem za zagotavljanje notranje varnosti EU in nacionalne ter javne varnosti na območjih držav članic EU.

V ta namen je Evropska Komisija v okviru razvojnega programa ISEC, ki je namenjen za sofinanciranje ukrepov za preprečevanje in boj proti kriminalu za obdobje 2007 - 2013, v letu 2013 izvedla razpis in razdelila evropska finančna sredstva 14-im državam članicam, ki so se prijavile na PNR projekt. Poleg Republike Slovenije (*v nadaljevanju: Slovenije*) v tem evropskem projektu sodelujejo še Bolgarija, Estonija, Španija, Francija, Italija, Latvija, Litva, Madžarska, Nizozemska, Avstrija, Romunija, Finska in Švedska. Te države članice med seboj v projektu že tesno sodelujejo z namenom zagotavljanja kompatibilnosti PNR nacionalnih sistemov ter učinkovite in namenske uporabe podatkov PNR. Pri tem prizadevanju eno večjih ovir predstavlja prav odsotnost enotne zakonodaje v EU pravnem redu, ki bi zagotovila harmonizacijo nacionalnih sistemov in delovanja organov odkrivanja oz. pregona na tem področju.

Slovenska policija je 20. 11. 2013 z Evropsko komisijo podpisala pogodbo o sofinanciranju in izvedbi nacionalnega SI PNR projekta, imenovanega »Establishing conditions for transfer and use of Passenger Name Record data«. V skladu s to pogodbo je Policiji začela izvajati projekt 1. 3. 2014. Namenom je vzpostavitev pogojev za posredovanje in uporabo podatkov PNR o potnikih v mednarodnem letalskem prometu, zaradi preprečevanja, odkrivanja, preiskovanja in pregona terorističnih in drugih hudih kaznivih dejanj, ki so v pristojnosti Europolu. Izvajanje projekta bo trajalo 24 mesecev, do 28. 2. 2016, pod okriljem projektne skupine, katere vodja je g. Slavko Koroš, pomočnik direktorja Uprave kriminalistične policije. Gre za medresorsko projektno skupino za izvedbo projekta SI PNR, v kateri sodelujejo predstavniki Ministrstva za notranje zadeve, Ministrstva za pravosodje in Ministrstva za infrastrukturo in prostor, ter predstavnika nacionalnega letalskega prevoznika Adrie Airways. Pridruženi partner v projektu pa je tudi urad Informacijskega pooblaščenca RS, ki bo s svojo svetovalno in nadzorno vlogo na področju varstva podatkov, tesno sodeloval pri vzpostavitvi in kasnejši uporabi podatkov PNR.

-
- 2 Kazniva dejanja z elementi terorizma in njihove izvršilne oblike so podrobno definirani členih 1 do 4 Okvirnega sklepa Sveta 2002/475/PNZ o boju proti terorizmu.
 - 3 Predlog DIREKTIVA EVROPSKEGA PARLAMENTA IN SVETA o uporabi podatkov iz evidence podatkov o potnikih za preprečevanje, odkrivanje, preiskovanje in pregon terorističnih in hudih kaznivih dejanj (SEC(2011) 132 konč.)(SEC(2011) 133 konč.)

V okviru SI PNR projekta je bila ustanovljena slovenska nacionalna enote za podatke o potnikih, poimenovana Oddelek za ocenjevanje varnostnih tveganj (OOVT), organizirana v Centru za kriminalistično obveščevalno dejavnost, Uprave kriminalistične policije na Generalni policijski upravi (*v nadaljevanju: SI enota za informacije o potnikih, ali OOVT*). Ta notranja organizacijska enota bo po zaključku projekta pristojna za zbiranje informacij o potnikih letalskih prevoznikov, za njihovo hrambo, obdelavo in izmenjavo istih podatkov z drugimi upravičenimi OE in NOE PU/GPU. Vse v okviru policijskega sodelovanja pa tudi z drugimi upravičenci; državnimi organi ter tujimi policijskimi, carinskimi in sorodnimi specializiranimi službami kazenskega pregona, ki bodo zakonsko vključeni kot upravičenci.

Predlog direktive PNR v EU parlamentu za sedaj še ni dobil zadostne politične podpore, zato smo se v PNR projektni skupini odločili pripraviti ustrezne predloge za spremembo oziroma dopolnitev nacionalne zakonodaje. Ta bi policiji omogočala zakonito pridobivanje, obdelavo in izmenjavo podatkov PNR. Vse z izključnim namenom preprečevanja, odkrivanja, preiskovanja in pregona terorističnih in drugih hujših oblik kaznivih dejanj. Skladno s Smernicami Informacijske pooblaščenke⁴ (*v nadaljevanju Smernice IP RS*) v pripravi dokumenta sledimo metodologiji PIA⁵, v cilju odklonov vseh potencialno nezakonitih ravnanj ali prekomernih posegov v pravico do zasebnosti posameznika. V uvidu imamo, da morajo biti tovrstne spremembe zakonodaje policiji v pomoč pri legitimnemu in zakonitemu obdelovanju in uporabi podatkov PNR, s pričakovanim učinkom boljše učinkovitosti in uspešnosti pri preprečevanju, preiskovanju in pregonu hujših oblik kaznivih dejanj. Zato bo ta dokument služil utemeljitvi upravičenega širjenja policijskih pooblastil na področju obdelave osebnih podatkov. Z njim bomo skušali upravičiti nujnost, primernost in sorazmernost predlaganega orodja. Ob tem smo vnaprej predvideli tudi tveganja, z vgradnjo potrebnih varovalk za varstvo pred nesorazmernimi posegi v človekove pravice.

Ustrezna obdelava in uporaba podatkov PNR po izkušnjah predstavlja učinkovit pristop v boju in preprečevanju hujših oblik kriminala. Zavedamo se, da širitev določeno usmerjenega oziroma razširjenega nabora policijskih pooblastil, lahko na eni strani predstavlja poseg v temeljne ustavno varovane človekove pravice in svoboščine (*v nadaljevanju TČPS*), vendar le kot sorazmeren poseg pri preprečevanju terorističnih kaznivih dejanj in drugega organiziranega kriminala. Isto sledi tudi iz utemeljitve Predloga Direktive PNR in z njo povezanimi dokumenti, na katerih temelji.

2 OCENA UČINKA UPORABE PODATKOV PNR

2.1 Ocena stanja za področje hujše kriminalitete

Slovenija v svetovnem in evropskem merilu predstavlja razmeroma majhno gospodarsko tržišče, njen geografski položaj v osrčju Evrope in na presečišču glavnih transportnih koridorjev pa jo uvršča med pomembne tranzitne države. Prav ta položaj povzroča pojave različnih vrst organiziranega kriminala. Čez slovensko ozemlje potekajo pomembne tihotapske poti od juga na sever in od vzhoda na zahod. Ključni odklon za tvegano varnostno situacijo Slovenije

4 Presoja vplivov na zasebnost pri uvajanju novih policijskih pooblastil, Smernice Informacijske pooblaščenke, verzija 1.0, z dne 14. 1. 2014

5 »Presoja vplivov na zasebnost je orodje za identifikacijo, analizo in zmanjševanje tveganj glede nezakonitih ravnanj z osebnimi podatki oziroma prekomernih posegov v pravico do zasebnosti, do katerih lahko pride pri določenem projektu, sistemu ali uporabi tehnologije«, iz Smernic, str. 10.

predstavljajo kriminalne dejavnosti organiziranih kriminalnih združb z razvejanimi omrežji iz zahodnega Balkana. Ta prepredajo območja celotne nekdanje skupne države, vključno z velikimi izseljenskimi središči zahodne Evrope. Jugovzhodna Evropa in zahodni Balkan sta tradicionalni tranzitni območji ilegalnih tokov blaga in ljudi iz območja Bližnjega in Daljnega vzhoda ter severovzhodne Afrike. Ti tokovi se zgrinjajo proti severni in zahodni Evropi. Prav zato so se zahodno-balkanske kriminalne združbe uveljavile kot posredniki med organiziranimi kriminalnimi združbami s ciljem delovanja v bližini izvornih, ali blizu ciljnih držav. Sinonim te komunikacije je t.i. Balkanska pot.

V zadnjih letih se opaža vse večja raznolikost in razvejanost tihotapskih tokov. Ti vse bolj mobilni in razvejani vstopajo in izstopajo iz regije ter prehajajo med različnimi kraki balkanske poti. Tihotapljenje prepovedane droge, ilegalnih migrantov, žrtev trgovine z ljudmi in drugih oblik nezakonitega blaga poteka v vseh dandanes že utečenih in izgrajenih tihotapskih kanalih. Ti tokovi so vpeti v logistična središča organiziranih kriminalnih združb z njihovimi vodilnimi člani na zahodnem Balkanu. Posledično v Sloveniji vse pogosteje zaznavamo dobro organizirane in tesno povezane mednarodno delujoče kriminalne združbe. Najpogosteje je prisoten le del članstva, katerega naloga je skrb za nemoten potek ilegalnih transportov preko ozemlja Slovenije. Omenjeni posamezniki nudijo organizacijske in logistične kapacitete z dobrim poznavanjem mentalitete tranzitnih območij in ilegalnih poti do ciljnih držav. Z utrjevanjem položaja mednarodno usmerjenih organiziranih kriminalnih združb iz območja Zahodnega Balkana se povečuje tudi kriminalna izpostavljenost pristanišč v Kopru, kot tudi v neposredni bližini na Reki (R. *Hrvaška*) in Trstu (R. *Italija*). V okviru kontejnerskega in drugega ladijskega prometa z različnimi tehnikami razvijajo vstopne točke za transport prepovedanih drog in drugega ilegalnega blaga iz globalnih izvornih središč (*Južna Amerika, Afrika, Azija*). Poleg navedenih logističnih centrov, so za kriminalne tokove zanimiva tudi bližja letališča. Z načrtovano širitvijo brniškega letališča »dr. Jožeta Pučnika«, se bo vsekakor povečala tudi njegova vloga pri povezovanju mednarodnih kriminalnih združb oziroma kot nov tihotapski kanal, kar se je v letošnjem letu že potrdilo z dvojnim zasegom prepovedane droge.

Zaradi tranzitne vloge Slovenije se tu vse pogosteje naseljujejo tudi sami vodje tujih kriminalnih združb, ki neposredno vodijo svoje mednarodne kriminalne posle. Pri tem se še vedno povezujejo z domačimi kriminalci in tako razvijajo ter gradijo kriminalna omrežja tudi na območju Slovenije.

Vstop v Schengensko območje je ob klasičnih kriminalnih združbah na območje Slovenije omogočil potovanja tudi številnim mobilnim kriminalnim združbam drugih držav. Te s specialnimi oblikami izvrševanja kaznivih dejanj, izkoriščajo mobilnost, zlasti na hitrih transportnih povezavah. Isti ob sočasnem izvrševanju kriminalnih ravnanj v Sloveniji, ista izvršujejo po širšem območju EU. Spretno izkoriščajo svoboščino, zagotovljeno pri prostem pretoku blaga, storitev, kapitala in oseb. Zato se slovenska policija dandanes sooča z vse širšimi oblikami kriminala in tako različnimi viri ogrožanja notranje nacionalne varnosti. Ti vse bolj globlje posegajo v TCPS državljanov. Aktualni viri ogrožanja javne varnosti se odražajo v oblikah povečanih obsegov napadov na življenje in premoženje ljudi, gospodarske kriminalitete, korupcije, kibernetске in okoljske kriminalitete, nezakonitih migracij, v pojavih množičnih kršitev javnega reda in miru ter nenazadnje tudi v najhujših oblikah varnostnih groženj, kakor je

terorizem. Te kritične spremembe od policije terjajo agilno in čimbolj fleksibilno organizacijsko, zlasti pa funkcionalno prilagoditev.

Zagotovitev visoke stopnje varnosti je v temeljnem razvojno-usmerjevalnim dokumentu na področju nacionalne varnosti⁶ (*v nadaljevanju: Resolucija*) zahtevana kot eden izmed temeljnih nacionalno varnostnih ciljev slovenske države. Sloni lahko le na boljši organiziranosti, usposobljenosti in pripravljenosti Policije ter drugih varnostnih subjektov, pristojnih za zagotavljanje varnosti. Isti dokument prepoznava terorizem in organizirano kriminaliteto, kot ene od bistvenih izvorov ogrožanja in tveganj za nacionalno varnost. Zato predstavlja kompleksno in dolgoročno grožnjo varnosti Republike Slovenije.

Da organizirana kriminaliteta preko zahodnega Balkana vse bolj posega tudi na območje Slovenije in kot takšna predstavlja vse večjo grožnjo, ugotavlja tudi agencija EUROPOL v svojih analitičnih poročilih. V svojih ocenah ogroženosti⁷ pripisuje izjemen pomen prav »Balkanski osi«, kot teritorialno najpomembnejšemu segmentu, ki odločilno vpliva na razvoj in širjenje organizirane kriminalitete v vse države EU. Poroča, da je večina groženj iz področja organiziranega kriminala mednarodno razsežna, saj so mednarodna potovanja storilcev in z njimi povezanega prepovedanega blaga postali sestavni del našega vsakdana.

Graf 1: Trend organizirane kriminalitete na območju RS



Enako kot agencija EUROPOL porast organiziranega kriminala ugotavlja tudi slovenska policija (*glej graf 1*). Statistični kazalniki izkazujejo naraščanje obravnavanih kaznivih dejanj prav iz področja organizirane kriminalitete in posledično organiziranih združb. Kriminalistična policija je zato vse bolj obremenjena, saj je situaciji nasproti, prisiljena izvajati vse bolj zapletene in kompleksne preiskave kaznivih dejanj, razširjene na mednarodni prostor.

Glede na obstoječe trende slovenska policija v svoji Oceni ogroženosti Republike Slovenije zaradi hudih in organiziranih oblik kriminalitete, iz leta 2013, prognozira nezmanjšan trend tesnih povezav organizirane kriminalitete na zahodno-balkansko. Isto pomeni tudi veliko tveganje zaradi nezmanjšanih kriminalnih aktivnosti Trgovina s prepovedanimi drogami, z njimi povezano

6 Resolucija o strategiji nacionalne varnosti Republike Slovenije, Ur. l. RS št. 27/2010 z 2. 4. 2010.

7 OCTA 2011-2013, SOCTA 2014-2017 – Serious Organized Crime Threat Assessment.

tihotapljenje, ilegalne migracije, organizirane oblike premoženjske kriminalitete, tranzitni tokovi prepovedanega blaga in ljudi, mobilne kriminalne združbe in nanje vezane pojavne oblike sekundarne kriminalitete bodo srednjeročno še naprej poglavitni modusi hude in organizirane kriminalitete v Sloveniji.

Resolucija o nacionalnem programu preprečevanja in zatiranja kriminalitete za obdobje 2012–2016⁸ (*v nadaljevanju: Resolucija 2012-2016*), ob organizirani kriminaliteti, nezakonitih migracijah in kibernetnem kriminalu, kot bistveno varnostno grožnjo, prepoznava terorizem z vsemi njegovimi pripadajočimi oblikami ekstremnega nasilja. Resolucija ugotavlja krepitev terorizma, z nekaterimi oblikami ekstremizma na območju EU. Isto potrjuje tudi Situacijsko poročilo agencije Europol o teroristični dejavnosti v EU⁹. V dokumentu za preteklo leto 2013 sicer poroča o upadu terorističnih napadov, vendar pa v okviru teh beležijo porast števila aretiranih posameznikov¹⁰. Še posebej sta zaskrbljujoča regionalno zaznamovana hitrorastoča nasilna radikalizacija in rekrutiranje islamskih skrajnežev. Ta pojava sta tudi eno od petih prioritetenih področij omejevanja terorizma v EU. Značilnost novodobnega terorizma je tudi njegova transnacionalnost, zato tudi Slovenija, v teroristični ogroženosti ni izvzeta. Teroristi, ekstremisti in osebe, odgovorne za krepitev oziroma razvoj procesa nasilne radikalizacije, tranzitirajo preko Slovenije vse pogosteje. Kot že povedano se nahajamo na enem izmed zračnih oziroma kopenskih transportnih koridorjev, ki povezuje severni in zahodni evropski prostor z državami jugovzhodnega Balkana. Tudi preko Slovenije postaja Bližnji vzhod, vse bolj ciljno območje za posameznike ali manjše skupine, ki tja odhajajo na bojišča in delujejo v korist terorističnih organizacij, kot je npr. »Islamska država«. Te poti so podrobno predstavljene v zgoraj navedenem Europolovem situacijskem poročilu, ter v Interpolovem analitičnem poročilu o potovanjih tujih borcev v Sirijo¹¹.

Resolucija 2012-2016 nadalje ugotavlja, da je Slovenija po dogodkih 11. 9. 2001 sicer vzpostavila temelje sistematičnega obravnavanja groženj mednarodnega terorizma, vendar pa se zmogljivosti slovenske policije zaradi navidezne odsotnosti grožnje terorizma še niso krepile. V zaključku Resolucija 2012-2016 podaja smernice, o nujnosti posodobitve policijskih pooblastil ter nujne ustrezne organizacije z izrabo obstoječih resursov. Ti bi ob neposredni teroristični nevarnosti morali omogočati učinkovitejše delo varnostnih in pravosodnih organov.

Medresorska delovna skupina za boj proti terorizmu je maja 2014 izdelala Oceno ogroženosti Republike Slovenije z vidika mednarodnega terorizma in podala NIZKO stopnja ogroženosti. Vendar ocena ne more prognozirati številnih nepredvidljivih družbenih dejavnikov, zato se lahko ta stopnja zelo hitro spremeni. Najpomembnejši dejavniki, ki jih velja omeniti so odhodi radikaliziranih posameznikov na »džihad« v Sirijo in njihove povezane aktivnosti v tej regiji ter tveganja vezana na njihovo vrnitev domov. Zaskrbljujoči so tudi indici širjenja terorja z lani

8 Resolucija o nacionalnem programu preprečevanja in zatiranja kriminalitete za obdobje 2012–2016 (ReNPPZK12-16), Uradni list RS, št. 83/2012 z dne 6. 11. 2012.

9 TE-SAT 2014, European Police Office, 2014.

10 Za primerjavo je bilo v letu 2012 na območju EU zabeleženih 219 terorističnih dogodkov (uspehi, neuspehi in preprečeni teroristični napadi) in v teh aretiranih 537 oseb, v letu 2013 pa »zgolj« 152 terorističnih dogodkov, v teh pa aretiranih 535 ljudi. Vir; EUROPOL-vo poročilo; EUROPEAN UNION TERRORISM SITUATION AND TREND REPORT 2014 (str. 12)

11 Travel routes into Syria used by Foreign Terrorist Fighters, Interpol, november 2014.

odkritimi in zaseženimi primerki orožja v Sloveniji pa tudi poročila partnerskih služb o zaznanih udeležbah posameznih slovenskih državljanov na sirskih bojiščih. Nenazadnje tudi nekatere relevantne informacije in članki medijev, poročajo o zaznanih razsežnostih terorizma v Sloveniji. Odmevne akcije v naši bližini¹² in nekatere navedbe v medijih, nakazujejo na prisotnost ene izmed najekstremnejših skupin vehabitov¹³ v Sloveniji.

Stanje posredne ogroženosti Slovenije (*zlorabe ozemlja za pripravljala dejanja ali kot tranzitnega območja*), ali celo neposredne, ko lahko postane celo tarča terorističnega napada, je trenutno zaradi spreminjanja trendov in nepredvidljivih okoliščin, težko definirati. Dejstvo je, da lahko ogroženost Slovenije s strani teroristov postane tudi neposredna, v primeru vrnitve mentalno nepredvidljivih »slovenskih« skrajnežev iz sirskih bojišč. V vsakem primeru je zaradi resnosti problematike potrebno stanje redno spremljati, vse podatke analizirati in vrednotiti, aktivnosti pa izvajati z vso resnostjo. Teroristične organizacije v zadnjem desetletju še posebej aktivno demonstrirajo svojo nepredvidljivost in okrutnost tudi v evropskem prostoru, saj vedno znova presenetijo organe odkrivanja oziroma kazenskega pregona z novimi premetenimi načini napadov na življenja nedolžnih ljudi. To je prav gotovo hujši poseg v človekove pravice ljudi od tega, ki bi ga na striktno nadzorovan način izvajala policija z obdelavo/uporabo podatkov PNR. Zakaj se ne bi učili iz grenkih izkušenj v tujini in z usmerjenim proaktivnim delom policije teroristom povečali tveganje za njihove napade oziroma jim takšna dejanja preprečili? V slovenski policiji se v luči našega poslanstva še kako zavedamo pomembnosti proaktivnega pristopa pri preprečevanju kaznivih ravnanj. Tak pristop bi policiji omogočala tudi proaktivna in sprotna uporaba podatkov PNR. Potrebno je poudariti, da pri uporabi teh podatkov ne gre za zbiranje osebnih in drugih podatkov na zalogo, kot pri hrambi podatkov o prometu elektronskih komunikacij, temveč gre za njihovo sprotno uporabo s preverjanjem skozi zelo pomembna in nediskriminatorna ocenjevalna merila (specifični potovalni vzorci večine storilcev) ter skozi nacionalne in mednarodne podatkovne baze, ki se uporabljajo na področju zatiranja kriminalitete.

Po ocenah Interpola iz ozemlja EU na bojišča v Sirijo letno odpotuje cca 3000 borcev - ekstremistov. Zaskrbljujoč pa je podatek, da je navkljub zaznanemu številu odkritih zgolj 700 takšnih oseb, zoper katere so organi pregona uspeli uvesti sodne postopke zaradi suma izvrševanja terorizma. Ocenjuje se, da je tako velik odklon prav zaradi pomanjkanja ustreznih orodij, kot npr. možnost sledenja elektronskim sledem storilcev. Ocena se nadaljuje z ugotovitvami, da bi k znatno boljšemu deležu odkritja in preiskanosti tovrstnih kaznivih dejanj, prispevali prav podatki o letalskih potnikih (PNR in API).

Izjemen porast terorističnih migracij ilustrira tudi nedavno poročilo direktorja ameriškega nacionalnega centra za boj proti terorizmu (National Counterterrorism Center – NCTC), Nicholasa Rasmussena. Njegovo izjavo povzemajo vsi vodilni mediji¹⁴, ki poročajo o nedavni pridružitvi 20.000 prostovoljcev borcem Islamske države v Siriji in Iraku. Od zadnje ocene v letošnjem januarju naj bi se po poročilu NCTC število tovrstnih »potnikov« povečalo za vsaj tisoč borcev in ti prihajajo iz več kot 90 držav. Od teh naj bi jih vsaj 3400 prihajalo prav iz zahodnih

12 Akcija Damask v BiH 3.9.2014, Palmera Avstrija 28.11.2014.

13 Jutarnji list, 2.9.2014.

14 Spletni časopis CNN, v članku UAE resumes anti-ISIS strikes, z dne 11.2.2015
<http://edition.cnn.com/2015/02/10/world/isis-syria-iraq/index.html>.

držav, med tem ko naj bi bilo Američanov kakšnih 150. Podatek predstavlja izjemen razlog za skrb, saj se večina teh (*preživelih*) potnikov po vojskovanju tudi vrača v lastna domovanja in tam lahko predstavljajo veliko nevarnost za svojo okolico.

Slovenija se za sedaj še ne pojavlja na statističnih lestvicah, oziroma grafih, ker ne sodi v ciljne države, vendar pa kot že rečeno geografsko sodimo v tranzitno območje. Zaradi že naštetih dejavnikov je se lahko takšna varnostna situacija v trenutku spremeni in iz nizka stopnje, preide v visoko neposredno. Zlasti nepredvidljivi so lahko primeri vrnitve mentalno nestabilnih »slovenskih« skrajnežev¹⁵ iz sirskih bojišč. Takšni zaradi različnih vojnih travm nemalokrat obolijo za t.i. vietnamskim, oziroma legionarskim sindromom. Zato je nujno redno spremljanje stanja, s potrebnim analiziranjem in vrednotenjem, potrebne aktivnosti pa promptno izvajati z najvišjo stopnjo varnosti. Izdaten in uporaben podatkovni vir za načrtovanja in organiziranje teh aktivnostih predstavljajo prav podatki PNR. Tuje izkušnje uporabe teh, so bile že predstavljene za učinkovito orodje pri izdelavi in izmenjavi obveščevalnih informacij v cilju preprečevanja terorizma in drugih hujših oblik kaznivih dejanj. Neidentificirani kriminalci pogosto potujejo skozi mednarodni prostor prav z letalskimi prevozniki, saj so takšna potovanja hitra in vse bolj cenena. Določeni ponavljajoči vzorci pa kriminalce zaznamujejo, kar je lahko skozi temeljite analize prepoznano. Isti pojavi lahko predstavljajo ustrezne temelje za izgradnjo ustreznih meril tveganja, katera pa nakazujejo na varnostno zanimive odklone.

Teroristične grožnje in napadi so vse pogostejša osrednja tema razprav širše mednarodne in evropske skupnosti. Zlasti aktivno po nedavnih terorističnih napadih v Franciji¹⁶ in Danskem¹⁷. Po zadnjem francoskem pokolu je francoski premier Manuel Valls predstavil vrsto protiterorističnih ukrepov. Med temi tudi vzpostavitev skupne baze podatkov letalskih potnikov (PNR), za kar so v lanskem letu tudi že sprejeli nacionalno pravno podlago. Terorizem in druga huda kazniva dejanja navsezadnje povzročajo nepopravljivo škodo. Nesmiselne, nedolžne smrtne žrtve in ogromna gospodarska škoda sejejo strah med prebivalci. Zmanjšan ali neučinkovit občutek varnosti, je razlog ki posamezniku onemogoča učinkovito udejanjanje njegovih TČPS. Zato ti varnostni odkloni predstavljajo brezkompromisne grobe napade na osnovni človekovi pravici; svobodo in varnost. Slednji sta skozi družbeno pogodbo temeljni vrednoti vsake demokratične države. Zato boj proti tej varnostni grožnji postaja prioriteta vseh demokratičnih držav in skupnosti. Varnost enotnega prostora EU, kot tudi širše, zahteva sistem trdnega členjenja vseh varnostnih subjektov. Zato je izjemnega pomena, da vsaka od držav članic, kot tudi skupnosti dosledno odigrajo svojo vlogo. Zlasti v smislu osveščanja širše javnosti, strokovno

15 Neredki so primeri vračanja slovenskih borcev iz Sirskega bojišča, nekaj takih je bilo celo javno izpostavljenih občilih javnega obveščanja; <http://www.mladina.si/161035/boril-sem-se-za-islam/>, <http://www.rtvsllo.si/svet/rok-zavbi-zanika-povezave-s-skrajnezi-in-islamsko-drzavo/347543>, <http://svet24.si/clanek/novice/slovenija/54251b489eaae/kdo-so-slovenski-teroristi-islamske-drzave>, <http://www.slovenskenovice.si/novice/slovenija/razkritih-se-pet-slovencev-ki-jih-zaradi-terorizma-nadzira-sova>.

16 <http://www.dnevnik.si/svet/francija-napovedala-nove-protiteroristicne-ukrepe>, objavljeno v Dnevniku, 21.1.2015.

17 Spletni portal RTVSLO, spletni članek, Napad na Danskem: 22-letni osumljenec znan po nasilnih dejanjih <http://www.rtvsllo.si/svet/napad-na-danskem-22-letni-osumljenec-znan-po-nasilnih-dejanjih/358384> 16.2.2015.

pa v sistematičnem odkrivanju in preprečevanju vsake vrste terorja, ki grobo posega v TČPS poštenih ljudi.

2.2 Utemeljitev potrebe po uporabi in hrambi podatkov

Potrebno je poudariti, da v primeru uvajanja obdelave in uporabe podatkov o potnikih (PNR) ne gre za popolnoma novo, temveč za razširitev policijskega pooblastila za obdelavo sorodnih podatkov, ki se trenutno izvaja skladno z določbami Zakona o letalstvu (Uradni list RS, št. 81/10, z dne 15. 10. 2010), ki predstavljajo implementacijo Direktive Sveta 2004/82/ES z dne 29. aprila 2004 o dolžnosti prevoznikov, da posredujejo predhodne podatke o potnikih, t.i. Advance Passenger Information, (v nadaljevanju podatki API). Določba, v smislu boja proti nezakonitemu priseljevanju (kar kompleksno sodi tudi na področje odkrivanja in preprečevanja kriminalitete) v 3. členu, narekuje letalskim prevoznikom dolžnost, da »na zahtevo organov, odgovornih za izvajanje kontrole oseb na zunanjih mejah, do konca prijave potnikov posredujejo informacije o potnikih, ki jih bodo prepeljali na določen mejni prehod, preko katerega bodo te osebe vstopile na ozemlje države članice«.

Direktiva Sveta 2004/82/ES države članice zavezuje tudi k sprejetju potrebnih ukrepov in sankcij zoper prevoznike, ki takih informacij pristojnim organom za izvajanje mejnih kontrol ne bi ali bi jih napačno posredovali. Čas za popolno implementacijo določb te direktive v nacionalno zakonodajo je minil 5. septembra 2006. Slovenija je z vsebinskim vnosom direktive v nacionalno zakonodajo, izpolnila svojo dolžnost, vendar pa prevozniki do danes svojih dolžnosti še ne izpolnjujejo v celoti, saj pošiljajo nepopolne podatke API, ki so v nedoslednih formatih neprimerni za operativno rabo.

