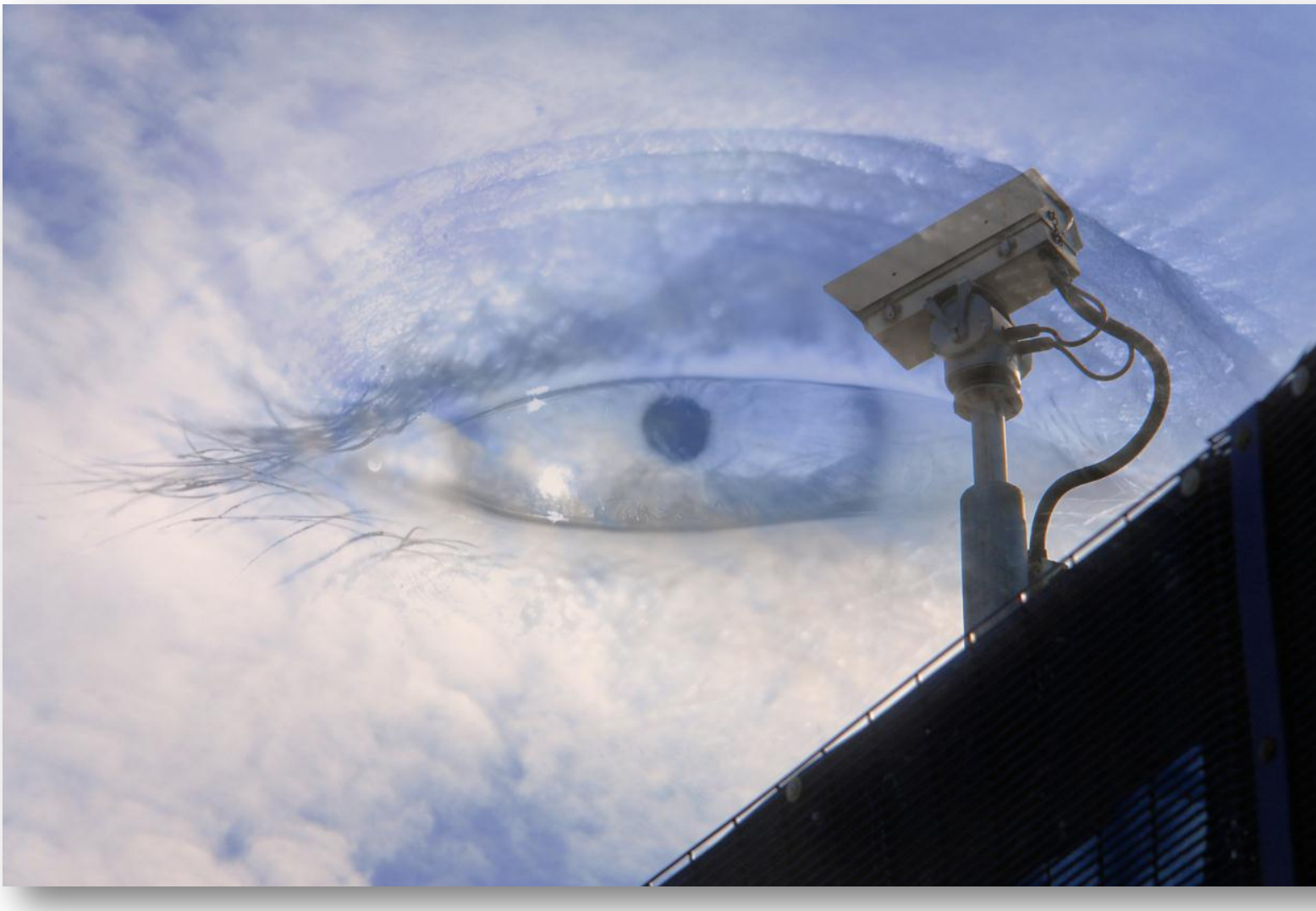

Presoje vplivov na zasebnost pri uvajanju novih policijskih pooblastil

Smernice Informacijskega pooblaščenca

INFORMACIJSKI POOBLAŠČENEC

Namen dokumenta:	Namen smernic je organom odkrivanja in pregona kaznivih dejanj ponuditi orodje, s katerim lahko pred uvajanjem novih pooblastil, zlasti glede uporabe tehničnih sredstev, izdelajo presojo vplivov na zasebnost in tako opravičijo nujnost, primernost in učinkovitost ter sorazmernost novih pooblastil, omogočijo javni diskurz o novih pooblastilih ter pravočasno predvidijo tveganja in varovalke za neupravičene posege v človekove pravice.
Ciljne javnosti:	Organi odkrivanja in pregona kaznivih dejanj, Državna tožilstva, Ministrstvo za pravosodje, zainteresirana javnost
Status:	javno
Verzija:	1.0
Datum izdaje:	14. 1. 2014
Avtorji:	Informacijski pooblaščenec
Ključne besede:	Smernice, policijska pooblastila, tehnična sredstva, zasebnost, varstvo osebnih podatkov, presoje vplivov na zasebnost, sorazmernost, test sorazmernosti.

KAZALO

O SMERNICAH INFORMACIJSKEGA POOBLAŠČENCA

Namen smernic IP je podati skupne praktične napotke za upravljavce zbirk osebnih podatkov (OP) na jasen, razumljiv in uporaben način in s tem odgovoriti na najpogosteje zastavljena vprašanja s področja varstva osebnih podatkov, s katerimi se srečujejo posamezni upravljavci zbirk OP. S pomočjo smernic naj bi upravljavci dobili priporočila, kako naj v praksi zadostijo zahtevam Zakona o varstvu osebnih podatkov (Uradni list RS, št. 94/07 – uradno prečiščeno besedilo; v nadaljevanju ZVOP-1).

Pravno podlago za izdajo smernic Pooblaščencu daje 49. člen ZVOP-1, ki med drugim določa, da Pooblaščenec daje neobvezna mnenja, pojasnila in stališča o vprašanjih s področja varstva osebnih podatkov in jih objavlja na spletni strani ali na drug primeren način ter pripravlja in daje neobvezna navodila in priporočila glede varstva osebnih podatkov na posameznem področju.

Oglejte si tudi:

- Mnenja IP: http://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/
- Brošure IP: http://www.ip-rs.si/publikacije/prirocniki/

Smernice IP so objavljene na spletni strani: http://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/smernice/

POVZETEK

Smernice Informacijskega pooblaščenca za presojo vplivov na zasebnost pri uvajanju novih policijskih pooblastil predstavljajo metodološki okvir za preudarno, smiselno in legitimno uvajanje novih policijskih pooblastil, zlasti tistih s tehnološkim značajem. Kot poudarjamo, je bil veljavni Zakon o kazenskem postopku v zadnjih desetih letih deležen številnih novel sprememb in dopolnitev (trenutno se piše že trinajsta), pri čemer so bila dodana številna nova policijska pooblastila. Žal pa policija predlogov novih členov ni vedno pospremila tudi z ustrezno obrazložitvijo, iz katere bi nedvoumno izhajale nujnost, primernost in učinkovitost ter sorazmernost predlaganega ukrepa. Prevečkrat je bila okrnjena tudi javna razprava o uvajanju novih policijskih pooblastil. Posledice so težave z rabo ukrepov v praksi (izločitvijo zbranih dokazov), neredko tudi v velikih, pomembnih in medijsko zelo odmevnih primerih ter občasno izrazit odpor splošne in strokovne javnosti pri uvajanju novih pooblastil.

Smernice postavljajo večfazni metodološki okvir za predhodno presojo vplivov ukrepa na zasebnost (angl. Privacy Impact Assessment, PIA). **Prva faza** zajema oceno stanja na področju urejanja, utemeljitev potrebe po novih pooblastilih, ter obrazložitev, kako točno naj bi nova pooblastila zadovoljila te potrebe. Pri tem je ključno, da je novo pooblastilo, posebej ko gre za tehnično sredstvo, tudi dovolj natančno opredeljeno. **V drugi fazi** se izdela analize vsakovrstnih tveganj v zvezi s posegi v ustavne pravice do zasebnosti in varstva osebnih podatkov, zlasti glede učinkovitosti ukrepa oz. izvajanja ukrepa (zbiranja podatkov, zavarovanja podatkov, uporabe, uničenja podatkov), ter izvede primerjavo z ureditvami v tujini. Pri tem je ključno, da se iz tuje prakse prenesejo ne le ideje o tem, kaj vse je mogoče, ampak tudi že izoblikovane in utemeljene pravne omejitve ter dejanske izkušnje pri rabi pooblastil. **V tretji fazi** se tako identificirana tveganja upravlja z ustreznimi varovalkami (kavtelami), npr. sodno avtorizacijo, višjim dokaznim standardom, minimizacijskimi postopki, zapisniki. **V četrti, sklepni fazi**, se na podlagi vseh zbranih informacij izvede test sorazmernosti, kot ga že poznamo v naši ustavnosodni praksi. V kolikor predlagani ukrep ne zadosti testu, ker bodisi ni primeren za dosego zadanega cilja, bodisi pri tem ne bo učinkovit, ali ker preprosto preveč posega v pravice osumljenca ali drugih oseb, bo o takšnem ukrepu kazalo še enkrat razmisliti. Šele na podlagi uspešno prestanega testa sorazmernosti velja pripraviti zakonsko besedilo predlaganega ukrepa. Tako bomo namreč lahko prepričani, da bo ukrep učinkovit, zakonit, uporabljiv pred sodišči, ter tudi sprejet s strani javnosti.