Podatki API so razvidni iz strojno berljive vrstice potovalnega dokumenta potnika, ki jih letalski prevozniki shranjujejo v sistemu vzletne kontrole (DCS - Departure Control System). Mednarodne organizacije (WCO, IATA, ICAO) so z namenom učinkovitega posredovanja teh podatkov organom, ki izvajajo mejno kontrolo, pripravile smernice¹⁸. V le-teh je naveden tudi razširjen nabor teh podatkov¹⁹, ki jih letalski prevozniki enotno zbirajo:

Podatki o letu:

- podatki o letu (IATA Airline code and flight number),
- načrtovan datum in ura vzleta in pristanka,
- **kraj vzleta in pristanka letala,**
- število vseh potnikov,

Podatki o potniku:

- številka potovalnega dokumenta (potni list ali drug potovalni dokument),

18 Guidelines on Advance Passenger Information (API), WCO/IATA/ICAO, leto 2010, (<http://www.icao.int/Security/FAL/Documents/2010%20API%20Guidelines%20Final%20Version.ICAO.2011%20full%20x2.pdf>)

19 Opomba: krepko poudarjeni podatki predstavljajo segment dodatnih podatkov API, ki niso navedeni v trenutni pravni podlagi v 84.a členu Zlet-UPB4. Ostali podatki so isti, kot jih že določa ta nacionalna pravna podlaga.

- **nacionalnost potovalnega dokumenta** (država ali organizacija, odgovorna za izdajo potovalnega dokumenta),
- vrsta potovalnega dokumenta (identifikator za opredelitev vrste potovalnega dokumenta),
- **datum poteka potovalnega dokumenta** (datum poteka veljavnosti potovalnega dokumenta),
- priimek / ime (priimek in ime(-na) imetnika, kot je prikazan na potovalnem dokumentu),
- datum rojstva,
- **spol,**
- državljanstvo,
- **status osebe** (potnik, član posadke, v tranzitu),
- kraj vkrcanja (kraj kjer je popotnik začel potovanje),
- mejni prehod vstopa potnika na območje Schengena,
- **kraj v tranzitu,**
- **PNR lokator,**
- **podatki o sedežu potnika,**
- **podatki o prtljagi (število kosov in teža povezana z vsakim).**

Nabor podatkov API iz smernic je dejansko širši, kot ga predvideva zgoraj navedena direktiva, vendar dodatni podatki vezani na osebo pomenijo zgolj konkretizacijo nekaterih zakonsko že določenih podatkov, ki se nanašajo na potovalni dokument in spol. Dodana sta dva nova podatka o potnikovem sedežu in njegovi prtljagi. Ostali dodani podatki se nanašajo na posamezen let. Glede na to, da podatki API predstavljajo preverjene podatke o potniku in letu, so zato tudi relevantni za uporabo. Za učinkovito analitično obdelavo prav gotovo predstavljajo dodano vrednost podatkom PNR iz sistema rezervacij letalskih kart, ki sami po sebi še ne omogočajo popolno identifikacijo posameznega potnika. To dodano vrednost dokazujejo že potovalne agencije, preko katerih lahko letalski potniki rezervirajo letalske vozovnice. Z obdelavo osebnih podatkov, ki jim jih pošljejo potniki ob rezervaciji vozovnice, namreč že ocenjujejo potnike za njihove komercialne namene. Zavedamo se, da gre v teh primerih za obdelavo osebnih podatkov po privolitvi posameznikov, vendar gre kljub temu v osnovi za poseg v TČPS. Ta poseg v zasebnost se strokovni in laični javnosti ne zdi sporen, kljub temu, da se izvaja v zasebno korist gospodarske družbe. Na drugi strani pa je ta poseg v zasebnost sporen, če bi ga izvajala policija v javno korist, to je za zagotavljanje splošne varnosti, varnosti ljudi in njihovega življenja.

Povezani podatki API in PNR bi z neposredno in popolno identifikacijo potnika pred njegovim prihodom na letališče ali pred odhodom z letališča, zmanjšali tveganje za preverjanje in kontrolo napačnih ljudi z enakimi ali podobnimi imeni. SI enoti za informacije o potnikih bi tako povezani podatki omogočali izvedbo ustrezne ocene tveganja, na podlagi katere bi se policisti, ki opravljajo mejno kontrolo že predhodno pripravili na podrobno preverjanje samo tistih oseb, ki predstavljajo veliko tveganje za javno in mednarodno varnost. Na ta način bi se prav gotovo skrajšal tudi čas mejne kontrole vseh potnikov.

Kot že omenjeno, se tudi Slovenija v družbi z evropskimi državami že dlje časa sooča z naraščajočo tendenco organiziranega kriminala. Temu primerno se je EU že odzvala v Stockholmskem programu, kjer izpostavlja proaktivni pristop na obveščevalno vodeni policijski dejavnosti. Na tem bo morala temeljiti bodoča notranja varnostna strategija, varovanja svobode, pravic in varnosti državljanov. Program izpostavlja krepitev zmožnosti držav in njenih institucij v boju preprečevanja in zatiranja kriminalitete. Strateško so izpostavljena področja kriminalitete, ki najbolj ogrožajo varnost državljanov EU. Ta so v programu prepoznana in opredeljena kot vse oblike organizirane kriminalitete, terorizma, trgovina s prepovedanimi drogami, korupcija, trgovina z ljudmi, prekupečevanje z orožjem in kibernetika kriminaliteta.

Po poročanju organov pregona drugih držav po svetu, kjer so si s sistemom obdelave in uporabe podatkov PNR, že pridobili bogate operativne izkušnje, velja ta sistem za učinkovit mehanizem pri zagotavljanju varnosti. Tako na mikro nivoju pri zagotavljanju javne varnosti, varnosti ljudi in premoženja, kot tudi na sistemskem nivoju, kot učinkovito orodje za usmerjanje dela policije na storilce kaznivih dejanj in primerni za izdelavo še uporabnejših kriminalistično obveščevalnih izdelkov za namen preprečevanja terorizma in drugih hujših kaznivih dejanj.

Iz tujih izkušenj, kjer podatke PNR že uporabljajo izhaja, da so analize teh podatkov na primer pokazale najpogostejše ali vzorčne poti trgovanja z ljudmi ali s prepovedanimi drogami; isti ponavljajoči vzorec je nato služil za izdelavo ocenjevalnega merila. S preverjanjem podatkov PNR je glede na takšna merila mogoče kazniva dejanja preprečiti ali odkriti. Poznan je primer države članice glede trgovine z ljudmi, kjer je analiza podatkov PNR razkrila skupino trgovcev z ljudmi, ki vedno potujejo po isti poti. Za prijavo na notranji let so storilci uporabljali ponarejene dokumente, svoje prave pa za prijavo na drug let, namenjen iz/v tretjo državo. Brez podatkov PNR te mreže trgovine z ljudmi ne bi bilo mogoče razkriti.

Drug takšen primer države članice je povezan s trgovino z ljudmi in s tihotapljenjem prepovedane droge v večjem obsegu, ki je potekala preko držav članic in v tretjih državah. Kriminalne združbe so tihotapile prepovedano drogo na več destinacij v Evropi. Pri tem so uporabljali »požiralce« prepovedanih drog, ki so bili hkrati tudi žrtve trgovine z ljudmi. Organi kazenskega pregona so njihovo istovetnost uspeli ugotoviti na podlagi podatkov PNR v povezavah z nakupom vozovnic z ukradenimi kreditnimi karticami. Isto odkritje je vodilo do prijett vseh storilcev v državi članici. Na tej podlagi je bilo nato oblikovano ocenjevalno merilo, posledica katerega so bile kasneje izvedene številne dodatne aretacije še v drugih državah članicah in v tretjih državah. Na tak način so dokazali tudi povezave med storilci navedenih kaznivih dejanj in njihovo povezovanje v kriminalno združbo.

Navedene izkušnje držav članic kažejo, da se je uporaba podatkov PNR že izkazala kot ključno analitično orodje za boj proti kriminaliteti, povezano s prepovedanimi drogami in trgovino z ljudmi. Njihove analitične obdelave so pripomogle tudi k boljšemu razumevanju povezovalnih značilnosti in delovanja kriminalnih mrež. Države članice so kot pozitivne izkušnje na področju odkrivanja prepovedanih drog poročale, da večino zasegov opravijo prav s pomočjo analitične obdelave podatkov PNR v realnem času in v okviru njihove proaktivne uporabe. Belgija²⁰ je tako

20 12. točka Mnenja Evropskega nadzornika za varstvo podatkov o predlogu direktive Evropskega

poročala, da je 95 % vseh zasegov prepovedanih drog v letu 2009 temeljilo izključno ali odločujoče na obdelavi podatkov PNR. Švedska je poročala, da je 65–75 % vseh zasegov drog v letu 2009 temeljilo izključno ali odločujoče na obdelavi podatkov PNR. To je pomenilo 278,9 kg kokaina, poleg tega pa še določene količine heroina in drugih prepovedanih drog. Združeno kraljestvo je poročalo, da je v obdobju šest mesecev leta 2010 zaseglo 212 kg kokaina in 20 kg heroina izključno ali v odločujoči meri na podlagi obdelave podatkov PNR²¹. Tudi Slovenija v podobnih prepovedanih ravnanjih ne sodi v nobeno izjemo, kar dokazujejo podobni zasegi prepovedanih drog. V letu 2012 so policisti Postaje letališke policije Brnik (*v nadaljevanju PLP Brnik*) tanzanijskemu državljanu, ki je potoval iz Nairobija, preko Zuricha do Ljubljane, zasegli skoraj 5 kilogramov heroina. Druga dva odmevnejša primera pa sta bila odkrita letos, 10. in 15. 1. 2015, ko sta sicer povezana somalijska državljana, vsak zase iz tretje države, preko notranjega leta pripotovala na letališče »dr. Jožeta Pučnika«, kjer so policisti in cariniki pri enem izmed njiju odkrili in zasegli okoli 20kg, pri drugemu pa nekaj čez 55 kg prepovedane droge »khat«, ki sta jo prenašala v svojih potovalnih kovčkih.

Nasproti vse večji mednarodni razsežnosti organiziranega kriminala, mednarodno organiziranih kriminalnih združb, ki se za razliko od organov odkrivanja in kazenskega pregona zelo hitro in dobro prilagajajo na nove okoliščine in jih izrabljajo v svoj prid za izvrševanje kriminalnih dejanj, postajajo na drugi strani kriminalistične preiskave vse zahtevnejše in dolgotrajne. Organi odkrivanja in kazenskega pregona različnih držav članic, ki vodijo posamezne kriminalistične preiskave se morajo zaradi vse novejših kriminalnih trendov in neomejenih sredstev kriminalnih združb nenehno prilagajati, usklajevati in tesno medsebojno sodelovati. V okviru mednarodnih kriminalističnih preiskav ta dejavnost terja izjemne napore in dragoceni čas. Nenazadnje pa v zadnjih letih k pešanju moči pripomorejo tudi vse večji deficiti kadrovskih in finančnih resursov, namenjenih preprečevanju in omejevanju mednarodne kriminalitete.

Organiziran kriminal se v okviru mednarodne razvejanosti kriminalnih združb v mednarodnem prostoru povezuje in deluje mnogo hitreje, kot to velja za delovanje organov odkrivanja oziroma kazenskega pregona. Ti so v nasprotju s kriminalci pri lastnih prizadevanjih določno omejeni tudi z varovanjem TČPS, ki pripadajo seveda tudi kriminalcem. Iste pravice nemalokrat kolidirajo z nasprotno pravico do varnosti poštenih državljanov. To sočasno predstavlja enega od razlogov, ki organe odkrivanja in kazenskega pregona zavira v dohajanju organiziranega kriminala. Dokaz za to ponujajo tudi statistični podatki slovenske policije (*glej graf 2*), ki v zadnjih dveh letih izkazuje očitno rast organizirane kriminalitete na območju Slovenije. Ugotovimo lahko, da je njena rast v obliki linearne trendne črte večja, kot pa je trend policijske zaznave pri odkrivanju iste vrste kriminalitete. Policija prav zato v svojem novem razvojnem dokumentu²² pripravlja smernice namenjene čim uspešnejšemu preprečevanju, odkrivanju in preiskovanju kriminalitete.

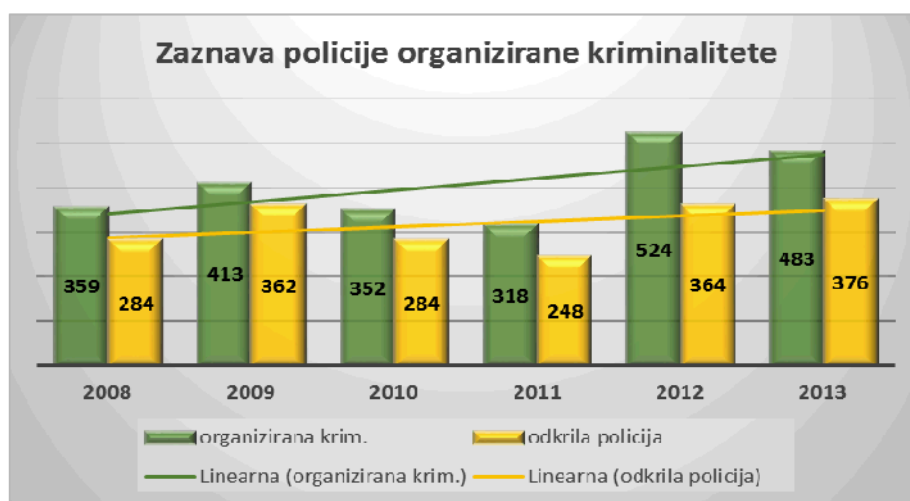
parlamenta in Sveta o uporabi podatkov iz evidence podatkov o potnikih za preprečevanje, odkrivanje, preiskovanje in pregon terorističnih in hudih kaznivih dejanj, 2011/C 181/02 ([http://eur-lex.europa.eu/legal-content/SL/TXT/?qid=1417208292976&uri=CELEX:52011XX0622\(02\)](http://eur-lex.europa.eu/legal-content/SL/TXT/?qid=1417208292976&uri=CELEX:52011XX0622(02)))

21 Vsi navajani povzetki primerov uspešne rabe PNR podatkov, izhajajo iz Spremnega dokumenta k predlogu DIREKTIVE EVROPSKEGA PARLAMENTA IN SVETA o splošnem pristopu k uporabi podatkov iz evidence podatkov o potnikih POVZETEK OCENE UČINKA {SEC(2011) 132 konč..

22 Resolucija o dolgoročnem razvojnem programu policije do leta 2022 EVA 2011-1711-0026.

Slednja namreč resno ogroža javno in mednarodno varnost, red, stabilnost in demokracijo ter grobo posega v TČPS posameznika. Strateški namen dokumenta teži k ustrezni prilagoditvi formalnih in funkcionalnih organizacijskih struktur, sodobnim trendom razvoja kriminalitete doma in v mednarodnem prostoru. Zato ugotavlja, nujne potrebe vpeljevanja novih metod, taktike in tehnike dela, z souporabo sodobnih tehničnih in tehnološko, informacijsko naprednih telekomunikacijskih rešitev. Iz istih razlogov Policija načrtuje tudi nadgradnjo specializiranih enot za boj proti terorizmu in drugim hujšim grožnjam javni varnosti ter varnosti ljudi in njihovega premoženja. Od teh enot se pričakuje višja učinkovitost izvedenih nalog, zlasti z uvajanjem novih taktik in metodik delovanja, z kar se da mogočo sodobno opremo. Eno od tovrstnih vizij slovenske policije bi bilo mogoče operacionalizirati tudi z ustrezno programsko in sistemsko uporabo podatkov PNR.

Graf 2: gibanje organizirane kriminalitete in lastna zaznava policije le-te



Pričakovano ocenjujemo, da bomo z uporabo podatkov PNR in njihovo izmenjavo, povečali delež lastnih zaznav pri odkrivanju hujših kaznivih dejanj s čezmejnimi elementi in njihovih storilcev. Tem storilcem bo z uporabo podatkov, torej t. i. elektronskih sledi, ki jih puščajo za seboj, mnogo lažje dokazovati utemeljene sume izvršitve in povezovanja pri izvrševanju navedenih kaznivih dejanj. Isto vodi v večjo učinkovitost, oziroma do uspešnejših zaključkov kazenskih postopkov zoper te storilce. V proaktivnem smislu bodo ti podatki omogočali izdelavo še kvalitetnejših in uporabnejših kriminalistično obveščevalnih informacij²³, kar zagotavlja učinkovito dejavnost policije v boju zoper hujše oblike kriminala.

Ustrezno ovrednotenje podatkov o potnikih (API), ob njihovi primerjavi z mednarodnimi (*SIS*, *SIS II*, *VIS*, *Interpol*, *EIS*, *FIU.net*) in nacionalnimi podatkovnimi zbirkami (*FIO*), po ocenah občutno pripomore tudi k izsleditvi iskanih oseb, ter oseb zoper katere so razpisani veljavni ukrepi s strani organov odkrivanja oziroma kazenskega pregona, v skladu z mednarodnim pravom, pravom EU in nacionalnim pravom. Mednarodno vzpostavljene podatkovne zbirke se uporabljajo za namene, potrditev identitet oseb, prijemanja iskanih oseb in razkrivanja

²³ 11. člen kriminalistično pridobivanje in vrednotenje informacij, Zakona o nalogah in pooblastilih policije (v nadaljevanju ZNPPol), Uradni list RS, št. 15/13.

kriminalnih združb, ter za izvajanje drugih zakonitih ukrepov zoper storilce kaznivih dejanj. S primerjavo teh podatkov s podatki PNR bi pričakovano dosegli tako kvantitativno, kot tudi kvalitativno višjo učinkovitost pri izvrševanju takih nalog policije, povezanih z mednarodnim sodelovanjem. S tem bi bila v veliki meri zapolnjena dosedanja vrzel kriminalističnega pridobivanja in vrednotenja informacij o kriminalnih dogodkih.

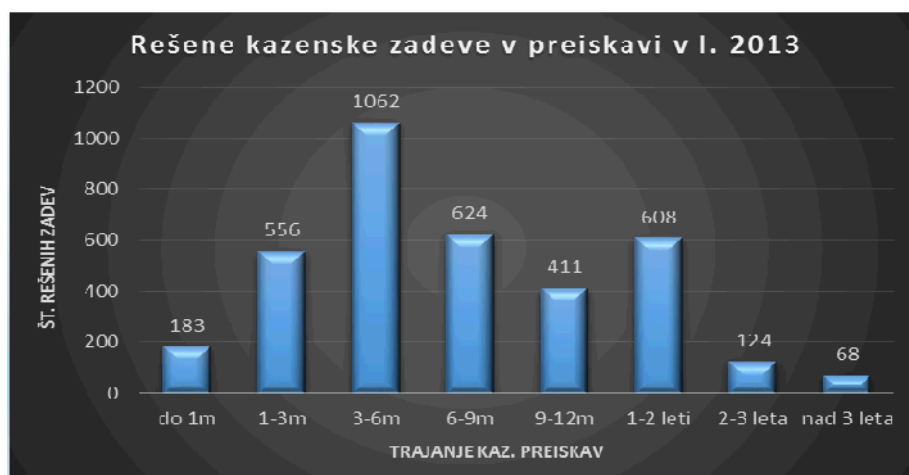
Podatki PNR se bodo uporabljali v predkazenskem postopku in v kazenskem postopku, tudi za uspešno dokazovanje krivde storilcev. Zaradi optimalnosti v kazenskem postopku bi morali biti organom odkrivanja in kazenskega pregona ti podatki dosegljivi ves čas trajanje preiskave, ki kot vemo, do pravnomočne obsodbe terjajo svoj čas. Zaradi boljšega pregleda trajanja celotnih postopkov smo pridobili statistične podatke iz policijskih evidenc o povprečnem trajanju kriminalističnih preiskav v letu 2013 pri preiskovanju organizirane kriminalitete (*glej graf 3*), ter podatke o sodni statistiki²⁴ za leto 2013 o trajanju kazenskih zadev v preiskavah na Okrožnih sodiščih (*glej graf 4*). Iz policijske statistike v grafu 3 je razvidno, da je v letu 2013 povprečna kriminalistična preiskava pri preiskovanju organiziranih oblik kriminalitete trajala približno 6 mesecev. V nadaljevanju pa se je v istem letu na Okrožnih sodiščih kazenska preiskava pri večini kazenskih zadev zaključila v obdobju od 1 do 2 let. V tem obdobju je bilo v fazi preiskav rešenih 94,7 % vseh kazenskih zadev. V kolikor čase iz policijske in sodne statistike seštejemo, ugotavljamo, da bi organi odkrivanja in kazenskega pregona za ta namen podatke PNR potrebovali vsaj dve leti.

Graf 3: Povprečno trajanje kriminalističnih preiskav v letu 2013 za organizirano kriminaliteto



²⁴ Bilten sodne statistike za leto 2013, tabela 393.

Graf 4: Trajanje rešenih kazenskih zadev v preiskavah na Okrožnih sodiščih v letu 2013



V Biltenu sodne statistike za leto 2013²⁵ smo iskali tudi podatek o pogostosti uvedbe kazenskih preiskav, kjer je razvidno, da so na Okrožnih sodiščih v RS v tem letu skupaj rešili 4651 zadev, pri čemer pa je bilo v istem obdobju izdanih 3486 sklepov o uvedbi kazenske preiskave. To pomeni, da je bila v kar 75 % vseh rešenih zadevah uvedena preiskava. Preiskava je namreč za potek kazenskega postopka zelo pomemben procesni institut, saj je namenjena prav zbiranju dokazov in drugih podatkov (glej 167. člen ZKP), ki so potrebni za odločitev o nadaljevanju kazenskega postopka. Eden od pomembnih informacijskih virov za zagotavljanje objektivnih dokazov in dejstev v kazenski preiskavi bi prav gotovo bila tudi evidenca o potnikih v letalskem prometu, s pomočjo katere bi lahko dokazovali krivdo storilcem, ter njihovo povezovanje z drugimi člani kriminalnih združb.

Dejstvo je, da mora biti rok hrambe podatkov v luči preizkusa sorazmernosti ustrezno utemeljen. Vsekakor mora biti omejen z namenom uporabe podatkov na eni strani, ter z doseganjem ustavno dopustnega cilja na drugi strani. Namen naše obdelave/uporabe podatkov PNR bo preprečevanje, odkrivanje, preiskovanje ali pregon terorističnih in drugih hudih kaznivih dejanj, pri čemer se bodo uporabljali za naslednje cilje:

- 1.) za odkritje in prijetje storilcev in sotorilcev navedenih kaznivih dejanj,
- 2.) za razkritje kriminalnih mrež in povezave med njihovimi člani,
- 3.) za dokazovanje krivde storilcem navedenih kaznivih dejanj.

V primeru podatkov PNR bo njihova uporabnost oziroma učinkovitost predvsem v predkazenskem, pa tudi v kazenskem postopku odvisna prav od časa hrambe podatkov in njihovega povezovanja s podatki API. Primarno so ti podatki v proaktivnem smislu namenjeni za izdelavo ocenjevalnih meril in na njihovi podlagi za (1. cilj) ugotavljanje istovetnosti t.i. »neznanih« oseb, ki predhodno še niso bile obravnavane ali osumljene sodelovanja pri navedenih kaznivih dejanjih, vendar pa bo iz analize podatkov izhajalo, da bi konkretna oseba lahko sodelovala pri teh dejanjih in bi jo bilo zato potrebno podrobneje varnostno obravnavati.

²⁵ glej tabele 50a in 62.

Natančna ocenjevalna merila, ki bi to omogočala, je mogoče izdelati le na podlagi reprezentativnega vzorca, kar pomeni, da potrebujemo dovolj velik obseg podatkov v določenem časovnem obdobju, ki nam predstavljajo lastnosti oziroma vzorec velike večine opazovane populacije. Z natančnimi ocenjevalnimi merili bi tako zmanjšali možnosti t.i. lažnih zadetkov, kar bi posledično seveda pomenilo tudi manjše tveganje za poseg v informacijsko zasebnost nedolžnih potnikov. Na drugi strani bo sprotna in reaktivna uporaba podatkov PNR organom odkrivanja v okviru tekočih kriminalističnih preiskav omogočala (2. cilj) odkrivanje nevarnih storilcev oziroma razkritje kriminalnih mrež in povezovanje med njihovimi člani pri izvajanju kriminalnih aktivnosti, ter (3. cilj) dokazovanje njihove krivde. Znano je, da gre v primeru terorističnih in drugih hudih kaznivih dejanjih za mednarodno razsežne kriminalne aktivnosti, pri čemer so mednarodna potovanja storilcev teh kaznivih dejanj postali sestavni del našega vsakdana. Po ocenah Interpola iz ozemlja EU na bojišča v Sirijo letno odpotuje cca. 3000 borcev – ekstremistov, ki se tam najprej urijo, nato pa se udeležijo v bojih na strani terorističnih skupin. Ta njihova potovanja so dolga in trajajo vse od enega leta in več. Za člane mednarodno delujočih kriminalnih omrežja je na drugi strani značilno, se pri izvajanju kriminalnih aktivnosti vse pogosteje med seboj povezujejo, pri čemer so zaradi časovno hitrejšega premagovanja daljših razdalj prisiljeni potovati z letali. Prav v tem segmentu ima čas hrambe podatkov izredno velik pomen, saj nam le ustrezno dolgo zgodovinsko obdobje podatkov za posameznega potnika omogoča zaznati njegov morebiten specifičen način potovanja/delovanja, ki se v sistemu PNR avtomatično prepozna in alarmira skozi posamezna ocenjevalna merila.

Uporabnost podatkov o potnikih je odvisna tudi od celovitosti analitičnega pristopa pri obdelavi podatkov o potnikih. Za uspešno odkrivanje hujših kaznivih dejanj s čezmejnimi elementom je potrebno uporabiti tudi dovolj širok nabor podatkov. Zato smo predvideli, da se bo zbiranje podatkov PNR izvajalo za mednarodne komercialne lete iz tretjih držav na ali preko ozemlja Slovenije oziroma obratno, za čarterske polete ter tudi za lete znotraj EU. Kot je znano, organiziran kriminal oziroma storilci, ki se s tem ukvarjajo ne izbirajo letov, posameznih letalskih družb ali zgolj lete iz tretjih držav na območje EU ali obratno. Potujejo namreč v kraje, kjer se neposredno povezujejo z drugimi kriminalnimi združbami oziroma tja, kjer trenutno izvajajo svoje kriminalne aktivnosti. Te kraje oziroma smer svojega potovanja ter njihov specifičen način izvrševanja kaznivih dejanj pogosto tudi menjajo zaradi prilagajanja na ukrepe organov odkrivanja oziroma kazenskega pregona. Eden tak primer iz izkušenj države članice smo že navedli, kjer je analiza podatkov PNR razkrila kriminalno združbo, ki se je ukvarjala s trgovino z ljudmi, pri čemer so pri potovanju z letali za prijavo na notranji let storilci uporabljali ponarejene dokumente, svoje prave dokumente pa za prijavo na let, namenjen iz/v tretjo državo. Poleg tega so pogosti tudi primeri, ko storilci za vstop v Schengensko območje izkoristijo velike ilegalne migracijske pritiske, kjer lahko nato z migracijsko urejenim statusom neovirano potujejo znotraj EU in izvajajo kriminalne aktivnosti. Izhajajoč iz tega dejstva je utemeljen naš predlog za zbiranje podatkov o potnikih tako na »zunanjih« EU letih, kot tudi na vseh »notranjih« EU letih. Na ta način bomo lahko celovito zaznavali kriminalno problematiko, ter enakovredno obravnavali vse potnike v letalskem prometu.

V sistemu vzletne kontrole (DCS) letalski prevozniki zbirajo in hranijo podatke o potnikih, t.i. API. Z vidika proaktivne uporabe, samostojni podatki API, kot so trenutno določeni v naši nacionalni zakonodaji (84.a člena Zakona o letalstvu) prav gotovo ne zadostujejo za doseg zgoraj navedenega 1. cilja. Takšni podatki namreč ne omogočajo izdelave ustreznih ocenjevalnih meril, ki bi predstavljali specifične potovalne vzorce večine storilcev hujših kaznivih dejanj. Vendarle pa so mednarodne organizacije (WCO, IATA, ICAO) z namenom standardizacije in posledično enotnega ter učinkovitega posredovanja teh podatkov pripravile smernice, v katerih je predstavljen širši nabor oziroma struktura podatkov API, ki naj bi jih v evidenci enotno obdelovali letalski prevozniki (*glej stran 14, 15*). Po izkušnjah Nizozemskih varnostnih mejnih organov ti razširjeni podatki omogočajo izdelavo ocenjevalnih meril za storilce kaznivih dejanj, povezanih z nezakonitim priseljevanjem preko t.i. zunanjih dohodnih letov, zato bi bilo smotno za zagotavljanje še učinkovitejše mejne kontrole, uporabiti tudi tak pristop.