Sama izvedba presoje vplivov na zasebnost (PIA) bi potekala po sledečem modelu:

1. Predlagatelj (Policija / MNZ) pripravi PIA po predlaganem metodološkem okviru, ter jo pošlje v mnenje IP.
2. IP pregleda PIA in poda svoje pripombe.
3. Predlagatelj se opredeli do pripomb IP ter po potrebi dopolni PIA.
4. Predlagatelj na podlagi dopolnjene PIA pripravi predlog sprememb zakonodaje ter oboje pošlje Ministrstvu za pravosodje, skupaj z označbo, ali je predlog vsebinsko že usklajen s PIA in pripombami IP.
5. Gradivo se naprej obravnava po ustaljenih postopkih medresorskega usklajevanja.

Opomba: Smernice so primarno namenjene policiji, služijo pa lahko tudi drugim organom, ki sodelujejo pri pripravi predpisov s področja kazenskega prava, npr. Ministrstvu za pravosodje, Državnemu tožilstvu, sodiščem.

UVOD

Pri uvajanju policijskih pooblastil je treba izhajati iz dejstva, da je, poenostavljeno, kazensko pravo namenjeno omejevanju države pri posegih v pravice posameznikov, še zlasti pa policije kot njenega najbolj značilnega predstavnika. Od francoske revolucije naprej nasproti popolni policijski samovolji stojijo v ustavah zapisane in v kazenski zakonodaji konkretizirane temeljne človekove pravice in svoboščine, od enakosti pred zakonom, prepovedi mučenja, varstva osebne svobode, domneve nedolžnosti, do človekovega dostojanstva in zasebnosti. Varstvo posameznika v razmerju do policije je eden ključnih pokazateljev stopnje demokratičnosti države, zato je nujno, da so vsa policijska pooblastila sorazmerna s posledicami posegov v človekove pravice, ter da so predpisi, ki jih urejajo, jasni, določni in predvidljivi[1].

Pooblaščenec se je v kar nekaj nedavnih primerih soočil s tem, da organi pregona ne analizirajo in ne utemeljijo svojih predlogov za dodelitev novih pooblastil oziroma sprememb obstoječih (npr. pri predlogih za spremembe ZKP in ZEKom), s čimer je bil v znatni meri okrnjen javni diskurz o uvajanju novih pooblastil.

ZAKAJ METODOLOŠKI OKVIR ZA ANALIZO NOVIH POOBLASTIL?

Stanje na področju uvajanja novih pooblastil organov pregona je zaskrbljujoče. V zadnjih nekaj letih smo bili priča že skoraj simptomatičnemu stihijskemu uvajanju novih pooblastil ob odsotnosti uporabe primerne metodologije, ki bi:

- omogočila izvedbo presoje vplivov na zasebnost,
- upravičila nujnost, primernost in učinkovitost ter sorazmernost uvajanja novih pooblastil,
- analizirala tveganja glede uvajanja novih pooblastil,
- celostno obravnavala identificirana tveganja,
- ponudila primerne kriterije za izvedbo naknadnih analiz učinkov.

Običajno je k uvajanju novih pooblastil vodila **dostopnost neke določene nove tehnologije** na trgu (npr. brezpilotni letalniki, IMSI lovilci), oziroma **zmanjšanje učinkovitosti organov pregona zaradi uporabe novih tehnologij na strani osumljencev oz. preiskovancev** (npr. večja uporaba šifriranih komunikacij s strani storilcev kaznivih dejanj, uporaba predplačniških SIM kartic ipd.). Temu je običajno sledila takojšnja priprava pravnih podlag, ki naj bi z novimi pooblastili policiji nevtralizirale navidezno prednost potencialnih storilcev kaznivih dejanj pri rabi informacijskih tehnologij. **Predhodne analize nujnosti, primernosti in učinkovitosti ter sorazmernosti** takih pooblastil praviloma niso bile izvedene, **naknadne analize pa ne predvidene**. Obrazložitve so bile **skope**, pogosto oprte na neprepričljive **argumente**[2] in včasih celo zavajajoče[3].

---

[1] Logar, Jure: Občutljivo vprašanje uvajanja novih policijskih pooblastil. Ljubljana: GV Založba. Pravna praksa št. 5/2013.

[2] Obrazložitev ob uvajanju obvezne hrambe podatkov v prometu elektronskih komunikacij (Obrazložitev sprememb ZEKom-A, str. 88): »*Glede na dejstvo, da so morebitni dodatni stroški povezani s temeljno investicijo nadgradnje omrežne infrastrukture, da torej dodatni mediji za hrambo v tem pogledu ne predstavljajo večjega stroška, po drugi strani pa daljše obdobje hrambe pomembno prispeva k učinkovitosti pregona in izboljšuje možnosti pristojnih organov v zvezi z njim, je kot rok hrambe predlagan maksimum.*«

[3] Konec leta 2012 sta poskušali policija in SOVA spremeniti režim dostopa do prometnih podatkov, ki so jih dolžni hraniti operaterji po določbah ZEKom in sicer, da bi za pridobitev podatka o identiteti komunicirajočega, namesto odredbe sodišča zadostoval pisni zahtevek državnega organa (obrazložitev sprememb 7. odstavka 166. člena

Nekateri predlogi so bili zavrnjeni v medresorskem usklajevanju, drugim je uspelo priti do obravnave v Državnem zboru, npr. predlog novele Zakona o kazenskem postopku ZKP-K in novi Zakon o elektronskih komunikacijah – ZEKom-1[4]. Zadnja predloga sta dobila potrebno parlamentarno večino,[5] čeprav bi si zaslužila enako usodo kot prejšnji predlogi. Težava ni samo v izrazito vprašljivi sorazmernosti predlaganih pooblastil, temveč tudi v tem, da je zaradi skoposti obrazložitev predlogov, ki organom in javnosti izven pripravljavca in predlagatelja predpisa služijo skoraj kot edina opora pri razumevanju potrebnosti urejanja nekega vprašanja, javna in strokovna[6] razprava o novih in novih pooblastilih zelo otežena.

Izvrševanje obravnavanih policijskih pooblastil predstavlja tudi posege v pravico do zasebnosti in pravico do varstva osebnih podatkov. Prav tako ne gre spregledati, da nekatera pooblastila pomenijo posege tudi v pravico do svobode združevanja, s tem pa v pravico do svobode izražanja. Posegi v človekove pravice ali temeljne svoboščine so po ustaljeni ustavnosodni presoji dopustni, če so v skladu z načelom sorazmernosti[7]. Načelo sorazmernosti pomeni, da mora omejitev ustavnih pravic oziroma poseg vanje izpolnjevati tri pogoje[8]:

1. poseg mora biti **nujen**,[9]
2. poseg mora biti **primeren** (in s tem učinkovit) za dosego zaželenega, ustavno dopustnega cilja in
3. upoštevati je treba tudi t. i. **sorazmernost v ožjem smislu**, ki je v tem, da je pri ocenjevanju nujnosti posega treba tehtati tudi pomembnost s posegom prizadete pravice v primerjavi s pravico, ki se s tem posegom želi zavarovati, in odmeriti nujnost posega sorazmerno s težo prizadetih posledic.