Ker so z namenom zbiranja in hrambe podatkov API izvzeta teroristična in druga hujša kazniva dejanja, so za preprečevanje in odkrivanje slednjih pomembni tudi povezani vzorci podatkov o nakupu/rezervaciji vozovnice, o osebi, ki je rezervacijo vozovnice opravila, o turistični agenciji/potovalnem agentu, o načinu plačila, o vrsti vozovnice, o načrtu potovanja, o prtljagi potnika, ipd. Te podatke pa nam zagotavljajo podatki PNR iz sistema rezervacij letalskih kart, ki pa nam na drugi strani ne omogočajo popolne identifikacije posameznega potnika. Gre namreč za nepreverjene in delne osebne podatke, ki jih pri rezervaciji letalske karte posreduje potnik sam, brez datuma rojstva. Zaradi tega so podatki API iz sistema vzletne kontrole letalskih prevoznikov, njihova dodana vrednost, saj gre za preverjene podatke o potniku, ki omogočajo njegovo popolno identifikacijo. Tega se zavedajo tudi mednarodne organizacije IATA, WCO in ICAO, ki so v okviru delovne skupine oblikovali mednarodno priznan PNR.GOV standard za lažjo obdelavo podatkov PNR, katerih del so tudi podatki API²⁶.

Za doseg zgoraj navedenih ciljev definitivno potrebujemo povezavo med evidencama s podatki o potnikih²⁷ API in PNR. Ti povezani podatki bi **omogočali**:

- neposredno in popolno identifikacijo potnikov pred prihodom na letališče ali pred odhodom z letališča z namenom:
 - o identifikacije storilcev hujših kaznivih dejanj,
 - o razkritja kriminalnih mrež in osebnih povezav med njihovimi člani in
 - o dokazovanja krivde storilcem hudih kaznivih dejanj.
- manjše tveganje za preverjanje in kontrolo napačnih ljudi z enakimi ali podobnimi imeni (t.i. lažni zadetki), ki bi potovali v okviru rizičnega potovalnega modusa, ki bi bil značilen za storilce kaznivih dejanj.

Policisti, ki opravljajo mejno kontrolo na letališkem mejnem prehodu se bodo tako lahko že predhodno pripravili na podrobno preverjanje samo tistih oseb, ki predstavljajo veliko tveganje za javno, nacionalno in mednarodno varnost. Vsekakor bi povezava teh podatkov omogočala

26 Guidelines on Passenger Name Record (PNR) Data, Doc 9944, First edition 2010, glej prilogo 1.

27 V primeru podatkov API in PNR govorimo o dveh ločenih evidencah podatkov o potnikih, med katerima bi moral biti izveden sistem povezovanja osebnih podatkov za identifikacijo posameznega potnika.

identifikacijo storilcev terorističnih in drugih hudih kaznivih dejanj, ter identiteto drugih oseb, s katerimi se ti storilci povezujejo v kriminalna omrežja oziroma združbe. Le s takšnim celovitim in selektivnim načinom obdelave podatkov bomo lahko učinkoviti pri razbitju mednarodno delujočih kriminalnih mrež. Kot vemo storilci izvajajo svoje kriminalne aktivnosti še preden jim pride na sled policija in zoper njih začne kriminalistično preiskavo, ki kot smo navedli, v povprečju traja 6 mesecev. Za delo policijo so zato vsekakor pomembni tudi zgodovinski podatki. S tem povezan čas hrambe podatkov o potnikih je za tovrsten pristop preprečevanja kriminalitete izjemno pomemben segment, zato bi morala biti identifikacija potnikov omogočena dovolj dolgo, da bi lahko dosegli zgoraj navedena 2. in 3. cilj.

Glede na dejstvo, da letališki agentje na notranjih letih občasno opuščajo svojo dolžnost preverjanja skladnosti osebnih podatkov na vozovnici in v potovalnem dokumentu potnika, **bi uporaba povezanih API in PNR podatkov** v okviru obravnavanega novega pristopa policije pri preprečevanju, odkrivanju, preiskovanju in pregonu hudih oblik kaznivih dejanj **onemogočala tudi nekatere primere zakrivanja elektronskih sledi storilcev:**

- potovanje posameznika pod različnimi osebnimi imeni,
- uporabo ponarejenih osebnih dokumentov,
- zlorabe osebnih podatkov nedolžnim državljanom.

Izhajajoč iz predstavljenih potreb policije oziroma namena uporabe podatkov o potnikih, ter ob upoštevanju načela sorazmernosti pri doseganju ustavno dopustnega cilja ocenjujemo, da lahko zgoraj navedene cilje še lahko dosežemo ob upoštevanju naslednjih časovnih obdobj, povezanih s hrambo podatkov o potnikih, in sicer:

- hramba podatkov o potnikih PNR in API, bi se v ločenih samostojnih evidencah izvajala 12 mesecev od njihovega prvega posredovanja,
- po izteku tega obdobja, bi se podatki API in PNR hranili v samostojni evidenci še nadaljnjih 18 mesecev. V tem obdobju bi bili podatki maskirani z zakrivanjem določenih podatkovnih elementov²⁸. Dostop do popolnih podatkov bi bil možen le v posamičnih primerih pod zelo strogimi pogoji, in sicer le za namen zagotavljanja dokazov v predkazenskem oziroma kazenskem postopku. O upravičenosti tovrstnih argumentiranih zaprosil bi odločal predstojnik SI enote za informacije o potnikih,
- po preteku 30 mesečnega obdobja od prvega posredovanja podatkov API in PNR, bi se ti podatki iz evidence samodejno dokončno izbrisali.

Slovenija ima dolžnost v cilju zagotavljanja kar se da najvišje zagotovitve stopnje varnosti svojih državljanov, prilagoditi svoje nacionalno varnostne ukrepe, intenziteti vseh navedenih virov ogrožanja varnosti. Seveda s sočasnim zagotavljanjem državljanskih, ustavno zagotovljenih TČPS. Ob tem se zavedamo, da vsaka širitev policijskih pooblastil (v našem primeru na obdelavo in uporabo podatkov PNR) pomeni tudi dodatne posege v ustavno varovane človekove osebnostne

28 Maskiranje z zakrivanjem podatkov pomeni zakrivanje tistih podatkovnih elementov, na podlagi katerih bi bilo mogoče neposredno identificirati potnika, na katerega se nanašajo podatki API, PNR, in sicer tako, da jih uporabniki ne vidijo, ne da bi bili ti podatkovni elementi izbrisani.

pravice; varstvo zasebnosti posameznika in zaščito osebnih podatkov, ki sta ustavno varovani vrednoti.

V policiji obstaja zavest o nevarnosti zlorabe osebnih podatkov pri obdelavi podatkov PNR, kar bi seveda pomenilo tudi grob poseg v zasebnost posameznika, kateremu bi bili ti podatki zlorabljeni. Zavedamo se pomembnost in vrednosti TČPS, saj te vrednote niso omejene zgolj na območje ene same države, kjer jih varuje Ustava, temveč segajo mnogo širše v mednarodni prostor, kjer jih varujejo tudi Listina EU o temeljnih pravicah in Evropska konvencija o varstvu človekovih pravic in temeljnih svoboščin (*v nadaljevanju: EKČP*). Vendar so prav te pravice, nemalokrat kršene prav s kriminalno dejavnostjo. Primarna vloga policije je »zagotavljanje varnosti posameznikom in skupnosti, spoštovanje človekovih pravic in temeljnih svoboščin ter krepitev pravne države«²⁹. Za uspešno zagotovitev teh nalog v izjemnih primerih³⁰ že Ustava s podelitvijo pooblastil, kot varuhom najvišjih človeških vrednot, dopušča določena odstopanja in tako posredno izjemoma tudi posege v TČPS³¹. Takšna pooblastila so taksativno določena in omejena na strogo določene ustavne in zakonske okvire.

Ob prilagajanju na mednarodne razsežnosti kriminala, lahko policija le s pomočjo teh novih orodij – pooblastil, izpolni večji del svojega poslanstva. Slednje namreč izpolnjuje z izvajanjem policijskih pooblastil, ki so po svoji definiciji³² »z zakonom določeni ukrepi, ki policistom omogočajo opravljanje policijskih nalog in s katerimi se praviloma posega v človekove pravice ali temeljne svoboščine ali druge pravice.« Ti posegi so legitimni in legalni le, če so sorazmerni in nujno potrebni za zagotavljanje ustavno dopustnega cilja. Zavedamo se, da je v skladu z načelom sorazmernosti potrebno takšne posege izvrševati izjemoma, ko je to nujno in milejše sredstvo ni na voljo ter je sam cilj, ozirom pravica, ki se jo varuje ustavno dopustna. Zakonsko omejevanje človekove pravice ilustrira drugi odstavek 8. člena EKČP. Ta priznava pravico do zasebnega in družinskega življenja, vendar ne kot absolutno. Javni oblasti namreč v zakonsko pogojenih in nujnih razlogih dovoljuje vmešavanje; »v demokratični družbi zaradi državne varnosti, javne varnosti ali ekonomske blaginje države, zato, da se prepreči nered ali zločin, da se zavaruje zdravje ali morala ali da se zavarujejo pravice in svoboščine drugih ljudi.« In prav obdelava/uporaba podatkov PNR po našem tehtnem preudarku nedvomno sodi v okvir takšnih izjem, saj je njihov namen usmerjen v boj zoper terorizem in druge hujše oblike kriminalitete. Slednja na tehtnici nasproti varovanju zasebnosti in varstva podatkov, predstavlja očitno neravnotežje, v prid kriminalu.

EU je v zadnjih letih na področju preprečevanja terorizma in drugih hujših oblik kriminalitete dosegla velik napredek. Zaradi odprave notranjih mejnih kontrol na schengenskem območju je EU, kot odziv na nevarnost hujših oblik kaznivih dejanj, na podlagi Konvencije o schengenskih mejah, sprejela še druge ukrepe za izmenjavo obveščevalnih informacij, osebnih in drugih podatkov med pristojnimi organi držav podpisnic konvencije (*Europol, Eurojust, SIS, SIS II, VIS*,

29 Povzetek 2. odstavka 1. člena Zakona o nalogah in pooblastilih policije (ZNPPol), Ur. l. RS št. 15/2013, z 18.2.2013.

30 15. člen Ustave RS (uresničevanje in omejevanje pravic)

31 »Polijsko pooblastilo je z zakonom določen ukrep, ki policistom omogoča opravljanje policijskih nalog in s katerim se praviloma posega v človekove pravice ali temeljne svoboščine ali druge pravice.«, 2. točka, 1. odstavek, 3. člena, ZNPPol.

32 2. točka, 1. odstavek, 3. člena Zakona o nalogah in pooblastilih policije, Ur. l. RS št. 15/2013, z 18.2.2013.

EURODAC, CIS, Prumska pogodba, Švedska iniciativa,...). Ta orodja, oziroma evidence se uporabljajo za preverjanja identitet znanih oseb, ki so že osumljene storitve kaznivih dejanj. Za primere terorističnih groženj pa se izkazuje potrebe po izvajanju predhodnih, kar se da zgodnjih preventivnih ukrepanjih. Zato primeri zgolj reakcije, kot jih ponujajo opisana orodja, oz. evidence ne zadostujejo. Odkrivanju potencialnih storilcev in groženj (*vsa pripravljana teroristična dejanja predstavljajo samostojno kaznivo dejanje*)³³, je nujno v predhodnem obdobju, še preden bi uspeli svoja prepovedana ravnanja dokončati. V tem pogledu se sistem obdelave podatkov PNR ločuje od že obstoječih orodij. Uporaba teh podatkov je namenjena predvsem proaktivnemu delovanju enot za informacije o potnikih v državah članicah, ki bodo znatno prispevale k preprečevanju terorističnih in hudih kaznivih dejanj. Prav z razčlenitvijo podatkov o potnikih bodo te enote ugotovljale istovetnost »neznanih« oseb, ki predhodno še niso bile obravnavane ali osumljene sodelovanja pri navedenih kaznivih dejanjih, vendar pa bo iz analize podatkov izhajalo, da bi konkretna oseba lahko sodelovala pri teh dejanjih in bi jo bilo zato potrebno podrobneje varnostno obravnavati.

2.3 Primerjalno pravni zakonodajni vidik obdelave podatkov

Pred razpisom evropskega ISEC PNR projekta so redke države članice uporabljale podatke PNR za namen preprečevanja in omejevanja kriminalitete. Med temi redkimi državami sta bili tudi Švedska in Nizozemska, kjer so že pred tem imeli zakonsko podlago, ki je predvsem Carinskim organom omogočala zelo omejeno uporabo teh podatkov in na zelo nesistematičen način. Prav zaradi tega sta se ti dve državi članici prijavili na navedeni evropski razpis, v katerem sodeluje skupaj 14 držav članic, med katerimi je tudi Slovenija. Vse te države so že v lanskem letu podpirale sprejetje EU PNR direktive, saj bi le-ta omogočala harmonizacijo nacionalnih sistemov PNR in usklajeno obdelavo teh podatkov, ter njihovo izmenjavo. Ker kljub tem prizadevanjem predlog Direktive še ni bil potrjen v EU parlamentu, so nekatere posamezne države članice že sprejele nacionalno zakonodajo za regulacijo tega področja, vendar so pri tem izhajale iz vsebine navedenega predloga direktive. Pri pripravi tega dokumenta smo tudi mi izhajali iz istega vira, zato nismo pristopili k izvedbi obširne primerjalno pravne analize v tem poglavju.

Člani projektne skupine za izvedbo slovenskega PNR projekta so v mesecu marcu in aprilu 2015 izvedli dva študijska obiska pri varnostnih organih v Franciji in v Madžarski, ki so prav tako udeleženi v EU PNR projektu. Ti dve državi sta eni izmed redkih držav članic, ki že imajo sprejeto nacionalno zakonodajo za pridobivanje, hrambo, analizo in posredovanje PNR podatkov o potnikih. Za tovrstno analizo sta zanimivi tudi zato, ker gre za dva različna skrajna primera pravnih podlag, izhajajoč iz skupne osnove (predlog EU PNR direktive) in izhajajoč iz istih standardov varstva osebnih podatkov. Na eni strani je Francija po nedavnih terorističnih napadih sprejela zakonodajo, ki jim omogoča dokaj širok spekter obdelave in uporabe podatkov o potnikih API in PNR, na drugi strani pa Madžarska, kjer imajo relativno omejeno zakonsko podlago v tem kontekstu. V primeru Francije lahko dejansko zaznamo očitno zavedanje ljudi o neposredni ogroženosti s strani terorizma. To je bil prav gotovo razlog, da so se trenutno pripravljeni odreči določeni stopnji informacijske zasebnosti, za razliko od ljudi na Madžarskem,

33 1. člen točka (i) grožnja, da se bo izvršilo katero od dejanj, naštetih v točkah (a) do (h), Okvirnega sklepa Sveta 2002/475/PNZ o boju proti terorizmu.

kjer imajo trenutno ljudje zagotovljeno večjo stopnjo varnosti in zato tudi potrebo po večji stopnji informacijske zasebnosti.

2.3.1 PNR pravna ureditev v Franciji

Francija, podobno kot Slovenija, sodeluje v EU PNR projektu, v okviru katerega vzpostavlja lasten PNR sistem za ocenjevanje potnikov v letalskem prometu. Razvoj informacijskega sistema in IT infrastrukture, kot tudi kadrovska in organizacijska struktura so še v fazi postopne implementacije, ki bo predvidoma zaključena do jeseni 2015. Za potrebe obdelave podatkov PNR že imajo sprejeto novo nacionalno zakonodajo, ki v večini temelji na vsebini predloga EU direktive o uporabi PNR podatkov iz leta 2012. Ta njihova zakonodaja ima omejeno veljavnost (»sunset clause«), za obdobje 2015-2017. Po tem obdobju se bo zakonodajalec lahko odločil za njeno podaljšanje, če bodo iz analize stanja ugotovili uporabnost podatkov o potnikih v praksi. Francoska enota za informacije o potnikih bo multi institucionalna enota, v kateri bodo zaposleni uslužbenci iz različnih varnostno obveščevalnih služb, zaradi boljše izmenjave informacij. Trenutno ta enota še ni operativna. Podatke PNR bodo lahko obdelovali z namenom preprečevanja, odkrivanja, preiskovanja in pregona terorističnih in drugih hudih kaznivih dejanj (seznam KD iz EU direktive o EAW), ter zaradi zagotavljanja nacionalne varnosti. V prvi fazi projekta bodo PNR podatke zbirali samo za zunanje EU lete, v nadaljevanju pa tudi za notranje lete. Zbiranje teh podatkov bo potekalo izključno po »push« metodi, pri čemer bodo podatki posredovani 48 ur pred letom in nato še ob zaprtju leta. Vsebinsko gledano bodo prejeli širok nabor manj občutljivih podatkov PNR v mednarodno priznanem PNR.GOV formatu, pri čemer so podatki API določeni kot del podatkov PNR. Absoluten rok hrambe imajo določen na pet let, v okviru katerega se bodo podatki po dveh letih od njihovega posredovanje anonimizirali. Tudi v tem obdobju bo razkritje identitete posameznega potnika možno, vendar samo na podlagi argumentiranega zaprosila, o katerem bo odločal predstojnik PNR enote, njegov namestnik ali druga pooblaščen oseba.

2.3.2 PNR pravna ureditev v Madžarski

Tudi Madžarska je udeležena v EU PNR projektu, v okviru katerega vzpostavljajo svoj nacionalni PNR sistem za obdelavo, hrambo in uporabo podatkov o potnikih v letalskem prometu. S projektnimi sredstvi so kupili kompleksen PNR informacijski sistem z implementiranimi ustreznimi programskimi orodji, kateri bo z omejeno funkcionalnostjo začel delovati že od julija 2015. Ta sistem bo popolnoma ločen od drugih informacijskih sistemov policije, ki jih uporabljajo za preprečevanje in omejevanje kriminalitete. Naloge pridobivanja, hrambe, obdelave in uporabe podatkov PNR bo opravljala nacionalna enota za informacije o potnikih, ki je trenutno še neoperativna in je organizirana v tamkajšnjem »Coordination Centre Against Organized Crime«. Ta enota praviloma ne bo pridobivala podatkov API, razen v posameznih obrazloženih primerih za osebe, ki jim bodo predstavljale visoko stopnjo tveganja. Že v zgodnji fazi njihovega projekta so v okviru nacionalnega pravnega reda sprejeli zakonsko podlago za pridobivanje, hrambo, obdelavo in uporabo podatkov PNR. Nacionalno zakonodajo so sprejeli že novembra 2013, začela pa je veljati v januarju 2015. Pri oblikovanju te pravne podlage so izhajali iz predloga EU PNR direktive, vendar pa je končna sprejeta vsebina precej bolj omejena kot v tem predlogu. Namen obdelave podatkov je v zakonodaji omejen na preprečevanje,

odkrivanje in preiskovanje terorističnih aktivnosti in organiziranega kriminala ter na zagotavljanje nacionalne varnosti. Podatke PNR bodo zbirali izključno za vse zunanje EU lete. Od letalskih prevoznikov bodo podatke prejeli po »push« metodi, pri čemer bodo za vsak let podatke prvič prejeli 12 ur pred letom in drugič ob zaprtju leta, vendar pa podatkov API in PNR ne bodo združevali. Vsebinsko gledano bodo prejeli ožji nabor (16 segmentov) manj občutljivih podatkov PNR v mednarodno priznanem PNR.GOV formatu. Absoluten čas hrambe podatkov imajo omejen na 5 let, vendar pa se bodo ti po 30 dneh od prejema depersonalizirali. Tudi v tem obdobju bo razkritje identitete posameznega potnika možno, vendar samo na podlagi dovoljenja za to pooblaščen osebe.

2.4 Vsebina in način obdelave ter operativna uporaba podatkov

2.4.1 Splošno o uporabi podatkov

Analitična obdelava podatkov o potnikih (PNR, API) pred prihodom potnika iz tretjih držav na območje EU, kot tudi znotraj Schengenskega območja, ne more predstavljati začetka izvajanja mejne kontrole. V 33. členu Zakona o nadzoru državne meje je namreč določeno, da je »*Območje opravljanja mejne kontrole je del mejnega prehoda, kjer policist opravlja mejno kontrolo.*« Naloge policistov, ki opravljajo mejno kontrolo pa so določene v 28. členu istega predpisa, iz katerih je razvidno, da analitični pristop policije s predhodno obdelavo podatkov o potnikih nikakor ni del mejne kontrole. To izhaja tudi iz pravilnika³⁴ o izvajanju navedenega zakona, ki podrobno predpisuje način opravljanja mejne kontrole. V primeru predhodne obdelave podatkov gre vsekakor za usmerjen pristop policije, ki omogoča lahko pripravo na izvedbo mejne kontrole in s tem njeno učinkovitejše izvajanje pri odkrivanju hujših oblik kriminalitete. V teh primerih gre za izvajanje analitične podpore najprej policistom, ki zoper letalske potnike ob prihodu na mejni prehod izvajajo mejno kontrolo, ter v nadaljevanju vsem drugim policistom, ki se ukvarjajo s preprečevanjem, odkrivanjem in preiskovanjem hujših oblik kaznivih dejanj.

V nasprotju s podatki API, ki ob neposredni letališki kontroli ob vkrcanju potnikov na letalo pripomorejo k identifikaciji posameznikov, pa tega ne omogočajo podatki PNR. Ti bodo služili strateškemu in operativnemu ocenjevanju tveganj posameznikov, ki bodo povezani s kriminalno dejavnostjo. V teh okvirih bodo omogočali pri ugotavljanju morebitnih korelacij med znanimi in neznanimi osebami. Sami podatki API namreč trenutno takšne operativne ocene potnika ne omogočajo, zato tudi ne pripomorejo kaj veliko k odkrivanju neznanih storilcev kaznivih dejanj, kot so npr. teroristi³⁵.

Podatki PNR se bodo v sklopu njihove proaktivne uporabe avtomatizirano obdelovali in temu primerno uparjali na podlagi vnaprej določenih transparentnih ocenjevalnih meril. Temeljite analize podatkov bodo služile nadgrajevanju, oblikovanju ter posodabljanju nediskriminatornih³⁶ ocenjevalnih meril. Ista bodo povezana s specifičnimi posebnostmi podatkov PNR, oziroma z v

34 Pravilnik o izvajanju Zakona o nadzoru državne meje, Uradni list RS, št. 116/07 in 38/12).

35 Povzeto po obrazložitvenem memorandumu in 6. tč. Predloga Direktive PNR

36 Ustava RS, 14. člen (enakost pred zakonom) V Sloveniji so vsakomur zagotovljene enake človekove pravice in temeljne svoboščine, ne glede na narodnost, raso, spol, jezik, vero, politično ali drugo prepričanje, gmotno stanje, rojstvo, izobrazbo, družbeni položaj, invalidnost ali katerokoli drugo osebo okoliščino. Vsi so pred zakonom enaki.

naprej opredeljenimi potovalnimi modusi storilcev terorističnih in drugih hujših kaznivih dejanj in bodo na takšne osebe uspešno predhodno opozarjala. Navkljub zakonsko dopustnemu taktičnemu preudarku³⁷, bo v izogib mogočemu subjektivnemu in arbitrarnemu odločanju, potrebno vsako avtomatizirano ujemanje podatkov obvezno še dodatno ročno preveriti ter dodatno potrdi ali zavrniti visoko stopnjo tveganja posameznega zadetka. Taka sistematična ureditev obdelave podatkov PNR, vključujoč predhodne operativne izkušnje policistov, bodo pred prihodom/odhodom potnikov na letališče, SI enoti za informacije o potnikih, omogočala izvedbo ustrezne ocene tveganja. S to informacijo bodo policisti lahko vnaprej pripravljeni na selektivno obdelavo zgolj tistih oseb, ki predstavljajo veliko tveganje za javno in mednarodno varnost. Ostalim potnikom bo s tem potovanje olajšano, s hkratno zagotovljeno višjo stopnjo varnosti, ob vstopu v ali iz EU. Posledično bo isto zanje pomenilo nižje možnosti, podvrženosti podrobnim varnostnim pregledom, še zlasti pa očitkom domnevno diskriminatornih meril in diskrecijskih odločitev mejnih policistov in carinikov.

Ob proaktivni uporabi bodo organi odkrivanja oziroma kazenskega pregona podatke PNR uporabljali tudi reaktivno in sprotno. V sklopu aktualnih kriminalističnih preiskav bodo informacije omogočale uspešnejše preprečevanje in odkrivanje tistih kaznivih dejanj, ki se pripravljajo oziroma se že izvajajo, ter tudi odkrivanje storilcev in njihovo povezovanje s sotorilci hujših kaznivih dejanj (*zbiranje dokazov, identifikacija storilcev in kriminalnih mrež*). Sočasno pa bi v povezavah z ustreznimi zakonsko opredeljenimi nacionalnimi in mednarodnimi zbirkami, pripomogle k iskalni poti iskanih oseb ali oseb, zoper katere so razpisani drugi zakoniti ukrepi. Iskanje oseb je namreč eno izmed generalnih policijskih pooblastil, ki je določeno v 43. členu ZNPPol. Prav tako to policiji nalaga 148. člen ZKP, na podlagi katerega »...**mora policija ukreniti potrebno, da se izsledi storilec kaznivega dejanja, da se storilec ali udeleženec ne skrije ali ne pobegne...**«. Za izvršitev te naloge pa sme policija »...**ukreniti, kar je potrebno v zvezi z ugotavljanjem istovetnosti oseb in predmetov..., razpisati iskanje osebe in stvari, ki se iščejo...**«. Način iskanja, vrste razpisov in ukrepi so natančno določeni z navodilom³⁸, ki ga je na zakonski podlagi izdal generalni direktor policije. Pri iskanju oseb in predmetov podatki PNR niso uporabni, saj gre pri tem za iskanje znanih storilcev, ki so že izvedle kaznivo dejanja, ali ga izvajajo, ali pa se nanj pripravljajo, in je razpis ukrepov zoper te osebe nujno potreben za izvedbo kazenskega pregona. Ti ukrepi se razpisujejo v nacionalne in mednarodne evidence (FIO, SIS II, Interpol, Europol), ki se za razliko od evidence podatkov PNR uporabljajo za preverjanja (potrjevanje) identitet znanih oseb, ki so že osumljene storitve ali poskusa storitve kaznivih dejanj. V tem pa je tudi bistvena razlika, ki podatke PNR ločuje od obstoječih orodij. Prav zato predstavlja kombinirana uporaba obeh pristopov (avtomatizirano preverjanje podatkov o potnikih skozi policijske evidence – znani storilci in preverjanje podatkov skozi ocenjevalna merila – neznani storilci) še učinkovitejši in celovit pristop policije pri odkrivanju in prijemanju storilcev kaznivih dejanj.

37 ZNPPol, 7. člen (taktični preudarek) Policisti pri opravljanju policijskih nalog ocenjujejo, katere odločitve, policijska pooblastila ali uradna dejanja bodo za učinkovito preprečevanje in odpravljanje nevarnosti izvedli, glede na dejstva in okoliščine, ki so jim bile znane v trenutku ocenjevanja.

38 Dokument št. 024-94/2013/, z 20. 1. 2014.

2.4.1.1 Delovanje SI PNR dvotirnega sistema

Podatke o potnikih pridobijo letalski prevozniki v dveh ločenih podatkovnih bazah podatkov. Kot smo že predhodno omenili, gre za evidenco vzletne kontrole (DCS) in evidenco rezervacije letalskih kart (CRS). Te podatke pa že oziroma bodo lahko pridobivali tudi organi odkrivanja oziroma kazenskega pregona, vendar se tudi v zakonodaji že predvideva ločevanje podatkov API in PNR po njihovem namenu uporabe. Namen prvih je v zakonski podlagi že omejen na zunanje lete ter na učinkovit boj proti nezakonitemu priseljevanju in izboljšanje mejne kontrole, za podatke PNR pa se predvideva uporaba v boju zoper terorizem in druga kataloško določena hujša kazniva dejanja. To ločnico med podatki bomo ohranili tudi v našem SI PNR sistemu za obdelavo podatkov o potnikih, zato načrtujemo razvoj dvotirnega sistema, ki bo pri sprotnem preverjanju podatkov o potnikih (PNR, API) razdeljen na dva glavna segmenta:

1. Analitična obdelava podatkov (*zeleno polje v sliki 1*),
2. Tiralčno tehnična obdelava podatkov (*rdeče polje v sliki 1*).

Izvedba analitične obdelave podatkov

Skladno z dvotirnostjo sistema se bo analitična obdelava podatkov ločila na obdelavo podatkov PNR in obdelavo podatkov API. Letalski prevoznik bo za vsak let, 24 ur pred načrtovanim vzletom iz centralnega rezervacijskega sistema posredoval podatke PNR (*glej PNR1 v sliki 1*) SI enoti za informacije o potnikih. Ob sprejetju se bodo podatki PNR1 v SI PNR sistemu avtomatično preverili po predhodno določenih ocenjevalnih merilih, pri čemer se bodo uparili zadetki, ki jih bo moral operater vedno še dodatno ročno preveriti. Drugo posredovanje teh podatkov iz sistema CRS se bo izvedlo ob zaprtju posameznega leta (*glej PNR2 v sliki 1*). Takrat bo letalski prevoznik poleg teh podatkov posredoval še podatke API iz sistema DCS. Ko bodo ti podatki prispeli v SI PNR sistem policije, se bodo izvedle naslednje zaporedne aktivnosti:

Analitična obdelava podatkov PNR

- podatki PNR1 in PNR2 se bodo med seboj samodejno primerjali z namenom, da se ugotovi ali je na konkretnem letu prišlo do kakšnih koli sprememb pri potnikih. Morebitne spremembe se bodo uparile, ki jih bo operater moral ročno preveriti in potrditi njihovo morebitno aktualnost za kasnejše izvajanje mejne kontrole ob prihodu potnika na območje letališkega mejnega prehoda.
- za tem se bodo podatki PNR2 samodejno primerjali s prispelimi API podatki, zaradi ugotovitve identičnosti osebnih podatkov oziroma zaradi identifikacije posameznega potnika z namenom kasnejše izločitve morebitnih napačnih zadetkov pri uparjanju skozi ocenjevalna merila.
- v zaključku te primerjave podatkov, pa se bodo podatki PNR2 samodejno preverili skozi ocenjevalna merila, pri čemer se bodo uparili zgolj posamezni zadetki, ki bodo ustrezali danim kriterijem. Zadetke bo moral operater še ročno preveriti in označiti morebitne lažne zadetke.

Analitična obdelava podatkov API

Kot smo že predhodno navedli, so mednarodne organizacije (WCO, IATA, ICAO) pripravile smernice, v katerih je predstavljen širši nabor oziroma struktura podatkov API. Ti podatki po izkušnjah nizozemskih varnostnih mejnih organov omogočajo izdelavo učinkovitih ocenjevalnih meril za storilce kaznivih dejanj, povezanih z nezakonitim priseljevanjem preko t.i. zunanjih dohodnih letov.

API direktiva, ki je v našem nacionalnem pravnem redu implementirana v Zakonu o letalstvu določa, da se podatki API obdelujejo pri prevozu oseb na ozemlje držav članic zaradi:

- učinkovitega boja proti nezakonitemu priseljevanju in
- izboljšanje mejne kontrole.

V skladu s tem namenom bomo iz prejetih podatkov API (podobno kot pri podatkih PNR), izdelovali ocenjevalna merila (*v nadaljevanju: API ocenjevalna merila*), vendar za razliko od PNR podatkov **le za zunanje dohodne lete**, ki bodo predstavljala specifične vzorce storilcev **hujših kaznivih dejanj**³⁹, **povezanih z bojem proti nezakonitemu priseljevanju**, in sicer:

- Spravljanje v suženjsko razmerje (112. člen KZ),
- Trgovina z ljudmi (113. člen KZ),
- Ponarejanje listin (251. člen),
- Prepovedano prehajanje meje ali ozemlja države (308. člen)

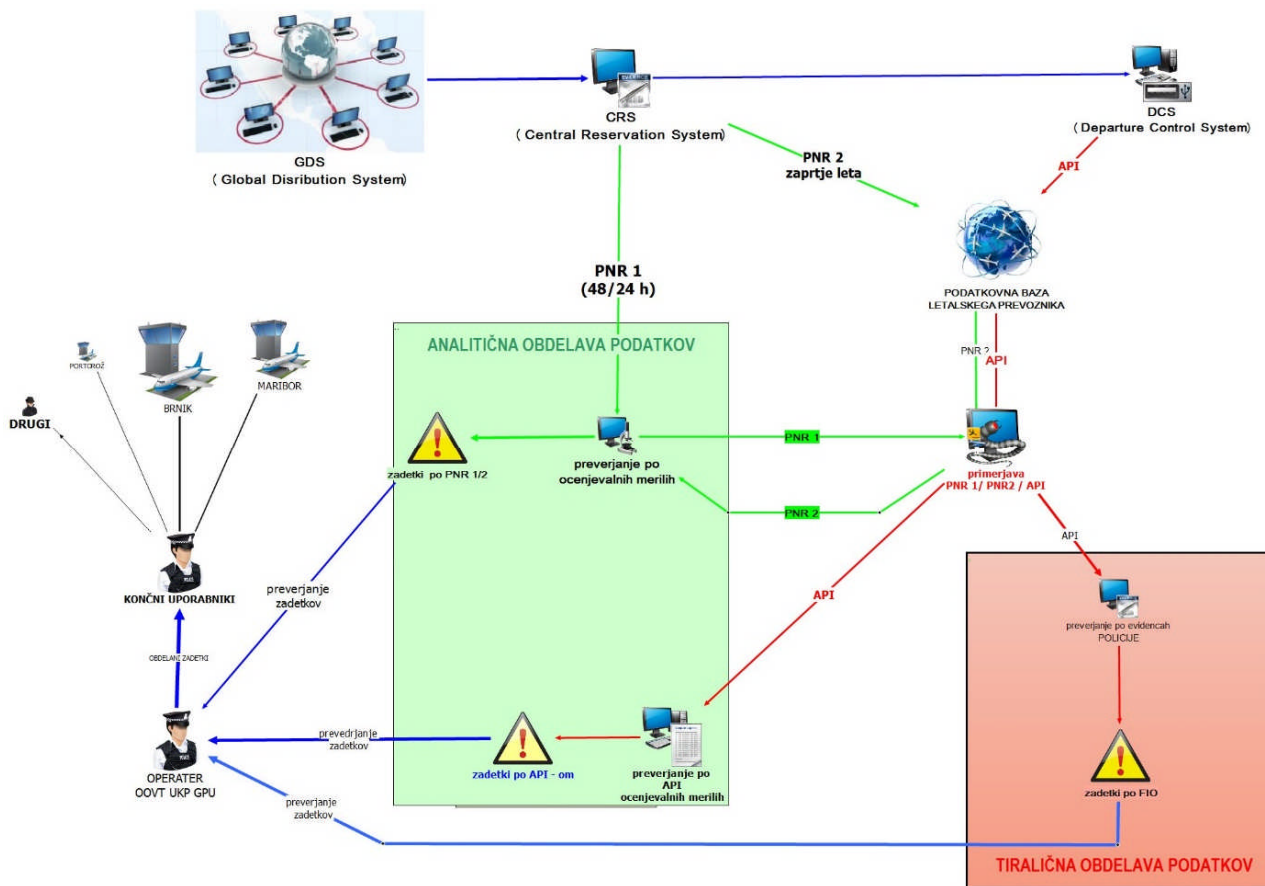
V zaključku zgoraj navedene primerjave podatkov API in PNR se bodo podatki API samodejno preverili še skozi API ocenjevalna merila, pri čemer se bodo uparili zgolj posamezni zadetki, ki bodo ustrezali danim kriterijem. Zadetke bo moral operater, tako kot vse ostale še ročno preveriti in označiti morebitne lažne zadetke.

Tiralično tehnična obdelava podatkov

V okviru celotne obdelave podatkov v SI PNR sistemu se bodo podatki API na koncu samodejno preverili še skozi zakonsko določene zbirke osebnih podatkov - evidence (FIO, Sirene, Interpol, Europol) z aktualnimi razpisanimi ukrepi za osebe in skozi operativne informacije, nanašajoč se na hujša kazniva dejanja, kot bodo z zakonom tudi natančno določena.

39 Gre za predvsem hujša ali z njimi povezana - predikatna kazniva dejanja.

Slika 1: Princip delovanja dvotirnega SI PNR sistema



2.4.2 Zbiranje podatkov

2.4.2.1 Vsebina zbranih podatkov

Z namenom preprečevanja, odkrivanja, preiskovanja in pregona terorističnih in drugih hudih kaznivih dejanj bi policija potrebovala nabor podatkov PNR, ki jih letalski prevozniki že zbirajo, obdelujejo in hranijo v sistemu rezervacij letalskih kart. Nabor teh podatkov je povzet iz smernic⁴⁰ mednarodne organizacije za civilno letalstvo (ICAO):

PNR podatek	Opis PNR podatka
Podatki v zvezi z letom	Informacije o letih pod skupno oznako Število potnikov
PNR referenčna številka ali PNR lokator	Rezervacijska referenčna številka, PNR lokator ali kateri koli drugi podatkovni lokator, ki ga je uporabil letalski prevoznik, s katerim je lociral potnika v svojem informacijskem sistemu

40

Doc 9944, Guidelines on Passenger Name Record (PNR) Data, ICAO, 2010

Datum rezervacije letalske karte/ datum izdaje letalske karte	Datum, na katerega je bila opravljena rezervacija/izdaja letalske karte
Datum/datumi nameravanega potovanja/a	Datum nameravanega potovanja
Ime in priimek	Ime in priimek kot je izpisan na rezervaciji
Naslov in kontaktni podatki	Kakršnakoli kontaktna telefonska številka Naslov Elektronski naslov
Vse oblike informacij o plačilu, vključujoč naslov za pošiljanje računa	Oblika plačila, ki je bila uporabljena za nakup letalske karte ali za izvedbo rezervacije Podrobnosti posamezne uporabljene oblike plačila, vključujoč številko kreditne, debetne ali katerekoli druge plačilne kartice Naslov za pošiljanje računa ATFQ iz katere je razvidna cena, ki je bila navedena in zaračunana
Celoten načrt potovanja	Celoten načrt potovanja za potnike na istem rezerviranem letu Podatek ali je rezervacija za enosmeren let "Odhodni" indikator, iz katerega je razvidno kam bo potnik nadaljeval let "Dohodni" vezni indikator, iz katerega je razvidno, kje točno je potnik začel potovanje, preden je prispel na letališče Razred v katerem potnik potuje
Informacije o potnikih, ki pogosto letijo	Številka potnika, ki pogosto leti Številka kartice potnika, ki pogosto leti Informacije v zvezi s programi zvestobe
Potovalna agencija/agent	Podatki o katerem koli uporabljenem potovalni agenciji/agentu Kraj izdaje letalske karte
Potovalni status	Potovalni status potnika, vključno s potrditvijo, prijavo na let, informacijami o neizkoriščenih in ne odpovedanih rezervacijah ter informacijami o vozovnicah brez rezervacije Čas prijave Identiteta osebe, ki je izvedla prijavo potnika na let

Splošne opombe ⁴¹	Ostale servisne informacije (potnik na primer zaprosil za sedež pri oknu, potnik doda še dodatno kontaktno telefonsko številko, vključno z vsemi razpoložljivimi informacijami o mladoletnikih z/brez spremstva mlajšimi od 18 let, kot so ime in spol, starost, znanje jezikov, ime in kontaktni podatki varuha, zastopnika pri odhodu/prihodu ter sorodstveno razmerje z mladoletnikom,...)
Podatki o letalski karti	Številka letalske karte Datum izdaje letalske karte Vrsta letalske karte (enosmerna, povratna,...) Razred, ki je bil rezerviran za potovanje in druge informacije na vozovnici
Številka sedeža ter druge informacije o sedežu	Dodeljena številka sedeža Zaprošena številka sedeža Druge informacije v zvezi s sedežem
Koda o deljenih informacijah	Naziv katerega koli prevoznika, ki bo prevažal potnika na določen delu celotnega potovanja
Informacije o osebni prtljagi	Število kosov, teža in opis prtljage potnika Kakršnikoli dokumenti, dodeljeni potniku, ki se nanašajo na njegovo prtljago
Številka ter druga imena potnikov v PNR	Število potnikov, ki so zabeleženi na isti rezervaciji Druga imena, ki se pojavijo na isti rezervaciji Druga imena, ki jih je uporabljal potnik v PNR rezervaciji
Vse zgodovinske spremembe PNR podatkov	Vse zgodovinske spremembe PNR podatkov, ki so navedeni zgoraj

2.4.2.2 Neselektivno zbiranje podatkov

Dejstvo je, da gre pri obdelavi podatkov o potnikih za neselektivno zbiranje podatkov za osebe, ki potujejo z letalskim prevozom na notranjih, zunanjih in čarterskih letih. V luči varovanja temeljnih človekovih pravic in svoboščin oziroma v našem primeru informacijske zasebnosti je neselektivnost pri zbiranju in hrambi podatkov ključni dejavnik pri teh posegih. To pomeni, da se z zbiranjem in hrambo podatkov o potnikih v prevladujočem delu posega v informacijsko zasebnost tistih (nedolžnih) potnikov, ki z namenom obdelave podatkov nimajo nobene zveze. Z

41 V tem in v drugih segmentih PNR sheme bodo izločeni vsi občutljivi podatki, ki se nanašajo na zdravstveno stanje potnika in s tem povezane posebne potrebe, prehrano, ter druge osebne okoliščine, povezane z verskim, političnim ali drugim prepričanjem ali katerokoli drugo TCPS.

neselektivnim zbiranjem in hrambo podatkov nastajajo pri upravljavcih obsežne podatkovne zbirke, iz katerih je z analitično obdelavo mogoče izluščiti tudi nekatere okoliščine o vsakdanjem življenju vsakega posameznika, ki uporablja letalski prevoz. S tem pa se poveča tudi tveganje za nezakonit dostop in zlorabo teh podatkov, kar smo podrobneje obdelali v podpoglavju 3.2 (*tveganja povezana z obdelavo podatkov PNR in upravljanje z njimi*).

Neselektivnosti zbiranja podatkov se moramo zavedati in striktno upoštevati pri presoji v okviru strogega testa sorazmernosti. Na to je opozorilo tudi Sodišča EU v svojih odločitvah C-293/12 in C- 594/12, kjer je glavni očitke neustavnosti utemeljen na obvezni hrambi podatkov, kot jo je določala Direktiva 2006/24/ES (t.i. data retention). Sodišče je v svoji sodbi z 8. 4. 2015 omenjeno direktivo razglasilo za neveljavno, ker je zakonodajalec z njenim sprejetjem prekoračil meje, ki jih zahteva spoštovanje načela sorazmernosti iz Evropske listine o temeljnih pravicah. Neselektivnost ukrepa je bil tudi eden glavnih očitkov Ustavnega sodišča RS, ki je z odločbo U-I-65/13-19 z dne 3.7.2014 razveljavilo posamezne člene Zakona o elektronskih komunikacijah⁴². Pri tem je Ustavno sodišče ukrep obvezne hrambe podatkov prepoznalo kot nesorazmeren prav zato, ker neselektivna in vnaprejšnja hramba prometnih podatkov nujno v prevladujočem delu pomenila poseg v pravice tistega dela populacije, ki ni imela nobene povezave z nameni hrambe takšnih podatkov in to ni bilo ustrezno sorazmerno zamejeno.

Vsena navedenega se zelo dobro zavedamo, zato smo to dejstvo pri vzpostavitvi sorazmernosti imeli ves čas v mislih z zagotovitvijo enakovrednih protiuteži oziroma učinkovitih varovalk, s katerimi smo v nadaljevanju zamejili tovrsten poseg v človekove pravice le na nujno potrebno za dosego našega ustavno dopustnega cilja. Kot pomembna protiutež posegu v informacijsko zasebnost potnikov z neselektivnim zbiranjem in hrambo podatkov o potnikih je prav gotovo selektivna oziroma usmerjena uporaba teh podatkov. V tej luči podatkovna zbirka PNR ne bo, za razliko od hrambe in uporabe prometnih podatkov elektronskih komunikacij, predstavljala zgolj preventivno (vnaprejšnjo) in nediskriminatorno zbiranje ter uporabo podatkov o potnikih v letalskem prometu, temveč gre v osnovi za njihovo sprotno preverjanje skozi transparentna in nediskriminatorna ocenjevalna merila ter ustrezne podatkovne policijske zbirke, ter na tej podlagi za »uparjanje« oseb, prvič z namenom odkritja neznanih (potencialnih) storilcev le terorističnih in drugih hudih kataloško določenih kaznivih dejanj, ter drugič z namenom odkritja drugih oseb, zoper katere so razpisani zakoniti ukrepi, s katerimi organi odkrivanja in pregona merijo na kazenski pregon storilcev kaznivih dejanj. Pri tej avtomatski obdelavi podatkov se bodo operaterjem prikazali zgolj podatki o potnikih, ki se bodo ujemali z navedenimi merili. Obdelava/uporaba podatkov PNR je s tem po našem mnenju selektivno omejena na jasn namen, ki ga želimo s tem pristopom doseči z osredotočanjem zgolj na »rizične« posameznike izmed celotne populacije letalskih potnikov. S tem ta ukrep neposredno ne posega v pretežni meri v pravice državljanov, ki z namenom zbiranja podatkov nimajo nobene zveze. Nasprotno, državljanom bi ta selektivni in usmerjen pristop policistov, poleg višje stopnje varnosti, zmanjšal možnosti pretiranih posegov v TČPS potnikov, omogočal pa tudi nemoteno koriščenje svobode do prostega pretoka oseb na Schengenskem območju, ter hitrejša postopka mejne kontrole na letališčih. Kot prav tako pomembna protiutež velja omeniti še naš predlog v nadaljevanju tega dokumenta za sprejetje nacionalne zakonske podlage za pridobitev, hrambo,

42 Urad. list RS, št. 109/12 in 110/13 (ZEKom-1), členi 162, 163, 163.1, 164, 165, 166, 167, 168, 169.

analizo in izmenjavo podatkov o potnikih, s klavzulo o časovni omejitvi (»sunset clause«). To pomeni, da bi po preteku 5 - letnega obdobja zakonodaja prenehala veljati, razen v primeru, da bi se s poglobljeno analizo izkazalo, da gre za učinkovit pristop policije v boju zoper terorizem in druge hujše oblike kaznivih dejanj.

V naslednjem podpoglavju izpostavljamo še več ključnih značilnosti tega usmerjenega pristopa policije z uporabo podatkov o potnikih, s katerimi smo uravnotežili neselektiven način zbiranja in hrambe podatkov.

2.4.3 Proces obdelave in uporabe podatkov

Splošno o usmerjenem pristopu policije

- podatki PNR se bodo obdelovali le za ožji del populacije ljudi – za potnike v letalskem prometu,
- pri avtomatski obdelavi podatkov PNR se bodo prikazali le podatki o potnikih (t.i. zadetki), ki se bodo ujemali z nediskriminatornimi in transparentnimi ocenjevalnimi merili in zoper katere bodo razpisani ukrepi v ustreznih podatkovnih policijskih zbirkah, ki so namenjena za preprečevanje, odkrivanje, preiskovanje in pregon hudih kaznivih dejanj, ali bodo zanje napisane operativne informacije, povezane z istovrstnimi kaznivimi dejanji.
- zagotovljena bo natančna sledljivost uporabe podatkov PNR za točno določen namen,
- obstaja konkretna selektivna povezava med podatki PNR in hudimi kaznivimi dejanji (potovalni modusi, ukrepi zoper osebe).

Zbiranje in prenos podatkov

- zbiranje podatkov PNR se bo izvajalo za mednarodne komercialne lete iz tretjih držav na ali preko ozemlja Slovenije oziroma obratno, za čarterske polete ter za lete znotraj EU,
- zbiranje podatkov se bo izvajalo od letalskih prevoznikov, ki svojo prevozno dejavnost opravljajo na ali preko ozemlja R Slovenije,
- prenos podatkov iz sistema letalskega prevoznika do SI specializirane enote za informacije o potnikih bo potekala po metodi »push⁴³«, v skladu s katero letalski prevozniki pošljejo zahtevane podatke PNR in tako lahko tudi sami ohranijo nadzor nad tem, katere podatke zagotavljajo,
- za konkreten let se bodo podatki PNR pošiljali dvakrat, in sicer 24 ur pred načrtovanim odhodom leta in neposredno po zaprtju leta, to je takrat, ko se potniki vkrcajo na letalo v pripravi na odhod in se nadaljnji potniki ne morejo več vkrcati.

43 Kar pomeni, da DC ne bodo imele nenehnega, samoumevnega in neomejenega dostopa do PNR podatkovnih baz s strani letalskih prevoznikov. Za te podatke bodo namreč morale v nasprotju z metodo »pull« zaprositi prevoznika, slednji pa nato te podatke pošlje pristojnemu organu. (Povzeto po obvestilu oddelka Migracij in notranjih zadev Evropske komisije, http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/passenger-name-record/index_en.htm). Pravno podlago za ta pristop pa določa 1. odstavek 6. člena Predloga Direktive PNR.

Predmet obdelave:

- bodo podatki iz evidenc podatkov o potnikih, kot jih zbirajo letalski prevozniki v sistemu rezervacij letalskih kart in sistemu vzletne kontrole, in sicer v mednarodno priznanem PNR.GOV.XML in Edifact PAXLST formatu,
- posredovanje teh podatkov bo izvedeno po metodi »push«, in sicer bo potekalo po HTTPS protokolu, kot nadomestek temu pa bo za letalske prevoznike na voljo tudi MQ protokol,
- nabor podatkov PNR bo omejen le na manj občutljive podatke, izključujoč podatke, povezane z zdravstvenim stanjem in prehrano

Specializirana policijska enota za zbiranje in obdelavo podatkov

- pristojna policijska enota bo Oddelek za ocenjevanje varnostnih tveganj v Centru za kriminalistično obveščevalno dejavnost v Upravi kriminalistične policije na Generalni policijski upravi, ki bo deloval kot specializirana nacionalna SI enota za informacije o potnikih,
- pristojnost te enote bo pridobivanje, hramba, analiza in posredovanje teh podatkov ali rezultatov njihove analize pristojnim subjektom.

Pristojni organi za prejem podatkov

- SI enota za informacije o potnikih bo podatke PNR v skladu s sprejeto zakonodajo posredovala le vnaprej določenim upravičencem. Med te pristojne subjekte bodo spadali varnostno obveščevalni subjekti, ki imajo pooblastila na področju preprečevanja, odkrivanja, preiskovanja ali pregona terorističnih in hudih kaznivih dejanj in sicer:
 - organizacijske enote oziroma notranje organizacijske enote policije, ki izvajajo naloge preprečevanja, odkrivanja in preiskovanja terorističnih in drugih hujših kaznivih dejanj,
 - državni organi odkrivanja in kazenskega pregona, ki so pristojni za odkrivanje in pregon tovrstnih kaznivih dejanj,
 - varnostno obveščevalne službe v okviru odkrivanja terorističnih in hudih kaznivih dejanj,
 - specializirane enote za informacije o potnikih (PIU) v drugih državah članicah,
 - evropske agencije, mednarodne organizacije, katerih članica je R Slovenija in drugi tuji varnostni organi, ki so pristojni za kazenski pregon storilcev tovrstnih kaznivih dejanj.
- podatkov PNR se ne bo posredovalo pravnim osebam zasebnega prava, tako v državah članicah, kot tudi ne v tretjih državah.

Posredovanje podatkov drugim organom

- SI enota za informacije o potnikih bo za osebe, za katere se na podlagi ocene ugotovi, da bi lahko sodelovale pri terorističnem in hudem kaznivem dejanju, poslala podatke PNR ali rezultate njihove obdelave pristojnemu nacionalnemu organu za ukrepanje ali enotam za informacije o potnikih drugih (PIU) v drugih državah članicah, če meni, da je takšen prenos potreben zaradi preprečevanja, odkrivanja, preiskovanja ali pregona takšnih kaznivih dejanj,
- za odzivanje v vsakem posameznem primeru bo SI enota za informacije o potnikih na ustrezno obrazloženo pisno zaprosilo upravičencem posredovala le tiste nujno potrebne podatkovne elemente PNR ali rezultate njihove analize v posameznih utemeljenih primerih zaradi preprečevanja, odkrivanja, preiskovanja in pregona konkretnega terorističnega ali hudega kaznivega dejanja,
- tretjim državam se bodo podatki PNR lahko pošiljali v posameznih utemeljenih primerih le, če bodo izpolnjeni vsaj takšni standardi glede varstva osebnih podatkov, kot so določeni s slovensko nacionalno zakonodajo. Tovrstno sodelovanje se bo urejalo v okviru posamičnih sporazumov oziroma dogovorov,

Namen obdelave podatkov:

- obdelava podatkov bo omejena na preprečevanja, odkrivanje, preiskovanje ali pregon terorističnih in drugih hudih kaznivih dejanj, ki so opredeljena v Okvirnem sklepu Sveta 2002/475/PNZ z dne 13. junija 2002 o boju proti terorizmu in v Okvirnem sklepu sveta 2008/919/PNZ z dne 28. novembra 2008 o spremembi Okvirnega sklepa 2002/475/PNZ o boju proti terorizmu, ter v Okvirnem sklepu Sveta 2002/584/PNZ z dne 13. 6. 2002 o evropskem nalogu za prijetje in postopkih predaje med državami članicami, spremenjen z Okvirnim sklepom Sveta 2009/299/PNZ, z dne 26. 2. 2009,
- za odkritje in prijetje storilcev in sotorilcev navedenih kaznivih dejanj,
- za razkritje kriminalnih mrež in povezave med njihovimi člani,
- za dokazovanje krivde za storitev navedenih kaznivih dejanj.

Omejitev na huda kazniva dejanja

Nujno potrebno je, da je poseg v informacijsko zasebnost posameznika v razumnem ravnovesju do javne koristi v obliki večje stopnje varnosti, ki jo bomo v našem primeru lahko zagotavljali z obdelavo/uporabo podatkov PNR. Za zagotovitev tega ravnovesja je prav gotovo pomembna tudi omejitev uporabe teh podatkov na določena huda kazniva dejanja. V evropskem pravnem redu namreč že obstaja seznam takšnih kaznivih dejanj, za katera je strokovna javnost ocenila, da zaradi njihove teže lahko organi odkrivanja oziroma kazenskega pregona upravičeno posegajo v pravico do svobode posameznika. Gre za seznam hudih kaznivih dejanj iz Okvirnega sklepa Sveta o evropskem nalogu za prijetje in postopkih predaje med državami članicami, ki so razlog za predajo osebe na podlagi evropskega naloga za prijetje. Ocenjujemo, da bi za veliko večino teh hudih kaznivih dejanj dejansko lahko uporabljali tudi podatke PNR. Pri podrobnem pregledu navedenega seznama smo ugotovili, da so med temi kaznivimi dejanji tudi nekatera takšna, ki ne

predstavljajo takšnih varnostnih groženj, da bi lahko v našem primeru upravičeno lahko govorili o razumnem ravnovesju do javne koristi. Takšna kazniva dejanja so npr. 1. goljufige, vključno s tistimi, ki ogrožajo finančne interese Evropske unije, 2. ponarejanje industrijskih izdelkov in prodaja takih izdelkov, 3. kazniva dejanja storjena zoper okolje, prostor in naravne dobrine, vključno z nedovoljeno trgovino z ogroženimi živalskimi in rastlinskimi vrstami, 4. nedovoljena trgovina s hormonskimi snovmi in drugimi spodbujevalci rasti, 5. nedovoljena trgovina s kulturnimi dobrinami, vključno s starinami in umetniškimi deli, 6. trgovina z ukradenimi vozili, ter 7. požig. Izključujoč ta kazniva dejanja tako dobimo seznam tistih hudih kaznivih dejanj, ki predstavljajo hujšo varnostno grožnjo javni, nacionalni ali mednarodni varnosti in zato predstavljajo tiste ustavnopravne izjeme, pri katerih je državni oblasti dovoljen poseg v informacijsko zasebnost. Prav tako imajo ta kazniva dejanja mednarodni element, kar pomeni, da gre za huda mednarodna kazniva dejanja, kot so definirana v Konvenciji združenih narodov proti mednarodnemu organiziranemu kriminalu Uradni list RS, št. 41/2004 z dne 22.4.2004. V tej konvenciji »hudo kaznivo dejanje« pomeni kaznivo dejanje, ki se kaznuje najmanj s štirimi leti zapor ali strožjo kaznijo. Kaznivo dejanje mednarodne narave po tej konvenciji pa je, če:

- (a) je storjeno v več kot eni državi,
- (b) je storjeno v eni državi, vendar se precejšen del priprav, načrtovanja, vodenja ali usmerjanja odvija v drugi državi,
- (c) je storjeno v eni državi in je vanj vpletena organizirana kriminalna združba, ki se ukvarja s kriminalnimi dejavnostmi v več kot eni državi,
- (d) je storjeno v eni državi, vendar ima precejšnje posledice v drugi državi.

Ta huda mednarodna kazniva dejanja so tako naslednja:

- pripadnost kriminalni združbi,
- terorizem,
- trgovina z ljudmi,
- spolno izkoriščanje otrok in otroška pornografija,
- nedovoljena trgovina s prepovedanimi drogami,
- nedovoljena trgovina z orožjem, strelivom in eksplozivi,
- korupcija,
- pranje denarja,
- ponarejanje denarja, vključno z evrom,
- kazniva dejanja, storjena z uporabo računalnika,
- omogočanje prepovedanega prehoda čez državno mejo in bivanja v državi,
- umor in povzročitev hudih telesnih poškodb,
- nedovoljena trgovina s človeškimi organi in tkivi,

- ugrabitev, protipraven odvzem prostosti, jemanje talcev,
- rasizem in ksenofobija,
- rop v skupini ali oborožen rop,
- izsiljevanje v skupini ali z uporabo orožja ali nevarnega orodja,
- ponarejanje in promet z uradnimi dokumenti,
- ponarejanje različnih oblik plačilnih sredstev,
- nedovoljena trgovina z jedrskimi in radioaktivnimi snovmi,
- posilstvo,
- kazniva dejanja, za katera je pristojno Mednarodno kazensko sodišče,
- ugrabitev letala ali ladje in
- sabotaža.

Načini preverjanja podatkov

- avtomatizirano preverjanje povezanih podatkov API in PNR se bo izvajalo skozi ustrezne nacionalne podatkovne evidence, vključno z mednarodnimi, ki so ali če bodo vzpostavljene na podlagi nacionalnega, mednarodnega ali prava EU, in sicer o iskanih osebah, ali o osebah zoper katere so razpisani zakoniti ukrepi ali so za osebe napisane operativne informacije, povezane s terorističnimi ali drugimi hujšimi kaznivimi dejanji,
- avtomatizirano preverjanje podatkov o potnikih skozi nediskriminatorna ocenjevalna merila, oblikovana na podlagi ocen tveganj, izdelanih v povezavi z odkrivanjem in preiskovanjem terorističnih in drugih hudih kaznivih dejanj,
- ročno preverjanje avtomatiziranih zadetkov skozi vse razpoložljive in javno dostopne informacijske vire, z namenom ugotovitve dejanske stopnje tveganja oziroma aktualnosti zadetka; izločanje t.i. »lažnih zadetkov«.