Bistvo sorazmernosti je v **tehtanju**, primerjanju oziroma iskanju pravega (so)razmerja med dvema stranema, na primer med splošno varnostjo vseh prebivalcev in človekovo pravico do zasebnosti. Vsaj približno bi bilo treba opisati oba pola, ju dati na »tehtnico« in se na podlagi rezultata odločiti, ali in kako naprej. Če rezultat tehtanja ni že izkustveno povsem jasen, bi moralo biti iz gradiva oziroma obrazložitev določb jasno razvidno, zakaj je npr. pridobivanje podatkov iz komunikacijske opreme (t.j. bazne postaje) nujno, oziroma zakaj pridobivanje prometnih podatkov o posamičnem telekomunikacijskem sredstvu (t.j. mobilnem telefonu) ne zadošča več, skratka, zakaj se istega cilja ne da doseči z blažjim posegom. Prav tako bi moralo biti razvidno, kako je ta ukrep sorazmeren v ožjem pomenu. Ali je sorazmerno poseči v zasebnost vseh posameznikov, ki so se znašli na območju določene bazne postaje, zato, da bomo lahko ugotovili, ali se je na njenem območju nahajalo določeno komunikacijsko sredstvo (npr. mobilni telefon) in v katerih primerih (vselej ali le, če gre za kazniva dejanja, ki družbo najbolj ogrožajo)? Iz obrazložitve bi moralo biti razvidno, zakaj je predlagani poseg nujen in ali bo resnično primeren in učinkovit. V konkretnem primeru bi bilo tako npr. treba

---

ZEKom-1: „določba nastala kot odraz potrebe prakse, ko naj operaterji v primerih gostovanja tujega telefonskega priključka v mobilnem omrežju slovenskega operaterja, te obveze niso mogli izvršiti brez vpogleda v bazo hranjenih podatkov."

[4] Ur. l. RS, št. 109/12.

[5] Gre za 113. in 114. člen Zakona o nalogah in pooblastilih policije (ZNPPol).

[6] Informacijski pooblaščenec na podlagi 48. člena ZVOP-1 daje predhodna mnenja ministrstvom, državnemu zboru, […] drugim državnim organom o usklajenosti določb predlogov zakonov ter ostalih predpisov z zakoni in drugimi predpisi, ki urejajo osebne podatke.

[7] Glej odločbo v zadevi št. U-I-152/03 z dne 23. marca 2006, v kateri je sodišče obravnavalo klasično policijsko pooblastilo ugotavljanja identitete. Glej še odločbi v zadevah št. U-I-137/93 z dne 2. junija 1994 in U-I-290/96 z dne 11. junija 1998.

[8] Glej Odločbo Ustavnega sodišča v zadevi št. U-I-137/93 z dne 2. junija 1994.

[9] Torej da cilja ni mogoče doseči z nobenim blažjim posegom v ustavno pravico ali celo brez njega.

upoštevati, da organiziranemu kriminalu ni tuje zamenjati sto SIM kartic na teden, oziroma uporabljati aplikacij kot je npr. Skype, kar pod resen vprašaj postavi učinkovitost takšnih novih policijskih pooblastil – povsem možno je namreč, da bi šlo v praksi za pridobivanje podatkov o izključno nedolžnih osebah. Razvidna bi torej morala biti tudi primernost predlaganega ukrepa.

Policija želi uporabljati visokotehnološka sredstva za npr. identifikacijo oseb, predmetov in vozil, pri čemer je poseg v zasebnost s temi sredstvi že po sami naravi stvari bistveno večji kot pri izvajanju klasičnih policijskih pooblastilo za ugotavljanje identitete. Vendar predlagatelj pri policijskih pooblastilih v zadnjem času ni znal ustrezno obrazložiti nujnosti, primernosti in učinkovitosti ter sorazmernosti predlaganih novosti. Primarno vodilo je bila učinkovitost policije, torej argument, da je v določenih primerih policija imela »težave« pri pridobitvi »določenih podatkov«, ali da teh podatkov ni mogla dobiti »od vseh ponudnikov«, ali ne od vseh v isto kratkem, primernem roku. Obrazložitev sorazmernosti posega v pravico do zasebnosti in pravico do varstva osebnih podatkov, skupaj z ostalimi analizami, pa je izostala. Ker takšno tehtanje ni bilo opravljeno, je posledica vprašljivo sorazmeren ukrep ter tudi negativno nastrojeno usmerjeno medijsko poročanje, ki prav gotovo ni v interesu policije.

Posledice neizvajanja ustreznih analiz so pogosto dolgoročne:

- javna razprava je onemogočena ali vsaj okrnjena[10],
- naknadno ukinjanje novih pooblastil je praktično nerealno,
- sfera zasebnosti se oži,
- ob odsotnosti predhodnih analiz primernosti in naknadnih analiz učinkovitosti predpisov stroške neučinkovitosti novih pooblastil nosimo vsi[11].