Načini uporabe podatkov

- reaktivna in sprotna uporaba podatkov bo organom odkrivanja v okviru tekočih kriminalističnih preiskav omogočala uspešnejše preprečevanje in odkrivanje tistih kaznivih dejanj, ki se pripravljajo oziroma se že izvajajo, ter odkrivanje storilcev in sotorilcev kaznivih dejanj ter pri dokazovanju njihovega kriminalnega povezovanja in krivde (*zbiranje dokazov, identifikacija ter povezovanje storilcev in kriminalnih združb*), pri čemer se bodo podatki preverjali skozi ustrezne podatkovne zbirke,
- proaktivna uporaba podatkov bo organom odkrivanja omogočila možnost analize podatkov z namenom oblikovanja relevantnih ocenjevalnih meril (*posodabljanje starih ali oblikovanje novih meril*), ki se jih bo uporabljalo za ocenjevanje podatkov o potnikih pred prihodom ali odhodom z namenom preprečitve, odkritja ali preiskave terorističnih ali drugih hudih kaznivih dejanj in prijetja njihovih storilcev.

Uporaba ocenjevalnih meril

- ocenjevalna merila se bodo oblikovala na podlagi ocen tveganj, izdelanih v povezavi z odkrivanjem in preiskovanjem terorističnih in drugih hudih kaznivih dejanj,
- uporabljala se bodo pri sprotnem in proaktivnem načinu uporabe podatkov PNR,
- z vnaprej transparentno določenimi ocenjevalnimi merili bo mogoče ugotavljali identiteto oseb, kater še niso bile prepoznane kot storilci navedenih kaznivih dejanj, vendar pa bodo analize podatkov PNR izkazovale, veliko verjetnost njihove soudeležbe pri takšnih kaznivih dejanjih. Tak razvid bo pristojnim organom narekoval podrobnejšo obravnavo, oziroma ukrepanje,
- ta merila ne bodo diskriminatorna; ne bodo posredno, niti neposredno temeljila na rasnem ali etničnem poreklu osebe, njenem verskem, filozofskem ali političnem prepričanju, članstvu v sindikatu, zdravstvenem stanju ali spolnem življenju,
- pristojni organ oziroma enota ne bo smela sprejemati odločitev, ki bi imela negativne pravne učinke na posameznika ali bi nanj pomembneje vplivale, le na podlagi avtomatizirane obdelave⁴⁴ podatkov PNR. Vsakršno avtomatizirano ujemanje podatkov bo SI enota za informacije o potnikih dodatno, selektivno preverjala,
- uporaba podatkov PNR bo osredotočena le na storilce dotičnih kaznivih dejanj, oziroma tiste osebe, ki na podlagi analize podatkov predstavljajo višjo stopnjo tveganja za javno varnost in varnost ljudi. Preostalim potnikom bi ta selektivni sistem le še povišal kvaliteto stopnja varnosti in koriščenja svoboščine do prostega pretoka oseb na Schengenskem območju.

Zagotavljanje pravic letalskim potnikom

- potniki bodo na ustrezen način⁴⁵ obveščeni, da bodo njihovi osebni podatki predmet obdelave s strani varnostnih organov. Eden od možnih in pogostih načinov obveščanja potnikov je preko spletne strani letalskih prevoznikov in Policije. Obveščeni bodo o namenu obdelave podatkov, o policijski enoti, ki bo podatke za določen namen obdelovala, o pravni podlagi za obdelavo podatkov in o pravnem varstvu,
- potnikom bodo pripadale določene pravice v upravnih in sodnih postopkih s tem, da bodo imeli pravico do dostopa do svojih podatkov PNR, ter v določenih primerih tudi do njihovega popravka in izbrisa. Pravica do upravnega in sodnega varstva podatkov pripada potnikom v primeru kršitve njegove zasebnosti ali predpisov, ki urejajo varstvo podatkov, in sicer jim mora biti zagotovljena nediskriminatorna obravnava.

Varstvo in hramba osebnih podatkov

- podatki bodo zaščiteni pred zlorabo in nepooblaščenim dostopom z ustreznimi tehničnimi varnostnimi postopki in ukrepi, usmerjeni v zagotavljanje visoke stopnje varnosti, zaupnosti in celovitosti podatkov PNR. Vzpostavljena je tudi že možnost nadzora s strani državnega organa, pristojnega za varstvo podatkov,

44 Člen 122 ZNPPol (avtomatizirana obdelava osebnih in drugih podatkov)

45 O načinu obveščanja potnikov se bomo dogovorili z letalskimi prevozniki.

- prenos, hramba, analiza in izmenjava podatkov se bo izvajalo v okviru strogih jamstev in na visoki ravni varstva osebnih podatkov, urejeno z že obstoječo nacionalno zakonodajo, ki ureja to področje (*Zakon o varstvu osebnih podatkov*), v cilju zagotavljanja zaščite letalskih prevoznikov, kot tudi njihovih potnikov,
- sistem SI PNR bo zagotavljal transparentnost obdelave podatkov PNR z avtomatiziranim beleženjem zgodovine popolnoma vseh aktivnosti, tako avtomatizirane obdelave podatkov z ujemanji v ocenjevalnih merilih in določenih podatkovnih bazah, kot tudi vseh izvedenih aktivnosti operaterjev v SI enoti za informacije o potnikih, vključno z avtorizacijo dostopov v sistem. Operaterji pa bodo po zaključku svojega dela vse izvedene aktivnosti zabeležili v dnevnem poročilu o delu, vključno z informacijami katere podatke so posredovali v uporabo, komu in za kakšen namen,
- za zagotovitev visokega standarda varstva podatkov pri hrambi, obdelavi in izmenjavi podatkov, urad Informacijskega pooblaščenca RS sodeluje v nacionalnem projektu SI PNR kot pridružen partner v projektu,
- hramba podatkov o potnikih PNR in API, bi se v ločenih samostojnih evidencah izvajala 12 mesecev od njihovega prvega posredovanja. Po izteku tega obdobja, bi se podatki API in PNR hranili v samostojni evidenci še nadaljnjih 18 mesecev. V tem obdobju bi bili podatki maskirani z zakrivanjem določenih podatkovnih elementov. Dostop do popolnih podatkov bi bil možen le v posamičnih primerih pod zelo strogimi pogoji, in sicer le za namen zagotavljanja dokazov v predkazenskem oziroma kazenskem postopku. O upravičenosti tovrstnih argumentiranih zaprosil bi odločal predstojnik SI enote za informacije o potnikih. Po preteku 30 mesečnega obdobja od prvega posredovanja podatkov API in PNR, bi se ti podatki iz evidence samodejno dokončno izbrisali,
- neposreden dostop do evidence podatkov o potnikih bodo imeli le uslužbenci SI enote za informacije o potnikih,
- rezultati obdelave podatkov o posameznih potnikih se bodo hranili toliko časa, kolikor časa bo mogoča identifikacija oseb v okviru celotnega obdobja hrambe podatkov, s čimer se bomo lahko izognili tudi napačnim oziroma lažnim zadetkom.

Dejstvo je, da mora biti rok hrambe podatkov v luči preizkusa sorazmernosti ustrezno utemeljen. Vsekakor mora biti omejen z namenom uporabe podatkov na eni strani, ter na drugi strani z doseganjem ustavno dopustnega cilja. Čas hrambe podatkov bo vsekakor bistveno vplival na natančnost oblikovanih ocenjevalnih meril in s tem povezanim zmanjšanjem števila napačnih zadetkov (False positives). To pomeni, da daljši kot bo čas hrambe podatkov (Data Retention), natančneje bo mogoče izdelati usmerjena ocenjevalna merila. Z daljšim časom je namreč mogoče pridobiti ustrezno velik, reprezentativen vzorec določenih podatkov, zaradi česar bo prognoza stopnje tveganja natančnejša in tudi bolj ciljno usmerjena v ožjo specifično skupino ljudi, namesto v širšo množico potnikov.

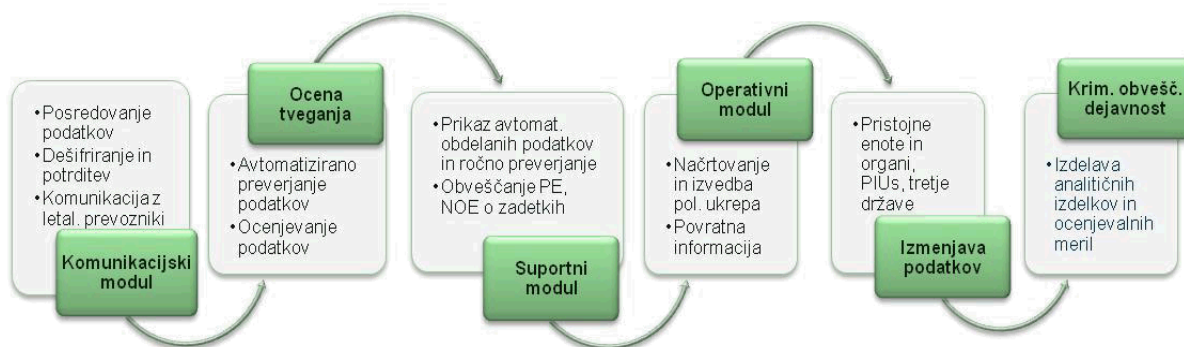
2.4.4 Delovni proces pri obdelavi podatkov

Delovni proces v SI enoti za informacije o potnikih bo potekal predvidoma po urniku 24/7, v okvirih spodaj prikazanih faz. Konceptualno bo vsebinski delovni proces temeljil na kriminalističnoobveščevalni dejavnosti. Za obdelavo bodo zagotovljena najstrožja jamstva varovanja osebnih podatkov. Načela zakonitosti, nediskriminacije potnikov in varovanje njihovih TČPS, bodo temeljna vodila procesa obdelave PNR podatkov.

Sistem SI PNR bo imel vgrajena ustrezna varovala nadzora nad spoštovanjem zakonitosti. Zaradi učinkovite izgradnje objektivnih ocenjevalnih meril, bo zagotovljena avtomatizacija hranjenja zapisov vseh izvedenih aktivnosti operaterja skozi celoten delovni proces. Nekoliko podrobneje je sistem varovalk opisan v 4. poglavju upravljanje s tveganji.

Na že pojasnjen način bodo operaterji avtomatizirani zadetke sistematsko ročno preverjali in na podlagi izsledkov nato zoper posameznike, na podlagi ZNPPol organizirali izvedbo ustreznih ukrepov oziroma policijskih aktivnosti. Delovni proces zato v osnovi delimo na avtomatiziran in neavtomatiziran del, glede na izvajane aktivnosti pa ga delimo na šest med seboj povezanih faz (glej sliko 2), ki kot zaključena celota predstavljajo temelj kriminalistično obveščevalne dejavnosti (3-i model). Prikazana faza ocenjevanja letalskih potnikov omogoča interpretacijo (INTERPRET) kriminalnega okolja, pri čemer se na podlagi ocenjevalnih meril in razpisanih ukrepov policije izpostavi osebe, ki bi lahko pomenile potencialno varnostno grožnjo javni varnosti ter varnosti oseb in premoženju. Z opozarjanjem na takšne osebe (INFLUENCE) se nato delo pristojnih policijskih enot ciljno osredotoči nanje z izvedbo ustreznih ukrepov oziroma aktivnosti policije (IMPACT).

Slika 2: Faze delovnega procesa pri obdelavi in uporabi podatkov PNR



1. faza: prenos podatkov

Letalski prevoznik bo po varnem informacijskem kanalu posredoval podatke PNR v informacijski sistem SI PNR v predpisani obliki, in sicer 24/48 ur pred letom in ob zaprtju leta, tik pred poletom, ko bo letalski prevoznik posredoval tudi podatke API iz njihovega sistema vzletne kontrole. Sprejeti podatki se bodo avtomatizirano dešifrirali v berljiv zapis, ki bo prav tako avtomatizirano prebran zaradi kontrole kakovosti podatkov. O prejemu podatkov in njihovi kvaliteti bo sistem avtomatsko obveščal pošiljatelja v obliki povratnega sporočila. Nadaljnja povezava API in PNR podatkov v informacijskem sistemu SI PNR bosta omogočali neposredno in popolno identifikacijo osebe in njihovo prisotnost na letu. Ta sistem bo ob transformirani

obliki, ohranil tudi izvorno obliko podatkov. S tem se bo prva avtomatizirana faza delovnega procesa zaključila.

2. faza: avtomatizirano ocenjevanje podatkov

Vnaprej transparentno oblikovana ocenjevalna merila bodo avtomatično filtrirala možne zadetke. Avtomatizirana ocena podatkov PNR bo izvedena tudi s primerjanjem skozi zgodovino PNR, ter s poizvedbami skozi nacionalne in mednarodne uradne podatkovne evidence iskanih oseb, ter drugih oseb, zoper katere so razpisani zakoniti ukrepi ali operativne informacije za potrebe preprečevanja, odkrivanja in kazenskega pregona terorističnih in drugih hudih kaznivih dejanj (FIO, SIS II, Interpol baza iskanih oseb, Europolov EIS).

3. faza: prikaz ujemanja avtomatiziranega preverjanja podatkov, njihovo ročno preverjanje in obveščanje upravičenih uporabnikov storitve

Osnovna naloga operaterja bo nadzor in spremljanje procesa izpisanih zadetkov ter njihovo ustrezno ovrednotenje. Ta način omogoča selektivno identifikacijo zgolj varnostno zanimivih oseb za teroristična in druga huda kazniva dejanja. Ilustrativno se bo operaterju na računalniški delovni površini PNR sistema prikazali zgolj uparjeni zadetki v obliki tabelaričnega – »na klik« drevesnega prikaza. Prepoznavno se bodo ločevali med seboj glede na vrsto zadetka oziroma druge s tem povezane specifične lastnosti. Vsak zadek bo vseboval osnovne informacije: številko leta, št. rezervacije, datum in ura leta, ime in priimek osebe, ukrep in odstotek njegove zanesljivosti. Operater bo zadetke po ročnem preverjanju potrdil ali izločil kot t.i. lažne ali neprave zadetke. Potrjeni zadetki bodo pred prihodom, oziroma odhodom ključnega letala posredovani policistom, ki bodo izvajali mejno kontrolo pri teh osebah (npr. PLP Brnik) in v določenih primerih tudi pristojni kriminalistični enoti na državnem ali regionalnem nivoju policije. Tako pridobljena pravočasna in popolnoma obdelana informacija bo za uspešnost policije najpomembnejši dejavnik.

4. faza: načrtovanje in izvedba operativnih aktivnosti in poročanje

S podano informacijo bo neposredno policijsko delo osredotočeno ciljno, zgolj v operativno zanimivo osebo, zoper katero bo razpisan zakonit ukrep ali bodo na podlagi rezultatov analize podatkov PNR predstavljala višjo stopnjo tveganja za varnost. O vseh izvedenih aktivnostih in ukrepih, ki jih bodo nato policisti izvedli, bodo pisno poročali v informacijski sistem SI PNR, kar bo omogočalo oblikovanje natančnih ocenjevalnih meril. Po izkazani potrebi bo operater nastopil tudi kot koordinator policijskih aktivnosti v primerih, ko bo v posamezni zadevi udeleženih več policistov iz različnih enot.

5. faza: izmenjava podatkov PNR

SI enota za informacije o potnikih bo podatke PNR lahko posredovala vnaprej določenim upravičencem, kar smo podrobno predstavili že v prejšnjem podpoglavju.

6. faza: kriminalističnoobveščevalna dejavnost

Izdelava in izmenjava kriminalistično obveščevalnih informacij o kriminalni dejavnosti oseb, za katere se bo z analizo operativnih podatkov ugotovilo, da pomenijo konkretno grožnjo zoper javno varnost, varnost oseb in premoženja in bodo zato terjala prioritarno obravnavo policije.

Operater bo sprotno sodeloval z operativnimi analitiki v isti enoti. Osnovna naloga slednjih bo izdelava operativnih informacij in kriminalistično obveščevalnih izdelkov, predvsem na podlagi ugotovitev in aktualnih informacij, ki bodo pridobljene v okviru delovanja enote. Pri analitični obdelavi podatkov in informacij bo skrbel tudi za sprotno posodabljanje ali oblikovanje novih meril za izvajanje ocenjevanja podatkov o potnikih, pri čemer bo strateškemu analitiku posredoval predloge za oblikovanje le-teh. Strateški analitik v enoti bo imel sistemsko-strateško vlogo in bo v enoti skrbel za izvedbo nalog s področja razvoja dejavnosti in strateške analitike. Na področju razvoja dejavnosti bo sodeloval pri organizacijskem, sistemskem in normativnem razvoju PNR področja, skrbel za sodelovanje z letalskimi prevozniki in za mednarodno sodelovanje s tujimi varnostnimi organi in mednarodnimi organizacijami iz področja dela enote. Na strateškem nivoju bo skrbel za pripravo ocen ogroženosti, drugih varnostnih in strateških analiz z namenom določanja prioritet dela policije, obveščanja o relevantnih pojavih in trendih in oblikovanja ter posodabljanja ocenjevalnih meril za potrebe ocenjevanja podatkov o potnikih.

3 ANALIZA TVEGANJ V ZVEZI S POSEGI V USTAVNE PRAVICE

V pravni državi je vloga policije tako pomembna, da je mogoče stanje demokracije prepoznati že ob pogledu na njeno učinkovito delovanje. Bistvo pravne države je, ne le v kvantiteti, temveč tudi v kvaliteti storitev. V tem kontekstu postaja sodobna policijska dejavnost zelo kompleksen proces, zato ne more potekati ločeno in neodvisno od splošnega družbenega razvoja. Njena vloga se namreč spreminja iz “dejavnosti za državo” v “dejavnost za skupnost”. Vključitev storitvene funkcije policijo spreminja iz pretežno represivnega v pretežno storitveni in proaktivno usmerjen organ. Slednja oblika je eden od gradnikov sodobnega pristopa opravljanja policijske dejavnosti. Navkljub vse bolj odprtemu pristopu pa policija ne sme pozabiti na svoje temeljne varnostne naloge, ki so povezane tudi z njeno represivno vlogo v varnostnem državnem aparatu.

Ob kakršnem koli uvajanju novih policijskih pooblastil oziroma ob širitvi teh pooblastil je potrebno skozi presojo njihovega vpliva na zasebnost, identificirati tudi vsa možna tveganja. Le na tak način lahko celovito in pravočasno predvidimo ustrezne možnosti upravljanja s posameznimi tveganji in jih s tem bistveno zmanjšamo na raven primernosti, nujnosti in sorazmernosti.

3.1 SWOT analiza za podatke PNR

Za uresničitev naših razvojnih ciljev je pomembno prepoznati prednosti / slabosti / priložnosti / nevarnosti, ki jih lahko pričakujemo pri implementaciji sistema SI PNR za obdelavo oz. uporabo podatkov PNR. Prav SWOT analiza nam omogoča v nadaljevanju lažjo izvedbo sorazmernostnega testa. S prepoznavanjem prednosti, priložnosti, pomanjkljivosti in nevarnosti našega pristopa lahko zelo hitro ugotovimo ali so naše aktivnosti pretežno nagnjene k negativnim izidom ali k pozitivnim izidom. S tem si ustvarimo osnovo, na podlagi katere vsekakor lahko odpravljamo slabosti tako, da izkoristimo priložnosti, s prednostmi pa dejansko premagujemo nevarnosti. Večino dejavnikov smo pojasnili že skozi celotno vsebino, zato smo jih v tem poglavju sistematično strnili.

3.1.1 Priložnosti

- celovitejše in učinkovitejše zaznavanje hujših oblik kriminalitete,
- dvig kriminalistično obveščevalne strokovnosti in učinkovitosti,
- uporaba sodobnih informacijskih tehnologij pri izvajanju kriminalistično obveščevalne dejavnosti,
- okrepitev kriminalistično obveščevalne dejavnosti,
- uvajanje novih sodobnih metod in taktik dela policije pri preprečevanju, odkrivanju, preiskovanju terorističnih in drugih hujših oblik kaznivih dejanj,
- pridobivanje novih znanj in izkušenj.

3.1.2 Prednosti

- sistematično osredotočanje na storilce hujših kaznivih dejanj oziroma na iskane osebe pri izvajanju mejne kontrole,
- zagotavljanje enakosti obravnave potnikov pri mejni kontroli,
- zagotavljanje dodatnega podatkovnega vira pri preiskovanju, odkrivanju hujših kaznivih dejanj in odkrivanju ter pregonu njihovih storilcev,
- zagotavljanje dodatnih dokazov za obdolžence oz. obtožence v kazenskem postopku,
- bolj okrepljeno operativno sodelovanje in izmenjava podatkov ter kriminalistično obveščevalnih informacij s tujimi varnostnimi organi kazenskega pregona,
- zagotavljanje učinkovitega in usklajenega sodelovanja s pristojnimi državnimi organi, zasebno-varnostnimi subjekti na letališču.

3.1.3 Nevarnosti

Osební podatki pomenijo občutljive podatke, katerih zloraba ima lahko za posameznika negativne učinke. Prav zaradi tega so ti podatki v slovenski zakonodaji⁴⁶ ustrezno zaščiteni pred morebitnimi neupravičenimi posegi, pri čemer so kršitve glede na intenziteto posega v zasebnost določene kot prekrški in kot kazniva dejanja, in sicer:

- zbiranje oziroma obdelovanje osebnih podatkov v neskladju z Zakonom o varstvu osebnih podatkov (*glej kazenske določbe ZVOP-1*),
- zloraba osebnih podatkov s posredovanjem ali uporabo osebnih podatkov v neskladju z zakonom (kaznivi dejanji Zloraba osebnih podatkov po 143. členu KZ-1 in Zloraba uradnega položaja ali uradnih pravic po 257. členu KZ-1),
- vdor ali nepooblaščen vstop v zaščitenó računalniško bazo podatkov s posredovanjem, kopiranjem ali prestrežanjem podatkov v sistemu (kazniva dejanja Zloraba osebnih podatkov po 143. členu KZ-1, Napad na informacijski sistem po 221. členu KZ-1 ter Izdelovanje in pridobivanje orožja in pripomočkov, namenjenih za kaznivo dejanje po 306. členu KZ-1),

46 Zakon o varstvu osebnih podatkov (ZVOP-1-UPB1), Uradni list RS, št. 94/2007, z dne 16. 10. 2007
in Kazenski zakonik (KZ-1-UPB2), Uradni list RS, št. 50/2012 z dne 29. 6. 2012.

- uničenje infrastrukture, informacijskega sistema (kaznivo dejanje Terorizem po 108. člen KZ-1),

3.2 Tveganja povezana z obdelavo podatkov PNR in upravljanje z njimi

Pri uvajanju novih policijskih pooblastil oziroma pri njihovi širitvi, kot je to v primeru obdelave/uporabe podatkov PNR, morajo biti posegi v človekove pravice, ki jih ta pooblastila predstavljajo, sorazmerno utemeljeni z ustavno dopustnim ciljem. Ta sorazmernost je še posebej pomembna pri posegih v človekove pravice, ki varujejo človekovo osebno dostojanstvo, varnost, osebnostne pravice in njegovo zasebnost. Orodje, s pomočjo katerega lahko to uravnoteženost dosežemo, nam predstavlja prav presoja vplivov na zasebnost, s pomočjo katerega zaznavamo posamezna tveganja, povezana z nezakonito oziroma prekomerno obdelavo osebnih podatkov. Na ta način lahko ta tveganja odpravimo ali ustrezno zmanjšamo na raven ustavno pravne dopustnosti. Na podlagi predhodno predstavljenih dejstev, okoliščin in stališč ter v skladu s smernicami IP RS zato v nadaljevanju predstavljamo identificirana tveganja, povezana s pridobivanjem, hrambo, analizo in posredovanjem teh podatkov ali rezultatov njihove analize pristojnim subjektom.

Oseba je v primerih zlorab lahko podvržena diskriminatornemu ravnanju, katero lahko bistveno poslabša njen pravni položaj v družbi. Še pomembnejše je dejstvo, da zloraba osebnih podatkov lahko posamezniku neposredno ogroža njegovo varnosti, saj oseba, katerih podatki so zlorabljeni, lahko postane celo tarča kriminala. Zato se mu lahko bistveno spremeni kvaliteta življenja. V tem cilju mora uporaba podatkov PNR temeljiti na nediskriminaciji potnikov in varovanju vseh njihovih TCPS, katere izhajajo iz mednarodno pravnih dokumentov. Temeljno osredotočanje je na zagotavljanju varstva informacijske zasebnosti in na varstvu osebnih podatkov posameznika. Za zagotavljanje visoke ravni varstva osebnih podatkov morajo biti določena stroga jamstva, tako pri sprejemu, hrambi, analizi in pri prenosu občutljivih podatkov. Slovenska zakonodaja ima to pravno področje urejeno na visokem nivoju, izvajanje česar s svojo nadzorno funkcijo zagotavlja Informacijski pooblaščenec RS.

V letu 2011 je EU Agencija za temeljne človekove pravice, v sodelovanju z Evropskim nadzornikom za zaščito podatkov, izdelala praktične usmeritve⁴⁷ za zagotavljanje visoke stopnje varstva osebnih podatkov pred prekomernimi ali nezakonitimi posegi v TSČP, kar bomo dosledno upoštevali pri upravljanju z identificiranimi tveganji.

3.2.1 Tveganja glede neustreznosti zakonodaje

Tveganje št. 1

Sprejetje neustrezne pravne podlage za pridobivanje, hrambo, analizo in posredovanje podatkov o potnikih (PNR, API).

Upravljanje s tveganjem:

Novodobni zgodovinski dogodki, povezani predvsem z najhujšimi terorističnimi napadi, so pokazali, da so države, kjer so bili ti napadi izvedeni, prehitro in nepremišljeno sprejeli vrsto

⁴⁷ Twelve operational fundamental rights considerations for law enforcement when processing Passenger Name Record (PNR) data.

protiterorističnih ukrepov, ki so prekomerno posegli v človekove pravice. Zaradi vse pogostejših terorističnih groženj je širša mednarodna skupnost začela razmišljati o odločnejšem, načrtnem in bolj sistematičnem boju zoper tovrstne varnostne grožnje, ki resno in neposredno ogrožajo mednarodno in nacionalno varnost. Temu primerna so tudi njihova prizadevanja za uvedbo novih učinkovitih ukrepov zoper takšne oblike groženj. To se trenutno dogaja tudi na EU ravni, kjer predlog EU PNR direktive še ni sprejet, zaradi nezadostne politične podpore. Prav zaradi tega smo se odločili, da pristopimo k pripravi predloga ustrezne nacionalne pravne podlage, ki bo na primeren in uravnotežen način določala pridobivanje podatkov o potnikih PNR in API, njihovo hrambo, analizo in uporabo za preprečevanje, odkrivanje, preiskovanje, ter pregon terorizma in drugih hujših oblik kriminalitete. S tem namenom, skladno s smernicami IP RS pripravljamo to presojo vplivov na zasebnost, ki jo sproti usklajujemo s tem avtonomnim in neodvisnim organom. Pri pripravi tega dokumenta sledimo metodologiji PIA, s ciljem izogniti se prekomernim posegom v pravico do zasebnosti posameznika. Poleg tega smo skupaj s predstavniki IP RS izvedli dva študijska obiska v Franciji in v Madžarski, kjer so v okviru EU PNR projekta že sprejeli ustrezno nacionalno podlago. V primeru teh dveh držav gre za dva različna skrajna primera pravnih podlag, izhajajoč iz skupne osnove (predlog EU PNR direktive) in izhajajoč iz istih standardov varstva osebnih podatkov. Na ta način bomo lahko bolj objektivno ocenili sorazmernost pri posegu v informacijsko zasebnost pri sprejetju lastne nacionalne zakonodaje.

Vsekakor bomo o učinkovitosti novega orodja policije z obdelavo/uporabo podatkov PNR objektivno lahko presojali šele na podlagi lastnih operativnih izkušenj uporabe teh podatkov. Prav v tem segmentu vidimo dodatno možnost systemskega varovanja pred neuravnoteženim trajnim posegom v človekove pravice. Zato po francoskem vzoru na področju zakonodaje predlagamo sprejetje nacionalne zakonske podlage za pridobitev, hrambo, analizo in izmenjavo podatkov o potnikih, s klavzulo o časovni omejitvi (»sunset clause«) le-te na 5 let. Po preteku tega obdobja bi zakonska podlaga prenehala veljati, razen v primeru, da bi se s poglobljeno analizo izkazalo, da gre za učinkovit pristop policije v boju zoper terorizem in druge hujše oblike kaznivih dejanj. V tem primeru bi zakonodajalec lahko sprejel podaljšanje predmetnih zakonskih določb.

Tveganje št. 2

Neusklajenost nacionalnih zakonodaj glede obdelave/uporabe podatkov o potnikih v državah članicah EU.

Upravljanje s tveganjem:

Dejstvo je, da predlog EU PNR direktive še ni dobil ustrezne politične podpore v EU Parlamentu, zato so države članice, ki so udeležene v tem evropskem projektu, že začele sprejemati lastne nacionalne zakonodaje za obdelavo/uporabo podatkov PNR. Zaradi različnih nacionalnih pravnih podlag, kar že lahko zaznamo na primeru Francije in Madžarske, bo v primeru mednarodnega policijskega sodelovanja na tem področju vsekakor prihajalo do zaprosil za izmenjavo podatkov o potnikih, ki v posamezni državi članici ne bodo pravno izvedljiva. Vsekakor menimo, da bi bila najboljša rešitev za to prav sprejem EU PNR direktive, ki bi v okviru evropskega pravnega reda omogočala državam članicam vzpostaviti učinkovite in

kompatibilne nacionalne PNR sisteme, ki bi obenem zagotavljali enotne standarde za varstvo osebnih podatkov. V primeru odsotnosti tega evropskega pravnega vira, pa bo SI enota za informacije o potnikih posredovala podatke v okviru zakona, ki ureja varstvo osebnih podatkov ter samo v primerih in na način, kot smo že predhodno predvideli (*glej prvi dve alineji v odstavku »Posredovanje podatkov drugim organom«, stran 37*).

Tveganje št. 3

Neustrezni standardi varstva osebnih podatkov s strani tretjih držav, ki bodo zaprošale za podatke o potnikih (PNR).

Upravljanje s tveganjem:

Evropska komisija je v okviru globalnega pristopa k prenosu podatkov iz evidence imen letalskih potnikov (PNR) za tretje države določila niz splošnih meril, ki bi bila podlaga za sklepanja dogovorov oziroma sporazumov o izmenjavi teh podatkov med državami članicami in tretjimi državami. S tem je določila splošne standarde, ki bi jih mednarodni sporazumi med EU in tretjimi državami morali upoštevati, da bi se dosegla čim večja skladnost v zvezi z jamstvi glede varstva podatkov v navedenih državah in postopki prenosa podatkov s strani letalskih prevoznikov. Določena so temeljna načela varstva osebnih podatkov, modalnost prenosa podatkov in drugi glavni koncepti, ki bi jih morala upoštevati tretja država.

Posredovanje podatkov o potnikih v tretje države se bo izvajalo v okviru strogih jamstev in na visoki ravni varstva osebnih podatkov, urejeno z že obstoječo nacionalno zakonodajo, ki ureja to področje, pri čemer bo SI enota za informacije o potnikih ravnala na način, kot smo predvideli (*glej tretjo alinejo v odstavku »Posredovanje podatkov drugim organom«, stran 37*).

3.2.2 Tveganja glede zbiranja podatkov

Tveganje št. 4

Obdelava podatkov o potnikih ne bi predstavljala učinkovitega usmerjenega pristopa policije v boju zoper hujše oblike kriminala.

Upravljanje s tveganjem:

V podpoglavju 2.1 smo iz različnih analitičnih poročil razbrali, da gre v primeru terorističnih in drugih hujših oblik kaznivih dejanj za mednarodno razsežne kriminalne aktivnosti, pri čemer so mednarodna potovanja storilcev teh kaznivih dejanj postali sestavni del našega vsakdana. Ti storilci so zaradi obsežnega mednarodnega prostora, prisiljeni potovati z letali zaradi časovno hitrejšega premagovanja daljših razdalj. Prav zaradi tega so se podatki PNR na podlagi tujih izkušenj na operativnem nivoju izkazali kot zelo uporaben informacijski vir pri preprečevanju in omejevanju tovrstne kriminalitete. Iz izkušenj držav članic, ki podatke PNR že uporabljajo za ta namen izhaja, da je z ustrezno analitično obdelavo ustreznega nabora podatkov PNR mogoče dovolj podrobno opredeliti specifične oziroma ponavljajoče potovalne vzorce teroristov in storilcev drugih hudih kaznivih dejanj. Ti vzorci so z vidika modusa operandi kriminalcev, predstavljali njihove zanimive odklone od običajnega vzorca večine potnikov. Temeljite analize podatkov bodo zato služile za oblikovanje nediskriminatornih ocenjevalnih meril, ki bodo na takšne storilce uspešno predhodno opozarjala in omogočala usmerjeno delovanje policije zgolj na

takšne osebe. Trenutno se lahko sklicujemo le na tuje izkušnje, samo primernost podatkov oziroma učinkovitost tovrstnega pristopa policije v boju zoper hujše oblike kriminalitete pa bomo lahko objektivno ocenjevali oziroma presojali šele na podlagi lastnih operativnih izkušenj uporabe teh podatkov. Ta bo vsekakor razvidna že iz letnih poročil o delu SI enote za informacije o potnikih, poleg tega pa tudi v tem kontekstu vidimo smotrnost uvedbe predhodno omenjene »sunset clause« pri nacionalni zakonski podlagi za obdelavo/uporabo podatkov PNR.

Tveganje št. 5

Z implementacijo sistema PNR v delo policije se uvaja policijsko pooblastilo za zbiranje in hrambo podatkov PNR z neselektivnim zbiranjem in hrambo osebnih podatkov o vseh potnikih v letalskem prometu. S tem bi lahko prihajalo do prekomernih posegov v informacijsko zasebnost posameznikov, predvsem tistih ki z namenom zbiranja nimajo nobene zveze.

Upravljanje s tveganjem:

Pri uvajanju obdelave/uporabe podatkov PNR ne gre za popolnoma novo pooblastilo, temveč za razširitev tega pooblastila za obdelavo teh podatkov API, ki se trenutno lahko izvaja skladno z določbami Zakona o letalstvu. Pri obdelavi podatkov o potnikih gre dejansko za neselektiven način zbiranja in hrambe podatkov za osebe, ki potujejo z letalskim prevozom na notranjih, zunanjih in čarterskih letih. V luči varovanja informacijske zasebnosti posameznika je neselektivnost pri zbiranju in hrambi podatkov ključni dejavnik, saj je iz te podatkovne zbirke z analitično obdelavo mogoče izluščiti tudi nekatere okoliščine o vsakdanjem življenju vsakega posameznika, ki uporablja letalski prevoz. To pomeni, da se z zbiranjem in hrambo podatkov o potnikih v prevladujočem delu posega v informacijsko zasebnost tistih (nedolžnih) potnikov, ki z namenom obdelave podatkov nimajo nobene zveze.

Neselektivnost zbiranja in hrambe podatkov je zato potrebno sorazmerno zamejiti z zagotovitvijo enakovrednih protiuteži oziroma učinkovitih varovalk. Le-te smo v podpoglavju »Proces obdelave in uporabe podatkov« (glej strani od 33-41) že navedli in s katerimi smo omejili poseg v informacijsko zasebnost le na nujno potrebno za dosego našega ustavno dopustnega cilja. Pomembno protiutež prav gotovo predstavlja selektivna oziroma usmerjena uporaba teh podatkov, ki smo jo podrobno opisali v navedenem podpoglavju. S tem pristopom pri obdelavi/uporabi podatkov o potnikih bomo prav gotovo lahko zagotovili sorazmernost posega v pravico do informacijske zasebnosti. S selektivno uporabo podatkov v osnovi ne bo šlo zgolj za preventivno (vnaprejšnjo) in nediskriminatorno zbiranje ter hrambo podatkov, temveč gre v osnovi za njihovo sprotno preverjanje skozi transparentna in nediskriminatorna ocenjevalna merila ter ustrezne podatkovne policijske zbirke, ter na tej podlagi za »uparjanje« oseb, prvič z namenom odkritja neznanih (potencialnih) storilcev terorističnih in drugih hudih kaznivih dejanj, ter drugič z namenom odkritja drugih oseb, zoper katere so razpisani ukrepi, s katerimi organi odkrivanja in pregona merijo na kazenski pregon storilcev kaznivih dejanj. Podatki o potnikih, ki z namenom zbiranja nimajo nobene zveze in se po navedenih kriterijih ne bodo »uparili«, operaterju ne bodo vidni, saj se bodo takoj po avtomatizirani obdelavi v sistemu shranili v prvotni kriptirani obliki in se bodo po zaključku časa hrambe podatkov avtomatično nepovratno izbrisali. Kot prav tako pomembno protiutež velja omeniti še naš predlog za sprejetje nacionalne

zakonske podlage za pridobitev, hrambo, analizo in izmenjavo podatkov o potnikih, s klavzulo o časovni omejitvi (»sunset clause«). S tem bodo vsekakor zmanjšane možnosti pretiranih posegov v TČPS potnikov, omogočeno jim bo tudi nemoteno koriščenje svoboščine do prostega pretoka oseb na Schengenskem območju, ter zagotovljeni hitrejši postopki mejne kontrole na letališču.

Odločitve, ki izhajajo na podlagi obdelave podatkov in ki imajo za posameznika negativne učinke, se ne smejo sprejemati zgolj na podlagi avtomatizirane obdelave osebnih podatkov, temveč je potrebno takšne zadetke ročno individualno preveriti in tako ugotoviti dejansko stopnjo tveganja oziroma aktualnost zadetka. Zato bodo operaterji vsako avtomatizirano ujemanje podatkov še ročno preverili ter dodatno potrdili ali zavrnili visoko stopnjo tveganja posameznega zadetka. S tem se bo zmanjšala možnost t.i. lažnih zadetkov, po drugi strani pa bo taka sistematična ureditev obdelave podatkov PNR, SI enoti za informacije o potnikih, omogočala izvedbo ustrezne ocene tveganja. S to informacijo bodo policisti lahko vnaprej pripravljeni na selektivno obdelavo zgolj tistih oseb, ki dejansko predstavljajo veliko tveganje za javno varnost.

Vsekakor obstaja realna možnost, da se bodo na podlagi ocenjevalnih meril, ki bodo predstavljala specifične potovalne vzorce storilcev hujših kaznivih dejanj, lahko po naključju uparili tudi posamezniki, ki s temi kaznivimi dejanji niso povezani. Prav tako se bodo lahko uparili posamezniki na podlagi razpisanih ukrepov policije, ki pa se dejansko ne bodo nanašali na njih zaradi predhodne zlorabe (kraje) njihove identitete s strani kriminalcev. V takšnih primerih bo SI PNR sistem omogočal označevanje takšnih oseb s t.i. lažnimi zadetki, zato te osebe pri potovanju ne bodo vedno znova podvržene temeljitim mejnim kontrolam. Možnost »lažnih zadetkov« bomo zmanjšali z izdelavo čimbolj natančnih ocenjevalnih meril. S tem bomo posledično tudi zmanjšali tveganje za poseg v informacijsko zasebnost nedolžnih potnikov.

Tveganje št. 6

Policija bi pridobivala in obdelovala prekomeren sklop podatkov o potnikih, vključno z bolj občutljivimi podatki.

Upravljanje s tveganjem:

Letalski prevozniki bodo policiji pošiljali podatke PNR v PNR.GOV standardu, ki ga priporočajo mednarodne organizacije IATA, WCO in ICAO. Gre za nabor manj občutljivih in vnaprej določenih podatkov, ki smo ga navedli v podpoglavju »Vsebina zbranih podatkov«. Vsi drugi občutljivi podatki, ki se nanašajo na zdravstveno stanje potnika in s tem povezane posebne potrebe, prehrano, ter druge osebne okoliščine, povezane z verskim, političnim ali drugim prepričanjem ali katerikoli drugo TČPS, se ne bodo pošiljali oziroma jih bo sistem avtomatično izbrisal.

Tveganje št. 7

Letalski prevozniki bi policiji pošiljali pomanjkljive, netočne in nepopolne podatke PNR, zaradi česar le-ti ne bodo uporabni za doseg želenega cilja

Upravljanje s tveganjem:

Podatki PNR so podatki o letalskih potnikih, ki jih letalski prevozniki hranijo v sistemu rezervacij letalskih kart. Gre namreč za nepreverjene in delne osebne podatke, ki jih pri rezervaciji letalske

karte posreduje potnik sam, brez datuma rojstva. Zaradi tega ti podatki ne omogočajo popolne identifikacije posameznega potnika. Pri popolni identifikaciji posameznika zato njihovo dodano vrednost predstavljajo podatki API iz sistema vzletne kontrole, ki se pridobivajo iz strojno čitljivega dela potovalnega dokumenta. Podatki PNR nam vsekakor lahko omogočajo identifikacijo specifičnih potovalnih vzorcev storilcev hujših kaznivih dejanj, in sicer na podlagi nabora podatkov, kot so podatki o nakupu/rezervaciji vozovnice, o osebi, ki je rezervacijo vozovnice opravila, o turistični agenciji/potovalnem agentu, o načinu plačila, o vrsti vozovnice, o načrtu potovanja, o prtljagi potnika, ipd. Letalski prevozniki bodo podatke PNR posredovali v mednarodno priznanem formatu PNR.GOV, ki poleg enotnosti in kompatibilnosti podatkov različnih prevoznikov, omogoča tudi kvaliteto teh podatkov. Tudi v tem formatu bo potrebno med različnimi letalskimi prevozniki zagotoviti kompatibilnost datotečnih shem, zato bomo temeljili na PNRGOV.XML formatu. Podatki API se bodo pošiljali v standardni obliki (Edifact PAXLIST), ki se glede na trende v naslednjih letih po vsej verjetnosti še ne bo spreminjala. Posredovanje teh podatkov po metodi »push« bo potekalo po HTTPS protokolu, kot nadomestek temu pa bo za letalske prevoznike na voljo tudi MQ protokol.

Kljub temu se zavedamo, da se bomo pri pridobivanju podatkov od različnih letalskih prevoznikov občasno srečevali tudi s težavami zaradi uporabe različnih sistemov za njihovo obdelavo, ki med seboj niso povsem kompatibilni in zato za obdelavo teh podatkov zahtevajo različno tehnično opremo. Prav zaradi tega bomo ob pridobitvi ustrezne zakonske podlage začeli postopoma pridobivati podatke PNR. Že v času trajanja SI PNR projekta smo namreč že vzpostavili kontakt z dvema letalskima prevoznikoma Adrio Airways in Turkish Airlines, ki predstavljata tudi dve največji prevozniki družbi glede na prevoz potnikov preko brniškega letališča. Po vzpostavitvi tekočega posredovanja podatkov o potnikih s tema dvema letalskima družbama, bomo to sodelovanje v okviru tako utečenih procesov razširili še na vse ostale letalske prevoznike, ki svoje prevoze opravljajo na ozemlju R Slovenije. V SI enoti za podatke o potnikih bomo z vsemi letalskimi prevozniki, ki bodo svojo dejavnost opravljali na teritoriji R Slovenije, vzpostavili kontaktne točke za permanentno sodelovanje z namenom sprotnega odpravljanja težav pri posredovanju teh podatkov.

3.2.3 Tveganja glede zavarovanja podatkov

Tveganje št. 8

Podatki o potnikih bi bili zaradi pomanjkljive informacijske varnosti izgubljeni, spremenjeni ali kako drugače zlorabljeni, tudi z možnostjo zlorabe pooblastil javnih uslužbencev. Zaradi neselektivnega načina zbiranja in hrambe podatkov se namreč poveča tudi tveganje za nezakonit dostop in zlorabo teh podatkov. Zaradi ne-transparentnosti obdelave/uporabe podatkov, njihove zlorabe ne bi bile pravočasno odkrite.

Upravljanje s tveganjem:

Pridobivanje, hramba, analiza in posredovanje podatkov bo potekala izključno v specializirani SI enoti za informacije o potnikih, s čimer bo dostop do teh podatkov omejen na ozek krog usposobljenih javnih uslužbencev. Kot smo že podrobno opisali v podpoglavju »Proces obdelave

in uporabe podatkov« (glej strani od 35-41), bo prenos podatkov iz sistema letalskega prevoznika do SI enote za informacije o potnikih potekal po metodi »push«, v skladu s katero letalski prevozniki pošljejo zahtevane podatke PNR in API, ter tako lahko tudi sami ohranijo nadzor nad svojo evidenco in katere podatke zagotavljajo. V navedeni specializirani enoti policije bo pridobivanje in obdelava podatkov o potnikih potekala v posebnem prilagojenem PNR informacijskem sistemu, ki bo prejem podatkov avtomatizirano potrdil s povratnim sporočilom letalskemu prevozniku, ki je podatke posredoval. Ta sistem bo zagotavljal transparentnost obdelave podatkov o potnikih z avtomatiziranim beleženjem zgodovine popolnoma vseh aktivnosti, tako avtomatizirane obdelave podatkov z ujemanji v ocenjevalnih merilih in določenih podatkovnih bazah, kot tudi vseh izvedenih aktivnosti operaterjev v SI enoti za informacije o potnikih, vključno s posebno avtorizacijo dostopov v sistem (uporabniško ime in geslo s povratnim obveščanjem na mail glede vstopa v sistem, digitalni podpis,...). Iz te enote bodo podatki o potnikih v določenih primerih posredovani le vnaprej določenim upravičencem, ki imajo pooblastila na področju preprečevanja, odkrivanja, preiskovanja in pregona hudih kaznivih dejanj. Podatki o potnikih jim bodo posredovani v primeru, ko bodo po uradni dolžnosti izvajali s tem povezana pooblastila oziroma aktivnosti, ali pa na ko bodo sami pisno zaprosili za tovrstne podatke, pri čemer bodo morali svoje zahteve ustrezno utemeljiti. V zahtevi bodo morali navesti predvsem obseg podatkov, ki jih bodo potrebovali, ter za kakšen namen jih bodo uporabili pri svojem delu. Na tak način bo mogoče oceniti utemeljenost vsakega posameznega zaprosila za podatke o potnikih. Pri svojem delu bodo morali zagotavljati enako raven varstva podatkov, kot jo bo zagotavljal pošiljatelj. Z namenom zagotavljanja transparentnosti in celovitost obdelave/uporabe podatkov o potnikih bodo operaterji v SI enoti za informacije o potnikih po zaključku svojega dela vse izvedene aktivnosti zabeležili v dnevnem poročilu o delu, vključno z informacijami katere podatke so obdelovali ali posredovali v uporabo, komu in za kakšen namen. Hramba podatkov se bo izvajala v samostojni policijski evidenci, ki bo vzpostavljena za ta namen. V njej bodo ti podatki zaščiteni pred zlorabo in nepooblaščenim dostopom z vsemi tehničnimi varnostnimi postopki in ukrepi (kartično omejeni dostopi do prostorov, kjer bo potekal delovni proces z obdelavo podatkov, brez listinsko poslovanje v okviru SI PNR sistema in v Lotus Notes okolju,...), ki jih policija že izvaja za vse varovane podatke⁴⁸. Ta centralizirano vodena obdelava/uporaba podatkov omogoča visoko stopnjo varnosti, zaupnosti, transparentnosti in celovitosti podatkov o potnikih.

SI enota za informacije o potnikih bo delovala kot strokovno specializirana enota za ta namen. Tu bo zagotovljena visoka strokovnost, profesionalnost in usposobljenost zaposlenih. Pomembno vodilo in osnovni okvir za doseg teh poklicnih vrednot bodo zaposleni v tej enoti zasledovali osnovna načela, ki bodo njihove smernice za zagotavljanje visokih etičnih in moralnih standardov ter visoke stopnje osebne integritete zaposlenih. Ta načela so:

- zakonitost in nediskriminatornost
- strokovnost in profesionalnost

48 Varovan podatek je osebni podatek ali drug obdelovan podatek, ki ni taje, njegovo razkritje nepoklicanim osebam pa bi povzročilo škodo državnemu organu, poteku uradnih postopkov ali fizičnim ali pravnim osebam, zato morajo njegovo obdelavo spremljati določeni varnostni ukrepi in postopki (glej 16. tč, 1. odst., 3. člen ZNPPol).

- proaktivnost, selektivnost in sistematičnost
- javnost in transparentnost dela
- individualnost in temeljitost
- odprtost in sodelovanje

Delovanje SI enote za informacije o potnikih bo v okviru rednega dela sprotno nadziral vodja te enote, poleg tega pa bo njeno delovanje podvrženo še vsem ustaljenim oblikam notranjega in zunanjega nadzora⁴⁹.

Tveganje št. 9

Letalskim potnikom ne bi bile v celoti ali pravočasno omogočene njihove pravice in sodno varstvo.

Upravljanje s tveganjem:

Letalskim potnikom bodo pravočasno zagotovljene pravice do obveščanja ter do sodnega varstva (glej odstavke »Zagotavljanje pravic letalskim potnikom, stran 40). O načinu obveščanja potnikov se bomo predhodno dogovorili z letalskimi prevozniki. Eden od možnih in pogostih načinov obveščanja potnikov je preko spletne strani letalskih prevoznikov in Policije.

3.2.4 Tveganja glede uporabe podatkov

Tveganje št. 10

Podatki o potnikih bi se uporabljali tudi za druga kazniva dejanja, ki ne bodo na seznamu hudih kaznivih dejanj, za katere se bo te podatke lahko uporabljalo.

Upravljanje s tveganjem:

Kot smo že pod upravljanjem s tveganjem št. 8 zapisali, bo sistem avtomatično beležil vse izvedene aktivnosti obdelave podatkov o potnikih, vključno z informacijami glede njihovega posredovanja drugim pristojnim subjektom. Operaterji v SI enoti za informacije o potnikih bodo po zaključku svojega dela vse izvedene aktivnosti zabeležili v dnevnem poročilu o delu, vključno z informacijami katere podatke so obdelovali ali posredovali v uporabo, komu in za kakšen namen. Za odzivanje v vsakem posameznem primeru bo navedena enota na ustrezno obrazloženo pisno zaprosilo upravičencem posredovala le tiste nujno potrebne podatkovne elemente PNR ali rezultate njihove analize zaradi preprečevanja, odkrivanja, preiskovanja in pregona konkretnega terorističnega ali hudega kaznivega dejanja (*natančno so določena na strani 29*). Poleg tega bo namen uporabe podatkov (za posamezna huda kazniva dejanja) še posebej predstavljen v letnem poročilu te enote, kar bo zagotavljalo njeno javno in transparentno delovanje.

49 Notranji nadzor nad opravljanjem policijskih nalog opravlja Sektor za notranje preiskave in integriteto na Generalni policijski upravi v obliki splošnih, strokovnih in ponovnih nadzorov; Zunanji nadzor pa opravljajo uslužbenci Direktorata za policijo in druge varnostne naloge v okviru rednih, izrednih in ponovnih nadzorov. V okviru zunanjega nadzora ima na področju varstva osebnih podatkov to pristojnost tudi IP RS.

Tveganje št. 11

Podatki o potnikih ne bi bili uporabni za dokazovanje krivde storilcem hujših kaznivih dejanj v kazenskem postopku.

Upravljanje s tveganjem:

V okviru reaktivne in sprotne uporabe podatkov o potnikih v predkazenskem oziroma v kazenskem postopku za uspešno dokazovanje krivde storilcev hujših kaznivih dejanj. Dejansko bo njihova dodana vrednost prišla do izraza, ko bodo na podlagi ocenjevalnih meril odkriti storilci pri samem izvajanju hudih kaznivih dejanj (trgovina z ljudmi, tihotapljenje prepovedane droge, orožja, ipd...). V teh primerih prav gotovo ne bo težko dokazati utemeljenega suma storitve kaznivega dejanja, oziroma višje stopnje suma za izvedbo drugih preiskovalnih aktivnosti policije pri preiskavi teh kaznivih dejanj. Poleg neposredno odkritih storilcev bodo podatki omogočali tudi odkrivanje njihovih sotorilcev oziroma njihovo medsebojno poznavanje, kar je lahko razvidno na podlagi skupnih podatkov PNR (skupno potovanje, skupno plačilo letalske karte, isti kontaktni podatki, ipd...).

Tveganje št. 12

Pri obdelavi podatkov o potnikih bo prihajalo do t.i. lažnih zadetkov, ki lahko posamezniku povzročijo negativne pravne učinke.

Upravljanje s tveganjem:

Podatki o potnikih se bodo sprotno preverjali skozi ustrezne podatkovne policijske zbirke z namenom odkritja oseb, zoper katere so razpisani ukrepi, s katerimi organi odkrivanja in pregona merijo na kazenski pregon storilcev kaznivih dejanj. Ob tem se zavedamo dejstva, da so predvsem v bazi SIS in Interpol pogosto zoper osebe razpisani ukrepi, ki niso več aktualni, vendar iz teh baz niso pravočasno izbrisani. V teh primerih bodo podatki o potnikih za osebe z neveljavnimi ukrepi, ki bodo z letalom prihajali v R Slovenijo, omogočali predhodno preverjanje veljavnosti ukrepov v državi razpisnici, in sicer še preden bodo te osebe prišle na mejno kontrolo na letališču v R Sloveniji. S tem predhodnim preverjanjem zoper takšne osebe mejnim policistom ne bo potrebno odrediti nepotrebnih prijetij in drugih ukrepov, kar za osebo seveda pomeni poseg v njegovo svobodo gibanja z odvzemom prostosti zaradi preverjanja veljavnosti ukrepa v državi razpisnici.

Odločitve, ki izhajajo na podlagi obdelave podatkov in ki imajo za posameznika negativne učinke, se zato ne smejo sprejemati zgolj na podlagi avtomatizirane obdelave osebnih podatkov, temveč je potrebno takšne zadetke ročno individualno preveriti in tako ugotoviti dejansko stopnjo tveganja oziroma aktualnost zadetka. Zato bodo operaterji vsako avtomatizirano ujemanje podatkov tudi ročno preverili ter dodatno potrdili ali zavrnili visoko stopnjo tveganja posameznega zadetka. S tem se bo zmanjšala možnost t.i. lažnih zadetkov, po drugi strani pa bo taka sistematična ureditev obdelave podatkov, SI enoti za informacije o potnikih, omogočala pripravo ustrezne ocene tveganja. S to informacijo bodo policisti lahko vnaprej pripravljeni na selektivno obdelavo zgolj tistih oseb, ki dejansko predstavljajo veliko tveganje za javno varnost.

Vsekakor obstaja realna možnost, da se bodo na podlagi ocenjevalnih meril, ki bodo predstavljala specifične potovalne vzorce storilcev hujših kaznivih dejanj, lahko po naključju uparili tudi

posamezniki, ki s kaznivimi dejanji niso povezani. Prav tako se bodo lahko uparili posamezniki na podlagi razpisanih ukrepov policije, ki pa se dejansko ne bodo nanašali na njih zaradi predhodne zlorabe (kraje) njihove identitete s strani kriminalcev. V takšnih primerih bo SI PNR sistem omogočal označevanje takšnih oseb s t.i. lažnimi zadetki, zato te osebe pri potovanju ne bodo vedno znova podvržene temeljitim mejnim kontrolam. Možnost »lažnih zadetkov« bomo zmanjšali z izdelavo čimbolj natančnih ocenjevalnih meril. S tem bomo posledično tudi zmanjšali tveganje za poseg v informacijsko zasebnost nedolžnih potnikov.

Tveganje št. 13

Ocenjevalna merila, na podlagi katerih naj bi se ugotavljala identiteta t.i. neznanih (potencialnih) storilcev terorističnih in drugih hudih kaznivih dejanj, bi lahko bila diskriminatorna zaradi njihove netransparentne implementacije in uporabe v sistemu PNR.

Upravljanje s tveganjem:

Podatki PNR se bodo v sklopu njihove proaktivne uporabe avtomatizirano obdelovali in temu primerno uparjali na podlagi vnaprej določenih in nediskriminatornih ocenjevalnih meril (*glej strani 20 - 22, 29 – 30*). To pomeni, da ne bodo posredno, niti neposredno temeljila na rasnem ali etničnem poreklu osebe, njenem verskem, filozofskem ali političnem prepričanju, članstvu v sindikatu, zdravstvenem stanju ali spolnem življenju ali katerokoli drugo osebno okoliščino, kar določa Ustava RS. Vsekakor bo zagotovljena tudi njihova transparentnost pri implementaciji oziroma uporabi v sistemu SI PNR, saj bodo oblikovana na podlagi pisnih ocen tveganj, izdelanih v povezavi z odkrivanjem in preiskovanjem terorističnih in drugih hudih kaznivih dejanj (*glej odstavek Uporaba ocenjevalnih meril, stran 40*).

3.2.5 Tveganja glede hrambe podatkov

Tveganje št. 14

Zaradi predolgega roka hrambe podatkov bi lahko prišlo do prekomernega posega v TCPS, pri čemer ta čas ne bi bistveno vplival na učinkovitost tega usmerjenega pristopa policije.

Upravljanje s tveganjem:

Dejstvo je, da mora biti čas hrambe podatkov utemeljen ter omejen z namenom uporabe podatkov na eni strani, ter z doseganjem ustavno dopustnega cilja na drugi strani. Čas hrambe podatkov bo bistveno vplival na natančnost oblikovanih ocenjevalnih meril in s tem povezanim zmanjšanjem števila napačnih zadetkov. Z daljšim časom je namreč mogoče pridobiti ustrezno velik, reprezentativen vzorec določenih podatkov, zaradi česar bo stopnja tveganja natančnejša in tudi bolj ciljno usmerjena v ožjo specifično skupino ljudi. To bo posledično pomenilo tudi manjše tveganje za poseg v informacijsko zasebnost ostalih potnikov (*glej podpoglavje 2.2, stran 20 – 23, ter odstavek »Varstvo in hramba osebnih podatkov«, stran 40*). Poleg tega je, zaradi narave teh podatkov in njihove uporabnosti v predkazenskem in v kazenskem postopku nujno, da se hranijo ustrezen čas, kar smo predhodno podrobno utemeljili (*glej podpoglavje 2.2, stran 19 – 20*).

4 TEST SORAZMERNOSTI ZARADI KOLIZIJE ČLOVEKOVIH PRAVIC

V komentarju Ustave RS avtorji trdijo, da splošno načelo sorazmernosti predstavlja izvedbeno načelo pravne države, ki je opredeljeno v njenem 2. členu. Bolj kot so posamezniki prizadeti v svoji pravici, toliko močnejši morajo biti interesi varovanja pravic drugih v okviru javne koristi. Pri takšnem celostnem tehtanju nam zatorej načelo sorazmernosti predstavlja splošno napotilo pri omejitvah človekovih pravic. *(povzeto iz komentarja ustave RS, str. 56)*

Eno izmed bolj zanimivih in hkrati družbeno manj zavedajočih je prav gotovo protislovje, oziroma konflikt med posameznimi človekovimi pravicami, kot na primer med zgoraj navedenimi osebnostnimi pravicami in pravico do varnosti. Ugotovili smo že, da te človekove pravice nasproti represivnemu delovanju policije pogostokrat medsebojno kolidirajo. Pričakovanja in zahteve civilne družbe so, da morajo biti vsakemu posamezniku zagotovljene vse te ustavne vrednote v okviru njihovega maksimuma. Ker pa so med seboj neločljivo in paradoksalno povezane, je potrebno med njimi nenehno tehtati z uporabo strogega testa sorazmernosti. V sklopu istega testa je potrebno pri zasledovanju legitimnega in ustavno dopustnega cilja zagotoviti, da je uravnoteženost odnosa med zgoraj navedenimi pravicami v konfliktu. Drugače povedano, odločitev oziroma ukrep, ki v zavarovanju prve pravice posega v drugo ali v več od njih, mora v razumnem sorazmerju zadostiti vsem zahtevanim ustavnim vrednotam. Pri tovrstnem proučevanju si je vmesno zastaviti na videz protislovni vprašanje in sicer do katere meje sploh sme država omejevati TSČP ter ali ni morebiti nivo slednjih v določenem kontekstu na takšni ravni, da bi njihovo dosledno udejanjanje lahko sprožilo ogrožanje varnosti družbe ter varnost in stabilnost države.

Ustava RS s svojim splošnim načelom sorazmernosti jasno ograjuje zakonodajalca k omejitvi ustavno varovanih pravic posameznika, zgolj s pravicami drugih subjektov, ki morajo biti v tem okvirju tudi v javnem interesu. Zatorej mora biti vsak tak poseg v posameznikovo temeljno svobščino utemeljen s stvarnim in razumnim tehtanjem dvoje ali več nasprotujočih si ustavno varovanih dobrin, v cilju opredeljivosti, razumnosti in seveda ustavne legitimnosti določene rešitve⁵⁰.

Splošno načelo sorazmernosti v bistvu predstavlja test legitimnosti oziroma preizkus:

- ali je cilj, ki ga zasleduje država, legitimen oziroma ustavno dopusten in
- ali so od države uporabljena sredstva kot taka pravno dopustna, kar se preverja skozi preizkus sorazmernosti, kjer se nadalje ugotavlja:
 - o ali so izbrana sredstva za dosego cilja smiselna oz. primerna (sredstvo je primerno, če se je z njegovo pomočjo mogoče približati željenemu rezultatu - so uporabna in možna)
 - o ali ta sredstva kot taka pridejo v poštev za dosego cilja in so zato potrebna oziroma nujna (sredstvo je nujno, če ni na izbiro drugega enako učinkovitega sredstva, ki ne bi omejevalo TČPS ali pa bi jih manj omejevalo) ter

50 Povzeto po 9. točki 2. člena Komentarja Ustave RS.

- o ali so izbrana sredstva v okviru razumnega razmerja oziroma ali je bilo vzpostavljeno razumno ravnovesje med prizadeto ustavno pravico posameznika, ki jo povzroča uporaba izbranega sredstva in med ustrezno koristjo, ki jo pridobimo z uporabo sredstva za zaščito pravic drugih, skratka v javno korist.

Določba 2. odstavek 120. člena ob hkratni neodvisnosti in samostojnosti delovanja uprave, sicer zavezuje upravne organe k izvrševanju svojih nalog na podlagi Ustave in zakonov. Skladno z načelom pravne države se vsa pravna razmerja med državo in državljani urejajo s splošno veljavnimi zakoni, na način poznanosti⁵¹, preglednosti in predvidljivosti. Kumulativno vse troje predstavlja državljani visoko stopnjo pravne varnosti. Skladno z načeli varstva TČPS, demokratičnosti in pravne države, sme torej omejevati določene pravice državljanov, v Ustavno dopustnih pogojih, zgolj zakonodajalec. Skladno z navedenimi ustavnimi načeli smo v vsebini tega dokumenta skušali dosledno zasledovati in odgovoriti na temeljna vprašanja. Naš izdelan strogi test sorazmernosti v primeru širitve pooblastila policije na obdelavo podatkov PNR, v pravnem pomenu ne more biti kompetenten, saj je za ustavno presojo pravilnosti pristojno izključno le Ustavno sodišče RS. Kljub temu pa smo k izvedbi strogega testa sorazmernosti pristopili objektivno in z vso resnostjo ter v okviru pravnega znanja, ki smo si ga pridobili na podiplomskem študiju na področju prava. V širšem pomenu navedenega testa lahko trdimo, da gre nesporno za razumno povezavo med predlaganim ukrepom (*obdelava in uporaba podatkov PNR*) in ustavno dopustnim ciljem (*zagotovitev višje stopnje varnosti državljanom*).

Zaradi bolj objektivne presoje v okviru testa sorazmernosti, moramo pomen vsake od navedenih človekovih pravic поближе spoznati z ustavnopravnega vidika, kar smo storili v naslednjih podpoglavjih.

4.1 Ustavno pravni vidik zadevnih človekovih pravic

TČPS v sodobnih in demokratično urejenih državah veljajo za najvišje ustavno varovane vrednote. Te je Slovenija v Resoluciji predstavila za enega izmed pomembnih strateških interesov. Med vsemi so kot najpomembnejše izpostavljene neodtujljive osebnostne pravice definirane v členih od 34 do 38 Ustave RS. Ustavno sodišče RS⁵² izpostavlja poseben pomen ustavnega varstva človekove osebnosti, pri čemer imajo posebno mesto med TČPS določbe, ki varujejo človekovo osebno dostojanstvo, osebnostne pravice, njegovo zasebnost in varnost.

Ugotovili smo že, da iste pravice med seboj nemalokrat kolidirajo, zlasti ob nujnih posegih represivnih organov. Zakonodajalec ima možnost določenih ustavno varovanih pravic posameznika omejiti le s pravicami drugih, vendar mora biti to tudi v širšem javnem interesu. Zato morajo biti takšni posegi utemeljeni s sorazmernostjo, kjer se ugotavlja primernost in neogibna potrebnost za uresničitev zakonodajnih ciljev v javnem interesu. Vedno se presoja tudi, ali je morebiti z drugim milejšim sredstvom mogoče doseči enak ustavno dopusten cilj. Gre za test sorazmernosti, ki se mora izvesti v primerih, ko si posamezne človekove pravice med seboj nasprotujejo.

51 Jasnost, razumljivost in nedvoumnost zakonskih norm, na način iz katerega zmore povprečen nevešč prava občan zanesljivo razbrati svoj pravni položaj. Povzeto po 15. točki 2. člena Komentarja Ustave RS.

52 Odločitev US, U-I-25/95, Ur. l. št. 5/98.

Zavedamo se, da bi razširjeno policijsko pooblastilo pridobivanja, hrambe, obdelave in posredovanja podatkov PNR, lahko pomenilo tudi dodatni poseg v ustavno varovane človekove osebnostne pravice; varstvo zasebnosti posameznika in zaščito njegovih osebnih podatkov. Vendar policija stremi k zagotavljanju najvišje možne stopnje varnosti državljanov pri čemer mora imeti na voljo tudi določena orodja. Ta morajo biti v izogib koliziji osebnostnih pravic sorazmerno umerjena. V cilju ustrezne presoje in medsebojnega tehtanja vsake od navedenih človekovih pravic jim moramo поблиže spoznati. Pomagali smo si s proučevanjem novejšega Komentarja ustave Republike Slovenije. Po stališču Ustavnega sodišča⁵³, imajo med vsemi človekovimi pravicami, posebno mesto prav določbe, ki varujejo človekovo osebno dostojanstvo, varnost, osebnostne pravice in njegovo zasebnost. V skladu s pravno teorijo, ki pravi, da je prepovedano vse, kar ni izrecno dovoljeno, Ustava prepoveduje vsak poseg v našete pravice, razen v primerih, ko je to izrecno dopustno.

Razširjeno pooblastilo zbiranja/obdelave PNR podatkov bi po določenih interpretacijah predstavljal dodaten poseg v pravico do zasebnosti in z njo povezano pravico do varstva osebnih podatkov. Zato smo v konceptu njihovega uvajanja, striktno sledili načelom, ki zagotavljajo uresničevanje temeljnega ustavnega načela pravne države: zakonitosti, poštenosti, transparentnosti, sorazmernosti, točnosti in ažurnosti, ustreznim rokom hrambe, zavarovanju osebnih podatkov in seveda pravice posameznikov.

4.1.1 Varnost

Človekova pravica do varnosti je zagotovljena vsakomur in je določena v 34. členu Ustave RS, v katerem je posamezniku hkratno zagotovljena pravica do človekovega dostojanstva in varnosti. Pomembno pri tem je, da so dolžni ti združeni pravici spoštovati državna oblast, kot tudi posamezniki, torej brez izjem. V osnovi je zato to obrambna pravica. Iz narave stvari tudi izhaja, da je država dolžna pravico do osebnega dostojanstva in varnosti zagotavljati tudi sama, z lastnim ravnanjem, saj je to smisel temeljnih ustavnih načel; demokracije in pravne države.

Če se v tej človekovi pravici osredotočimo na varnost, pojem »varnost vsakogar« v 34. členu Ustave RS pomeni normo, ki pravico zagotavlja, in ne določbe, ki to omejuje. Ustavno dopustne so le omejitve v skladu s tretjim odstavkom 15. in 16. členom Ustave RS. V obeh pa je potrebno spoštovanje splošnega ustavnega načela sorazmernosti.

V primeru odločbe Ustavnega sodišča Up-7/98, z dne 30.9.1998, iz katerih povzemamo odločitev senata, da določbe Zakona o prekrških, glede odvzema lovske puške in streliva, če to zahtevajo razlogi splošne varnosti, predstavljajo ukrep v okviru zakonodajalčevega nadzora nad uporabo orožja. Zakonodajalec je z odvzemom orožja v tem primeru **sorazmerno** posegel v pravico do zasebne lastnine (33. člen Ustave) zato, da je zagotovil spoštovanje pravice do varnosti. Ista človekova pravica je ustavno privilegirana nasproti drugim TSČP. Podobno materiji lahko izluščimo tudi iz 20. člena Ustave RS, ki **dovoljuje odvzem prostosti** osumljencu kaznivega dejanja, »**kadar je to neogibno potrebno** za potek kazenskega postopka ali **za varnost ljudi**«. Nekaj teh navajanih določil služi prikazu rangiranja pravice do osebne in javne varnosti, pri čemer lahko ugotovimo, da je ta človekova pravica ustavno privilegirana pravica v navedenih primerih .

53 Gre za človekove pravice od 34. do 38. člena Ustave RS, odločitev US, št. U-I-25/95, Ur. L. št. 5/98.

Za primere, ko gre za vprašanje varnosti države ali javne varnosti⁵⁴ pa je možno isto (*pod določenimi pogoji*) zagotavljati tudi z drugimi ustavno dopustnimi omejitvami.

4.1.2 Zasebnost in varstvo podatkov

Zasebnost je ustavno varovana človekova pravica iz 35. člena, imenovana varstvo pravic zasebnosti in osebnostnih pravic. Za boljše razumevanje je potrebno vedeti, da se pravica do zasebnosti v pravu pojavlja kot osebnostna pravica, to je pravica zasebnega značaja in kot človekova pravica javnopravnega značaja. Človeka, posameznika varuje pred posegi države v njegovo zasebno sfero, v okviru osebnostne pravice pa varuje istega, oziroma njegovo osebnostno sfero (*nedotakljivost človekove osebnosti, družinskega življenja,...*) tudi v razmerjih do drugih posameznikov.

V našem primeru se bomo pri zasebnosti omejili na njen javnopravni značaj, ko je človekova pravica oziroma njegova zasebnost varovana pred posegi države. K takemu javnopravnemu statusu v veliki meri prispevajo prav zaradi določbe 8. člena EKČP⁵⁵ (*pravica do spoštovanja zasebnega in družinskega življenja*). Te dajejo vsakomur »pravico do spoštovanja svojega zasebnega in družinskega življenja, svojega doma in dopisovanja«. Javni oblasti pa prepovedujejo vmešavanje v izvrševanje te pravice, **»razen če je to določeno z zakonom in nujno v demokratični družbi zaradi državne varnosti, javne varnosti ali ekonomske blaginje države, zato, da se prepreči nered ali zločin, da se zavaruje zdravje ali morala ali da se zavarujejo pravice in svoboščine drugih ljudi«**. Posplošeno rečeno je pravica do zasebnosti predmet varstva posameznika pred arbitrarnimi posegi javne oblasti v zasebno in družinsko življenje. Človekovo zasebnost in osebnostne pravice je potrebno razumeti tudi širše, saj jo ustavni vidiki varujejo tudi v drugih njenih določbah (*36. člen: nedotakljivost stanovanja, 37. člen: varstvo tajnosti pisem in drugih občil, 38. člen: varstvo osebnih podatkov*) in se tako med seboj prepletajo ter dopolnjujejo.

Kljub temu, da gre za mednarodno pomembno ustavnopravno človekovo pravico, pa le-ta ni absolutna. Pri obravnavi te pravice je za ocenitev nasprotnega zornega kota nujna omemba pomembnega izvedenega pravnega načela, izhajajočega iz odločitve Ustavnega sodišča (*U-I-25/95, Ur.l. št. 5/98*), »da se pravica do zasebnosti za posameznika lahko konča samo takrat in tam, kjer kolidira z zakonsko izkazanim močnejšim interesom drugih«. Poleg tega načela je pomembno pri tem vedeti, da je potrebno pri tej človekovi pravici upoštevati načelo, da je v pravni državi javni oblasti prepovedano vse, kar ni izrecno dovoljeno, kar smo lahko videli pri zgornjem citiranju 2. odstavka 8. člena EKČP, ki javni oblasti, poleg prepovedi, izjemoma dovoljuje vmešavanje v izvrševanje te pravice. Med te izjeme lahko prav gotovo prištevamo tudi obdelavo podatkov o potnikih za zagotavljanje javne in mednarodne varnosti.

Varstvo osebnih podatkov se v literaturi pogosto označuje tudi s pojmom informacijska zasebnost, torej kot del človekove zasebnosti. Temu je sledilo tudi Evropsko sodišče za človekove pravice (*v nadaljevanju: ESCP*), ki je v okviru svoje pravne prakse osebno ime označilo kot sestavni del pravice do spoštovanja zasebnega življenja. Bistvo te t.i. informacijske zasebnosti je posamezniku zagotoviti, obdržati podatke o sebi zase, ker noče, da bi bili z njimi seznanjeni drugi. Ustava RS varstvo osebnih podatkov, kot že rečeno ureja v svojem 38. členu, v okviru

54 Npr pod pogoji členov 36, 37, 38, 42, in 90 Ustave RS.
55 Uradni list RS(13.6.1994) MP, št.7-41/1994 (RS 33/1994)

katerega je podana zahteva po zakonitosti zbiranja teh podatkov, njihove obdelave in uporabe, ter zahteva po njihovem zbiranju in uporabi za vnaprej določene namene. Posamezniku pa daje pravico do seznanjenosti o tem, kateri podatki se zbirajo o njem in pravico do sodnega varstva. Torej ni dolžnost države le varstvo osebnih podatkov temveč tudi pravna regulacija tega področja.

Vendarle pa tudi informacijska zasebnost, kot del zasebnosti ni absolutna. Posegi v varstvo osebnih podatkov iz 38. člena Ustave so po ustaljeni presoji Ustavnega sodišča dopustni, ko so ti v skladu z načelom sorazmernosti. Predhodno morajo zato prestati t.i. strogi test sorazmernosti. Iz navedene ustavne določbe in iz Konvencije o varstvu posameznikov izhajajo, da je poseg dopusten takrat, če je v zakonu določeno opredeljeno, kateri podatki se smejo zbirati in obdelovati, za kakšen namen jih je dovoljeno uporabiti, nadzor nad zbiranjem, obdelovanjem, in uporabo ter varstvo tajnosti zbranih osebnih podatkov. Namen zbiranja pa mora biti ustavno dopusten.

ESČP v svoji ustaljeni praksi sprejema stališče, da poseg, če naj bo dopusten, mora ustrezati »nujni družbeni potrebi«, in biti sorazmeren z legitimnim zasledovanim namenom, razlogi s katerimi jih država utemeljuje pa morajo biti relevantni in zadostni.

Na področju varstva pravic zasebnosti se pravna teorija⁵⁶ opira na opredelitev Komisije, ki je na očitek o posegu v zasebno življenje, zavrnila v primerih obveznosti privezovanja z varnostnim pasom, obvezne uporabe prehodov za pešce v prometu, varnostnih ukrepov zaradi varstva delavcev, odvzema voznškega dovoljenja, kot tudi glede uživanja alkohola in mamil, ipd. Ti ukrepi so bili utemeljeni z varstvom posameznikov, kjer je bila pravica do varnosti postavljena v prioritetni položaj nasproti pravici do zasebnosti in osebnostnih pravic.

4.2 Ustavna dopustnost cilja

V širšem okvirju najmilejšega testa sorazmernosti ugotavljamo, da je cilj, ki ga zasledujemo in ki je definiran kot preprečevanje terorističnih in drugih hujših kaznivih dejanj in z njim povezana širitev pooblastil na pridobivanje in obdelave podatkov PNR, legitimen oziroma ustavno dopusten, saj to predstavlja eno izmed nalog policije, ki so navedene v 4. členu ZNPPol. Nesporno gre za razumno povezavo med predlaganim ukrepom in ciljem zagotovitve višje stopnje varnosti državljanov. Zato predlagana širitev pooblastil sodi kontekst zagotavljanja višje stopnje javne in nacionalne varnosti.

4.3 Test primernosti in učinkovitosti

Sredstva za doseg navedenega ustavno dopustnega cilja v našem primeru predstavljajo PNR podatki oziroma njihova obdelava/uporaba za zgoraj naveden namen. V oceni stanja za področje hujše kriminalitete (*glej podpoglavje 2.1*) smo iz različnih analitičnih poročil razbrali, da gre v primeru terorističnih in drugih hujših oblik kaznivih dejanj za mednarodno razsežne kriminalne aktivnosti, pri čemer so mednarodna potovanja storilcev teh kaznivih dejanj postali sestavni del našega vsakdana (*glej stran 9, 11*). To je pomembno tudi za Slovenijo, saj se nahajamo v osrčju Evrope, kjer je presečišče glavnih (kriminalnih) transportnih koridorjev, kar našo državo v

56 Glej Komentar Ustave RS, urednik Lovro Šturm, člen 35, odstavek 14, stran 373.

evropskem prostoru uvršča med pomembne tranzitne države. Po ocenah Interpola iz ozemlja EU na bojišča v Sirijo letno odpotuje cca. 3000 borcev – ekstremistov, vendar pa je kljub temu odkritih zgolj 700 takšnih oseb, zoper katere so organi pregona uspeli uvesti sodne postopke zaradi suma izvrševanja terorizma. Tako velik odklon je prav gotovo posledica pomanjkanja ustreznih orodij, kot npr. možnost sledenja elektronskim sledem storilcev. Slednji so zaradi obsežnega mednarodnega prostora, v katerem se pri izvajanju kriminalnih aktivnosti vse pogosteje med seboj povezujejo, prisiljeni potovati z letali zaradi časovno hitrejšega premagovanja daljših razdalj. Takšna potovanja z letalskimi prevozniki skozi mednarodni prostor so tudi vse bolj cenena. Prav zaradi tega so se podatki PNR na podlagi tujih izkušenj na operativnem nivoju izkazali kot zelo uporaben informacijski vir pri preprečevanju in omejevanju tovrstne kriminalitete. Prav tako so se sistemi, znotraj katerih se ti podatki obdelujejo, na sistemskem nivoju izkazali kot učinkovito orodje za izdelavo uporabnih ocen tveganj, na podlagi katerih je mogoče skozi ustrezno oblikovana ocenjevalna merila, identificirati »neznane« storilce hujših kaznivih dejanj in na ta način takšna dejanja preprečevati (*glej podpoglavje 2.2, strani 16 – 17*).

Z učinkovitostjo ukrepa s strani tujih varnostnih organov utemeljujemo uporabnost podatkov PNR oziroma učinkovitost obdelave teh podatkov v povezavi z ustreznim časom hrambe podatkov in povezljivostjo podatkov API in PNR. Dejstvo je, da obdelava/uporaba podatkov PNR za slovensko policijo predstavlja popolnoma nov pristop pri preprečevanju in odkrivanju hujših oblik kriminalitete, zato je neprimerno kakorkoli brez izdelanih poglobljenih analiz špekulirati s prognostičnimi ocenami o kvantiteti preprečenih terorističnih in drugih hujših varnostnih grožnjah. Ti varnostni pojavi so tako zelo nepredvidljivi in odvisni od številnih raznovrstnih, v našem okolju, neraziskanih dejavnikov (okoljski, politični, verski, socialni, sociološki, psihološki, fizični, meteorološki, ipd...), da je v kvantitativnih okvirih to nemogoče napovedati.

Kot že navedeno, iz tujih izkušenj izhaja, da je s tovrstno ustrezno analitično obdelavo podatkov o potnikih mogoče dovolj podrobno opredeliti specifične oziroma ponavljajoče potovalne vzorce teroristov in storilcev drugih hudih kaznivih dejanj, ki predstavljajo odklone od običajnega vzorca večine potnikov. Na tovrstne moduse storilcev sta med drugim še posebej pozorni tudi EU agenciji Frontex in Europol, ter mednarodna organizacija Interpol, ki na te aktualne specifične vzorce redno opozarjajo v svojih periodičnih oziroma ad-hoc analitičnih izdelkih, ki jih pošiljajo organom odkrivanja oziroma kazenskega pregona v partnerskih državah. Tudi to je dokaz, kako pomembne in uporabne so tovrstne informacije za organe odkrivanja oziroma kazenskega pregona, saj se lahko uspešno borijo zoper kriminal le z dobrim poznavanjem njegovih značilnosti oziroma delovanja.

V policiji se zavedamo pomembnosti našega proaktivnega pristopa pri preprečevanju oziroma omejevanju kriminalitete, kar nam bo prav gotovo na zgoraj naveden način omogočala tudi obdelava/uporaba PNR podatkov. V primeru, da ob izvajanju tega pristopa v Sloveniji ne bomo zabeležili nobenega terorističnega napada, ter da bomo lahko ugotovili zmanjšanje kriminalitete oziroma porast lastne zaznave kaznivih dejanj, bomo lahko zatrdili, da je policija naredila vse potrebno pri izvajanju svojega poslanstva v skupnosti.

V zvezi učinkovitosti novega orodja z obdelavo/uporabo podatkov PNR bomo lahko v policiji objektivno presojali šele na podlagi lastnih operativnih izkušenj uporabe teh podatkov. Kot smo to že navedli v *podpoglavju 3.2.1*, prav v tem segmentu vidimo dodatno možnost systemskega varovala pred neuravnoteženim trajnim posegom v človekove pravice. Zato predlagamo sprejetje nacionalne zakonske podlage za pridobitev, hrambo, analizo in izmenjavo podatkov o potnikih, s klavzulo o časovni omejitvi (»sunset clause«) le-te na 5 let.

Z navedenimi dejstvi ocenjujemo primernost podatkov o potnikih PNR, ki so na podlagi tujih izkušenj že dokazano uporabni pri preprečevanju, odkrivanju, preiskovanju in pregonu storilcev terorističnih in drugih hujših kaznivih dejanj.

4.4 Test nujnosti

Kot že rečeno, obdelava oziroma uporaba podatkov PNR predstavlja eno izmed do sedaj najučinkovitejših analitičnih pristopov policije, predvsem v proaktivnem smislu, pri preprečevanju hujših oblik kriminalitete ter za izsleditev njihovih storilcev. Po splošni oceni gre za nižje rangirano poseganje v zasebnost, kot to velja za ukrepe, ki jih v teh primerih policija uporablja v sedanjih preiskavah. Navedena kazniva dejanja so vsebinsko, časovno in krajevno obsežna, zaradi tega so kriminalistične preiskave v teh primerih zelo zahtevne in dolgotrajne. S klasičnimi policijskim delom, ob vse bolj omejenih kadrovskih in finančnih virih, je ta kazniva dejanja vse težje odkrivati, pri čemer je odkritje v veliki meri stvar naključne lastne zaznave policistov. Policisti vsekakor začnejo vsa kazniva dejanja, vključno s terorističnimi in drugimi hujšimi kaznivimi dejanji, odkrivati in preprečevati z osnovnimi policijskimi pooblastili kot so zbiranje obvestil, vabljenje, ugotavljanje identitete osebe, iskanje osebe, prepoznavanje oseb po fotografijah, postavljanje cestnih zapor, opravljanje varnostnih pregledov, zaseg predmetov, izvajanje protiterorističnih pregledov, začasna omejitve gibanja oseb, ipd. Kazniva dejanja policisti začnejo preiskovati ob podanih razlogih za sum, da je bilo storjeno kaznivo dejanje, za katero se storilec preganja po uradni dolžnosti, na podlagi 148. člena Zakona o kazenskem postopku. Gre za t.i. klasična policijska pooblastila, ki jih policija lahko neposredno izvaja na podlagi 33. člena Zakona o nalogah in pooblastilih policije brez vsakršnih dodatnih sodnih odredb, ker ne predstavljajo grobih posegov v človekove pravice. S temi klasičnimi pooblastili je ob vse bolj omejenih kadrovskih in finančnih virih, vse težje odkrivati hujša kazniva dejanja. Gre namreč za kazniva dejanja, ki so vsebinsko, časovno in krajevno obsežna, zaradi tega so kriminalistične preiskave v teh primerih zelo zahtevne in dolgotrajne. Odkritje teh kaznivih dejanj s klasičnimi metodami je zato v veliki meri stvar naključne lastne zaznave policistov. Za takšno naključje je šlo tudi v primeru zasega droge na brniškem letališču, ki ga navajamo (*glej stran 17*). Zaradi informacijsko zelo zaprtih in previdnih kriminalnih združb, je zelo težko ali skorajda nemogoče pridobiti informacije o njihovem kriminalnem delovanju, ki bi dosegale visoko stopnjo utemeljenega suma. Ker policisti s temi klasičnimi pooblastili, ki predstavljajo najmilejše posege v človekove pravice, ne uspejo zoper storilce zbrati dovolj trdnih dokazov, s katerimi bi lahko utemeljevali zadostno stopnjo suma za podajo kazenske ovadbe, se začnejo posluževati drugih policijskih pooblastil, ki pa se zaradi hujšega posega v človekove pravice začnejo lahko izvajati le na podlagi predhodne sodne odredbe. Gre za prikrite preiskovalne ukrepe. Ta pooblastila policije pa z odredbo vsekakor ne morejo biti odobrena, če policija preiskovalnemu sodniku ne dokaže,

da s klasičnimi policijskimi pooblastili in metodami niso uspeli zbrati dovolj dokazov za utemeljitev suma storitve kaznivega dejanja zoper posameznega storilca. Zato se policisti pri doseženih razlogih za sum, da je bilo storjeno kaznivo dejanje, za katero se storilec preganja po uradni dolžnosti, začnejo pogosto posluževati uporabe prvega prikritega preiskovalnega ukrepa – pridobivanja podatkov o prometu v elektronskem komunikacijskem omrežju. Na podlagi tovrstnih ugotovitev lahko policisti v nadaljevanju svoje aktivnosti razširijo še na ostale prikrite preiskovalne ukrepe (*tajno opazovanje, nadzor elektronskih komunikacij s prisluškovanjem in snemanjem, kontrola pisem in drugih pošilk, prisluškovanje in snemanje, ter opazovanje v tujem stanovanju ali drugih tujih prostorih,...*). Uvedba teh ukrepov je mogoča šele po obstoju višjega dokaznega standarda v predkazenskem postopku, to je utemeljen razlog za sum, s pomočjo katerih lahko policisti nadalje uspešno preiskujejo kriminalne dejavnosti mednarodno delujočih kriminalnih združb v okviru mednarodnega policijskega sodelovanja. Takšne obsežne policijske preiskave so tudi dolgotrajne, kar časovno pomeni tudi veliko tveganje, da bi do nevarnih škodljivih in nepopravljivih posledic že prišlo. Tako je opisan tradicionalni pretežno reaktivni način delovanja policije pri preiskovanju mednarodnih kriminalnih združb. S tovrstnimi aktivnostmi policija vsekakor na zakonit način posega globoko v zasebnost in svobodo posameznikov.

Pogostost uporabe prikritih preiskovalnih ukrepov smo poskušali dokazati s statističnimi podatki policije v povezavi s hujšimi oblikami kaznivih dejanj, vendar tovrstnega statističnega prikaza, zaradi omejenosti sistema, žal nismo uspeli izdelati. Smo pa ta podatek lahko pridobili na drugačen način, in sicer policija je v letu 2013 na podlagi Zakona o kazenskem postopku izvedla prikrite preiskovalne ukrepe v okviru 107 zadev, t.i. operativnih obdelav ali operativnih kombinacij (OO, OK), v okviru katerih je bilo odrejenih kar 1791 prikritih preiskovalnih ukrepov. To pomeni 16,7 prikritih preiskovalnih ukrepov v eni operativni obdelavi oziroma operativni kombinaciji. Ta podatek pa je dovolj prepričljiv o kompleksnosti in pogostosti uporabe tovrstnih policijskih pooblastil, ki pomenijo zelo velike posege v človekove pravice, predvsem v zasebnost posameznika.

Uporaba podatkov o potnikih (PNR, API) za namen preprečevanja terorističnih in hujših kaznivih dejanj prav gotovo predstavlja manjši poseg v zasebnost posameznika, kot zgoraj navedeni prikriti preiskovalni ukrepi. Z njihovo proaktivno in sprotno uporabo v okviru avtomatizirane obdelave podatkov in njihovega uparjanja skozi vnaprej določena transparentna ocenjevalna merila, bo dokazano na podlagi tujih izkušenj mogoče ugotavljali identiteto oseb, ki še niso bile prepoznane kot storilci navedenih kaznivih dejanj, vendar pa bodo na podlagi analize podatkov argumentirano predstavljale veliko verjetnost njihove soudeležbe pri navedenih kriminalnih aktivnostih. Sočasno pa bodo s preverjanjem skozi zakonsko opredeljene nacionalne in mednarodne zbirke, pripomogle še k izsleditvi iskanih oseb ali oseb, zoper katere so razpisani drugi zakoniti ukrepi ali operativne informacije. To za policijo pomeni hitrejše odkrivanje oziroma preprečevanje kaznivih dejanj z manjšimi škodljivimi posledicami za ljudi in njihovo premoženje.

To utemeljujemo z izkušnjami držav članic, ki podatke PNR že uporabljajo za preprečevanje kriminalitete. Iz njihovih analiz podatkov je bilo mogoče podrobno opredeliti specifične oziroma ponavljajoče vzorce potovalnih modusov storilcev, povezanih s trgovino z ljudmi in s prepovedanimi drogami. Ti vzorci so posamezne kriminalne skupine zaznamovale v okviru

specifičnega modusa operandi, ki so predstavljali njihove varnostno zanimive odklone. Rezultati analitično obdelanih podatkov PNR so bistveno pripomogli k boljšemu razumevanju povezovalnih značilnosti in delovanja kriminalnih mrež (*glej strani 16 – 17*). Na tovrstne varnostne pojave Slovenija, zaradi svoje geografske lege ni imuna, saj tudi na brniškem letališču beležimo primere trgovine z ljudmi iz balkanskih držav, pa tudi primere tihotapljenja prepovedane droge v potovalnih kovčkih potnikov, že kar dva primera tudi v letošnjem letu.

Na podlagi navedenega ocenjujemo, da bomo z uporabo podatkov PNR in njihovo izmenjavo, povečali delež lastnih zaznav pri odkrivanju hujših kaznivih dejanj s čezmejnimi elementi in njihovih storilcev, s čimer bomo te trende približali trendom hitrejše rasti tovrstne kriminalitete. Tem storilcem bo z uporabo teh podatkov – elektronskimi sledmi, mnogo lažje dokazovati utemeljene sume izvršitve in povezovanja pri izvrševanju navedenih kaznivih dejanj. Z navedenimi dejstvi ocenjujemo nujnost obdelave/uporabe podatkov PNR za doseg našega ustavno dopustnega cilja, saj njihova uporaba pomeni bistveno nižjo stopnjo posega v zasebnost posameznika, kot to terjajo posebni policijski ukrepi, ki se jih policija poslužuje pri tradicionalnem pristopu preiskovanja hujših in organiziranih oblik kriminalitete.

4.5 Test sorazmernosti v ožjem smislu

Preostane nam še zadnji test, in sicer sorazmernost v ožjem smislu, pri čemer bomo ugotavljali ali je poseg v informacijsko zasebnost posameznika v razumnem ravnovesju do javne koristi v obliki večje stopnje varnosti, ki jo lahko zagotovimo z obdelavo/uporabo podatkov PNR.

Iz ustavnega načela (*U-I-25/95, Ur.l. št. 5/98*), »da se pravica do zasebnosti za posameznika lahko konča samo takrat in tam, kjer kolidira z zakonsko izkazanim močnejšim interesom drugih«, lahko iz 2. odstavka 8. člena EKČP ugotovimo, da je javni oblasti, poleg prepovedi, izjemoma dovoljeno vmešavanje v izvrševanje pravice do zasebnosti. Med te izjeme pa prav gotovo prištevamo tudi obdelavo/uporabo podatkov o potnikih za zagotavljanje »državne varnosti, javne varnosti....., zato, da se prepreči nered ali zločin, da se zavaruje zdravje ali morala ali da se zavarujejo pravice in svoboščine drugih ljudi«.

V poglavju ustavno pravnega vidika zadevnih človekovih pravic (*glej stran 58*) smo navedli primer odločitev Ustavnega sodišča RS (*Up-7/98, z dne 30.9.1998*), ki se je v primeru kolizije med varnostjo ljudi na eni strani in pravico do zasebne lastnine na drugi strani, odločilo v javno korist ljudi do varnosti. Enako je Komisija ravnala, ko je na očitek o posegu v zasebno življenje, zavrnila tudi v primerih obveznosti privezovanja z varnostnim pasom, obvezne uporabe prehodov za pešce v prometu, varnostnih ukrepov zaradi varstva delavcev, odvzema voznškega dovoljenja, kot tudi glede uživanja alkohola in mamil, ipd. Ti ukrepi so bili utemeljeni z varstvom posameznikov, vendar je bila pravica do varnosti postavljena v prioritetni položaj nasproti pravici do zasebnosti. Ta ustavno sodna praksa, ki sicer ni obvezen pravni vir, vendar pa ima v luči zagotavljanja enakosti pred zakonom (*glej 14. člen Ustave RS*) podobno moč, kot jo imajo ostali formalni pravni viri. Ta »argument precedensa« je pomemben predvsem zaradi zagotavljanja pravne varnosti, saj omogoča izvedbo načela predvidljivosti odločanja, in sicer enakost odločanja v istovrstnih primerih. S to ugotovitvijo test sorazmernosti v ožjem pomenu nadaljujemo v smislu ugotavljanja ali je teža morebitnih posledic posega v informacijsko zasebnost posameznika

uravnotežena z učinki javne varnosti, ter varnosti ljudi in njihovega premoženja, ki bodo zagotovljene z navedenim posegom.

Po ustaljeni ustavnosodni presoji pomeni vsako zbiranje in obdelava osebnih podatkov poseg v t.i. informacijsko zasebnost posameznika. Kljub temu ta človekova pravica ni absolutna, zato se mora posameznik zavedati te omejitve in dopustiti posege v tovrstno obliko zasebnosti zaradi prevladujočega splošnega interesa in ob izpolnjevanju ustavno določenih pogojev. Kot nadalje izhaja iz sodne prakse, je boj proti mednarodnemu terorizmu in drugim hujšim oblikam kaznivih dejanj, z namenom vzdrževanja javne in mednarodne varnosti v splošnem interesu Unije⁵⁷. Ta ustavno dopustni cilj bomo v obravnavanem primeru zagotavljali s podatki o potnikih (PNR). Ti podatki so vsekakor v tesni povezavi z varnostjo, ki jo želimo kot človekovo pravico zavarovati. Iz izkušenj držav članic, ki podatke PNR že uporabljajo za preprečevanje kriminalitete izhaja, da je z ustrezno analitično obdelavo podatkov PNR mogoče dovolj podrobno opredeliti specifične oziroma ponavljajoče potovalne vzorce teroristov in storilcev drugih hudih kaznivih dejanj. Ti vzorci so z vidika modusa operandi kriminalcev, predstavljali njihove zanimive odklone od običajnega vzorca večine potnikov. Temeljite analize podatkov bodo služile za oblikovanje ter posodabljanje nediskriminatornih ocenjevalnih meril, ki bodo na takšne storilce uspešno predhodno opozarjala. Natančnost ocenjevalnih meril je odvisna od širokega spektra podatkov PNR. Z naborom podatkov PNR, ki smo ga navedli v naši presoji vplivov na zasebnost, v podpoglavju »Vsebina zbranih podatkov« ocenjujemo, da je mogoče izdelati zelo natančna ocenjevalna merila. Gre za nabor manj občutljivih podatkov, ki so vključeni v mednarodno priznan PNR.GOV standard, ki ga priporočajo mednarodne organizacije IATA, WCO in ICAO.

Zbiranje podatkov PNR se bo izvajalo za lete znotraj EU, za mednarodne komercialne lete iz tretjih držav na ali preko ozemlja Slovenije oziroma obratno, ter za čarterske polete. Vendar pa ta podatkovna zbirka ne bo predstavljala zgolj preventivno zbiranje ter uporabo podatkov o potnikih v letalskem prometu, temveč gre v osnovi za njihovo sprotno preverjanje skozi transparentna in nediskriminatorna ocenjevalna merila z namenom odkritja neznanih (potencialnih) storilcev terorističnih in drugih hudih kaznivih dejanj, ter skozi ustrezne nacionalne podatkovne evidence, vključno z mednarodnimi, ki so ali če bodo vzpostavljene na podlagi nacionalnega, mednarodnega ali prava EU, in sicer z namenom odkritja iskanih oseb, ali oseb zoper katere so razpisani zakoniti ukrepi, s katerimi organi odkrivanja in pregona merijo na kazenski pregon storilcev hudih kaznivih dejanj ali so za osebe napisane operativne informacije, povezane s terorističnimi ali drugimi hujšimi kaznivimi dejanji. Podatki PNR namreč pri iskanju oseb in predmetov niso uporabni, saj gre pri tem za iskanje znanih storilcev oziroma operativno zanimivih oseb, ki so že izvedle kaznivo dejanja, ali ga izvajajo, ali pa se nanj pripravljajo, in je razpis ukrepov zoper te osebe nujno potreben za izvedbo kazenskega pregona. Ti ukrepi se razpisujejo v nacionalne in mednarodne evidence (FIO, SIS II, Interpol), ki se za razliko od evidence podatkov PNR uporabljajo za preverjanja identitet znanih oseb, ki so že osumljene storitve ali poskusa storitve kaznivih dejanj. V tem pa je tudi bistvena razlika, ki podatke PNR ločuje od obstoječih orodij. Prav zato predstavlja kombinirana uporaba obeh pristopov še

57 Glej sodbo Kadi in Al Barakaat International Foundation / Svet in Komisija, C.402/05 P in C. 415/05 P, EU:C:2008:461, točka 363, sodbo Al-Aqsa / Svet, C.539/10 P in C.550/10 P, EU:C:2012:711, točka 130), ter sodbo Tsakouridis, C.145/09, EU:C:2010:708, točki 46 in 47).

učinkovitejši, hitrejši in bolj celovit pristop policije pri odkrivanju in prijemanju storilcev kaznivih dejanj z manjšimi škodljivimi posledicami za ljudi in njihovo premoženje.

V računalniški aplikaciji se bodo po navedeni avtomatizirani obdelavi podatkov PNR prikazale le osebe, ki bodo ustrezale tem preverjanim kriterijem. Ostali »neuparjeni« avtomatsko obdelovani podatki PNR operaterju ne bodo vidni, saj se bodo takoj po tej obdelavi v sistemu shranili v prvotni kriptirani obliki in se bodo po zaključku časa hrambe podatkov avtomatično nepovratno izbrisali. S tem ta ukrep ne posega v pretežni meri v pravice državljanov, ki z namenom zbiranja podatkov nimajo nobene zveze. Nasprotno, uporaba podatkov PNR bo osredotočena le na storilce hujših kaznivih dejanj, oziroma na tiste osebe, ki na podlagi analize podatkov predstavljajo višjo stopnjo tveganja za javno varnost in varnost ljudi. Preostalem potnikom bi ta selektivni pristop, poleg višje stopnje varnosti, omogočal tudi nemoteno koriščenje svoboščine do prostega pretoka oseb v Schengenskem območju, ter hitrejša postopke mejne kontrole na letališčih.

Neposreden dostop podatkov PNR bodo imeli le uslužbenci SI enote za informacije o potnikih, ki jih bodo na upravičeno zahtevo lahko posredovali le vnaprej določenim policijskim enotam, državnim organom in drugim EU institucijam, ki imajo pooblastila za preprečevanje, odkrivanje, preiskovanje in pregon terorističnih in drugih hudih kaznivih dejanj. Iz tega namena uporabe podatkov PNR so vsekakor razvidne varovane vrednote, zaradi katerih se na drugi strani posega v informacijsko zasebnost posameznikov. Kot je že bilo predhodno omenjeno, so te vrednote po ustavno sodni presoji v splošnem interesu EU.

S sorazmernostjo v ožjem pomenu je tesno povezan tudi rok hrambe podatkov, ki mora biti določen v razumni povezavi z dosego ustavno dopustnega cilja. Ta vidik smo v tem dokumentu že podrobno utemeljili (*glej strani 19 – 20 in 23*). V tej povezavi je pomembno zopet poudariti naš predlog za sprejetje nacionalne zakonske podlage za pridobitev, hrambo, analizo in izmenjavo podatkov o potnikih, s klavzulo o časovni omejitvi (»sunset clause«) le-te na 5 let. To je vsekakor dodatno jamstvo za zagotavljanje sorazmernosti v časovnem vidiku.

V luči varovanja informacijske zasebnosti je neselektivnost pri zbiranju in hrambi podatkov ključni dejavnik, saj se s tem v prevladujočem delu posega v informacijsko zasebnost tistih (nedolžnih) potnikov, ki z namenom obdelave podatkov nimajo nobene zveze. Neselektivnost zbiranja in hrambe podatkov je potrebno sorazmerno omejiti z zagotovitvijo enakovrednih protiuteži oziroma učinkovitih varovalk, ki smo jih predhodno navedli (*glej podpoglavje 2.4*). Kot pomembna protiutež neselektivnosti je prav gotovo selektivna oziroma usmerjena uporaba teh podatkov zgolj na »rizične« posameznike izmed celotne populacije letalskih potnikov, ki se ujemajo z določenimi transparentnimi kriteriji. S tem ta ukrep neposredno ne posega v pretežni meri v pravice državljanov, ki z namenom zbiranja podatkov nimajo nobene zveze.

Z navedenimi ustavnimi odločitvami in lastnimi argumenti utemeljujemo, da je poseg v informacijsko zasebnost posameznika v razumnem ravnovesju do javne koristi v obliki večje stopnje varnosti, ki jo lahko zagotovimo z obdelavo/uporabo podatkov PNR. Obdelava teh podatkov, uvedena na dosleden in transparenten način, z določenimi že navedenimi elementi možnega stalnega nadzora, nedvomno predstavlja sorazmeren poseg v pravico do informacijske zasebnosti posameznika iz vidika katastrofalnih škodljivih posledic večjih razsežnosti zaradi

neodkritih in nepreprečenih terorističnih in drugih hujših kaznivih dejanj. V tem pogledu torej ne bi smelo biti dvoma o sami sorazmernosti ukrepa, saj se »jeziček« na tehtnici tehtanih pravic premakne v prid varnosti, ki predstavlja javno korist.

5 PREDLOG PRAVNE UREDITVE UPORABE PODATKOV PNR

Skozi samo obravnavo tematike smo opisno že na nekaj mestih skušali nakazati nekatere možne spremembe za pravno ureditev obravnavanega pooblastila, zato bi na tem mestu strnili le nekaj sugestij. Ustrezna interpretacija že citiranega 148. člena ZKP, ki predstavlja vrsto generalnega pooblastila policiji za pregon in odkrivanje storilcev kaznivih dejanj in zbiranja dokazov o njih, zaradi uspešne izvedbe kazenskega postopka, bi lahko bila ustrezno vodilo za uvedbo predlaganega pooblastila.

Obravnavano pooblastilo bi bilo potrebno ustrezno ovrednotiti v Zakonu o nalogah in pooblastilih policije, kjer bi bilo potrebno v poglavju zbiranja in obdelave podatkov, to področje ustrezno določiti, in sicer v 112. členu z abstraktno razlago obdelave podatkov PNR, ter z določitvijo nove evidence v 123. členu. Postopek obdelave/uporabe podatkov PNR bi podrobno predpisoval podzakonski akt ministra, pristojnega za notranje zadeve. Glede na to, da bo za to področje pristojna specializirana SI enota za informacije o potnikih (OOVT CKOD UKP), bi bilo smiselno pristojnost te enote predstaviti še v Zakonu o organiziranosti in delu v policiji, podobno kot za Europol in NPU UKP. Poleg teh sprememb bi bile potrebne še ustrezne dopolnitve 84.a člena Zakona o letalstvu.

6 ZAKLJUČEK

V primeru hujših groženj nacionalni varnosti, kot je npr. terorizem, mora potreba po varnosti v prvi vrsti, sprožiti hiter in brezkompromisen odziv napadene države. Nemalokrat smo takrat priča ad-hoc rešitvam, pogosto tudi s premalo umerjenim širjenjem pooblastil varnostnim organom, s katerimi država (*bote ali nebote*) vse globlje posega v TSČP posameznika. Najočitnejši primeri tovrstnih ravnanj se kažejo po terorističnih napadih v Združenih državah Amerike. Končno tudi v evropskem prostoru v Veliki Britaniji, Španiji, Franciji in nedavno tudi na Danskem. V strahu pred ponovnimi okrutnimi terorističnimi napadi, že državljani sami manifestirajo svoje zahteve, v nadaljevanju pa tudi brezpogojno odobravajo večino sprejetih in napovedanih protiterorističnih ukrepov, ki jih vlade sprejemajo pod takšnimi pritiski. V tem se eni bolj, drugi manj zavedajo višje stopnje restriktivnih posegov v njihovo bodočo svobodo. Teroristični napadi med ljudmi sejejo preplah; eksistenčni strah za življenje pa največkrat izzove neracionalnost. Slednja pa največkrat vodi k nepretehtanim odločitvam. Temeljna potreba po varnosti postane primarna in preraste človekove sekundarne težnje. V izsiljeni izbiri najboljše med slabimi rešitvami se ljudje takrat brez oklevanja odrekujejo določenim že pridobljenim, samoumevnim pravicam. In takrat pride na vrsto država, ki je v skladu z družbeno pogodbo, dolžna odigrati svojo temeljno vlogo. Zagotoviti ustrezno varnost, seveda premišljeno, racionalno in v skladu z vsemi načeli pravne države.

V izogib takšnim pojavom, je nujno reagirati pravočasno, z zadostnimi sredstvi in sorazmernimi ukrepi, s čimer bo mogoče storilce hudih kaznivih dejanj vsaj dohajati če že ne prehiteti. S

predlaganim nadzorom in torej selektivnim omejevanjem njihovih osebnostnih pravic jim povečujemo faktor tveganja v izvrševanju kriminalnih aktivnosti. Eno od tovrstnih primernih orodij bi bilo prav legalizirano pridobivanje in obdelava podatkov PNR. Kot že prebrano so določeni organi pregona drugih držav, ki te podatke že uporabljajo, prepoznali za učinkovito orodje za boj proti hujšim oblikam kriminalitete s čezmejnimi posledicami. Uporabnost teh informacij na makro nivoju predstavljajo kot mehanizem uspešnejšega zagotavljanja notranje varnosti skupnosti držav članic. Na mikro nivoju za zagotavljanje neposredne javne varnosti ter varnosti ljudi in premoženja posamične države članice. Na sistemskem nivoju pa kot učinkovito orodje za izdelavo in izmenjavo obveščevalnih informacij, ki bodo služile preprečevanju terorizma in drugih hujših kaznivih dejanj. Ugotovili smo že, da enega od temeljnih elementov neidentificiranih storilcev obravnavanih kaznivih dejanj, predstavljajo prav mednarodna letalska potovanja.

Javna dilema »svoboda ali varnost« oziroma koliko svobode za ceno varnosti je torej po strokovni plati zgrešena. V tem okviru si je namreč pomembno zastaviti vprašanje, kako zagotoviti optimalno razmerje med svobodo in varnostjo posameznika v družbi. Za zagotavljanje obeh vrednot sta odgovorni tako civilna družba, kot tudi demokratična država. Zaradi optimalnega konsenza je nujno nenehno usklajevanje prioritet glede stališč in vrednot ter vzpostavitev medsebojnega zaupanja.

Razbrali smo, da Slovenija na lestvicah, grafih in ocenah ogroženosti sicer (še) ne izstopa, niti za sedaj ni ciljna država. Vendarle pa geografsko sodimo v tranzitno območje, preko katerega potuje veliko tovrstnih oseb. Aktivno delovanje države, je t.i. pozitivna obveznost, zavarovati lastne državljane pred posledicami terorističnih dejanj in preprečevanja le teh. Skladno z lastno prakso v primerih ko gre za tako hude grožnje, ESČP tolerira določene manjše posege, oziroma omejitve pravic v skladu s EKČP. Vendar mora biti izpolnjen temeljni pogoj, zagotovitev ustrezne sodne kontrole nad samo uporabo ukrepov, ki kakorkoli posegajo v TSČP. Jasno morajo biti izvedeni ukrepi, proporcionalni samemu cilju, kateremu država, oziroma njen organ sledi. Takšni ukrepi morajo torej temeljiti na nedvoumnih določbah, nepristransko oceno nad izvedenimi ukrepi pa zagotavlja od zunanjega neodvisnega organa izvedena kontrola⁵⁸.

Uporabno vrednost podatkov PNR že dokazujejo potovalne agencije, preko katerih lahko letalski potniki rezervirajo letalske vozovnice. Z obdelavo osebnih podatkov, ki jim jih pošljejo potniki ob rezervaciji vozovnice, namreč že ocenjujejo potnike za njihove komercialne namene. Ta poseg v zasebnost se strokovni in laični javnosti ne zdi sporen, kljub temu, da se izvaja v zasebno korist gospodarske družbe oziroma za njen profit. Na drugi strani pa se ta poseg v zasebnost dojema kot sporen, ko ga izvaja policija v javno korist, to je za zagotavljanje splošne varnosti, varnosti ljudi in njihovega življenja.

58 Povzeto po; Dunja Jandl, Problem terorizma v strasbourški sodni praksi, članek v reviji Revus, revija za ustavno teorijo in filozofijo prava, <http://revus.revues.org/1610#tocto2n5>, 16.2.2015.

7 VIRI IN LITERATURA

Publikacije in prispevki

- IP RS, Ljubljana 2014, Smernice informacijskega pooblaščenca - Presoje vplivov na zasebnost pri uvajanju novih policijskih pooblastil.
- Arhar France in ostali, Komentar Ustave republike Slovenije, Kranj, Fakulteta za podiplomske državne in evropske študije.
- Bruselj, 2.2.2011, COM(2011) 32 konč., 2011/0023 (COD), Predlog direktive evropskega parlamenta in sveta o uporabi podatkov iz evidence podatkov o potnikih za preprečevanje, odkrivanje, preiskovanje in pregon terorističnih in hudih kaznivih dejanj.
- Bruselj, 2.2.2011, SEC(2011) 133 konč., Delovni dokument služb komisije, Spremeni dokument k Predlogu direktive evropskega parlamenta in sveta o splošnem pristopu k uporabi podatkov iz evidence podatkov o potnikih, povzetek ocene učinka.
- Cerar Miro, Večrazsežnost človekovih pravic in dolžnosti, Znanstveno in publicistično središče, Ljubljana, 1993.
- Kodeks policijske etike, Ministrstvo za notranje zadeve RS, Policija, Ljubljana.
- Mekinc Janez, Evropski kodeks policijske etike - Priporočilo Rec (2001) 10. Ministrstvo za notranje zadeve RS, Policija, Ljubljana, 2003, str. 17–19.
- Pagon Milan, Policijska etika kot zvrst uporabne etike, Varstvoslovje: revija za teorijo in prakso varstvoslovja, letnik 2, št. 2 (2000), str. 158-167.
- Anžič Andrej (2002). Mednarodni terorizem – varnostni izziv in dileme, znanstveni članek, Teorija in praksa, letnik 39, številka 3, stran 454-466, Ljubljana, 2002.
- Arhar France in ostali, Komentar Ustave Republike Slovenije, Fakulteta za podiplomske državne in evropske študije, Kranj.
- Bavcon Ljubo, Varnost in človekove pravice, Zbornik - varnost in družbeno politične spremembe, stran 61-63, Ljubljana, 1990.
- Pagon Milan / Meško Gorazd / Lobnikar Branko, Etika, integriteta in človekove pravice z vidika policijske dejavnosti, Ministrstvo za notranje zadeve RS, Visoka policijsko-varnostna šola, Ljubljana, 2003.
- Delovni zvezek za praktično usposabljanje, Svet Evrope, Informacijski center za človekove, Strasbourg, 1998.
- Flander Benjamin, Svoboda in / ali varnost?, Varstvoslovje, letnik 4, št. 1, stran 86-87.
- Kirn Roman, Varovanje človekovih pravic v konfliktnih situacijah, Dignitas, letnik 3, številka 9, stran 23-27, Ljubljana, 2001.

- Klemenčič Goran, Svoboda ali varnost – zgrešena dilema!, Posvet - Varovanje človekovih pravic in svoboščin v postopkih represivnih organov, stran 33-39, Ljubljana, 2002.
- Mekinc Janez, Evropski kodeks policijske etike - Priporočilo Rec (2001) 10, str. 17–19, Ministrstvo za notranje zadeve RS, Policija, Ljubljana, 2003.
- Mill Johan Stuart, O svobodi, Ljubljana, 1994.
- Pagon Milan / Meško Gorazd / Lobnikar Branko, Etika, integriteta in človekove pravice z vidika policijske dejavnosti, Ministrstvo za notranje zadeve RS, Visoka policijsko-varnostna šola, Ljubljana, 2003.
- Švarc Dominika, Teror prava - Človekove pravice v globalni vojni proti terorizmu, Revus, letnik 4, številka 6, stran 135-148, Ljubljana, 2006.
- Bilten sodne statistike za leto 2013, Ministrstvo za pravosodje, Ljubljana, 2014.
- Evidence EUROPOL-a.

Pravni viri

- Ustava Republike Slovenije, s komentarjem.
- Kazenski zakonik Republike Slovenije.
- Zakon o kazenskem postopku.
- Zakon o tajnih podatkih.
- Zakon o letalstvu (Uradni list RS, št. 81/10, z dne 15. 10. 2010).
- Zakon o nalogah in pooblastilih policije (Uradni list RS, št. 15/13).
- Direktiva Sveta 2004/82/ES, z dne 29. aprila 2004 o dolžnosti prevoznikov, da posredujejo podatke o potnikih, Uradni list EU št. L 261/24, z 6.8.2004.
- Okvirni sklep Sveta 2002/475/PNZ z dne 13. junija 2002 o boju proti terorizmu in Okvirni sklep sveta 2008/919/PNZ z dne 28. novembra 2008 o spremembi Okvirnega sklepa 2002/475/PNZ o boju proti terorizmu.
- Okvirni sklep Sveta 2002/584/PNZ z dne 13. junija 2002 o evropskem nalogu za prijetje in postopkih predaje med državami članicami.

Judikati

- Odločitev US, U-I-25/95, Ur. l. št. 5/98.
- odločitev US, št. U-I-25/95, Ur. L. št. 5/98.
- odločitev U-I-25/95, Ur.l. št. 5/98)

Razvojno usmerjevalni dokumenti

- Resolucija o strategiji nacionalne varnosti Republike Slovenije, Uradni list RS št. 27/2010.

- Resolucija o nacionalnem programu preprečevanja in zatiranja kriminalitete za obdobje 2012–2016 (ReNPPZK12-16), Uradni list RS, št. 83/2012 z dne 6. 11. 2012.
- Resolucija o dolgoročnem razvojnem programu policije do leta 2022 EVA 2011-1711-0026.
- Stockholmski program – Odprta in varna Evropa, ki služi državljanom in jih varuje, EU Uradni list C 115 , 04/05/2010 str. 0001 – 0038.
- Predlog DIREKTIVA EVROPSKEGA PARLAMENTA IN SVETA o uporabi podatkov iz evidence podatkov o potnikih za preprečevanje, odkrivanje, preiskovanje in pregon terorističnih in hudih kaznivih dejanj (SEC(2011) 132 konč.)(SEC(2011) 133 konč.) <http://eur-lex.europa.eu/legal-content/SL/TXT/?qid=1417212019249&uri=CELEX:52011PC0032>.
- Europolove ocene ogroženosti OCTA 2011-2013 in SOCTA 2014-2017 – Serious Organized Crime Threat Assessment.
- Situacijsko poročilo agencije Europol o teroristični dejavnosti v EU TE-SAT 2014, European Police Office, 2014.
- Interpolovo analitično poročilo o potovanjih tujih borcev v Sirijo, Travel routes into Syria used by Foreign Terrorist Fighters, Interpol, november 2014.