Premakniti se moramo iz trenutnega stanja:

…v naslednje:

[10] Narava in kakovost javne razprave je povsem drugačna, če se razprava odvija glede splošnih izrazov, kot so „tehnična sredstva“ ali pa če so sredstva dovolj jasno opredeljena, npr. elektrošokerji, kot se je že izkazalo v preteklosti.

[11] Zelo plastičen primer predstavlja obvezna hramba podatkov v prometu elektronskih komunikacij, kjer večina študij ni pokazala pomembnega vpliva obsežne hrambe podatkov na preiskanost kaznivih dejanj. Operaterji elektronskih komunikacij so stroške obvezne hrambe zelo verjetno prelili na pleča svojih uporabnikov.

Pooblaščenec je zato pripravil smernice na temo analiziranja uvajanja oz. spreminjanja novih pooblastil organov pregona v **povezavi z določenimi tehnologijami, katerih uporaba lahko predstavlja obsežne posege v pravico do zasebnosti, ter ukrepi, ki pomenijo množično zbiranje osebnih podatkov** (npr. brezpilotni letalniki, biometrijska prepoznava obraza, avtomatska prepoznava registrskih tablic, hramba prometnih podatkov...). Smernice se prav tako nanašajo na primere **sprememb pooblastil**, če imajo le te pomemben učinek na človekove pravice (npr. spreminjanje pogojev ali obsega dostopa do prometnih podatkov, lokacijskih podatkov, drugih osebnih podatkov ipd.). Namen smernic je zato predvsem **opozoriti na pravilen metodološki pristop k uvajanju invazivnih tehnologij oziroma novih pooblastil, ki bi temeljil na pravočasni in celovitejši identifikaciji potreb, analizi nujnosti, primernosti in učinkovitosti ter sorazmernosti s posegi v zasebnost** (angl. Privacy Impact Assessment, PIA) ter presoji ustreznih varovalk in naknadnih analiz učinkov predpisov (angl. Regulatory Impact Assessment, RIA). Končni cilj smernic je predvsem učinkovito in zakonito delovanje policije, verodostojnost in uporabnost zbranih podatkov v kazenskih postopkih ter posledično večja preiskanost kaznivih dejanj - vse to ob ustreznem tehtanju med pregonom storilcev kaznivih dejanj in upoštevanjem njihovih temeljnih človekovih pravic, predvsem pa temeljnih človekovih pravic tistih oseb, ki se »ujamejo« v preiskave in postanejo tako t.i. kolateralna škoda.

Predlagano področje uporabe pričujočih smernic predstavljajo predvsem ukrepi, ki omogočajo množično zbiranje osebnih podatkov v povezavi s sodobnimi informacijsko-komunikacijskimi tehnologijami. Mednje sodijo npr. naslednji ukrepi in tehnična sredstva, ki so že v uporabi v policiji oz. je mogoče v bližnji prihodnosti pričakovati povečane pritiske po njihovi uporabi mogoče pričakovati v bližnji prihodnosti:

- brezpilotni letalniki (droni),
- biometrijska prepoznava obraza,
- avtomatska prepoznava registrskih tablic,
- obvezna hramba podatkov v prometu elektronskih komunikacij (data retention),
- naprave za dekodiranje šifriranih komunikacij (dekoderji, rootkiti, spyware),
- lažne bazne postaje, lovilci in prestrezniki v mobilnih komunikacijah (IMSI catcher ipd.),
- inteligentni video nadzor,
- varnostni roboti,
- termovizijske, infrardeče in druge kamere itd.

Hkrati opozarjamo, da je načelo sorazmernosti kot prepoved čezmernih posegov samo en – ex ante - del analize učinkov predpisov[12]. Praksa pozna tako *predhodne* kot tudi ***naknadne* analize učinkov predpisov**. Gre za poseben postopek preverjanja učinka predpisa na družbo, ki omogoča sistematično obliko presoje različnih učinkov predpisov[13]. Računsko sodišče v revizijskem poročilu »Ali v Sloveniji preverjamo učinke predlaganih predpisov na družbo[14]« meni, da bi moralo biti

[12] Resolucija o normativni dejavnosti (Ur. l. RS, št. 24/09) in revizijski poročili Računskega sodišča »Ali v Sloveniji preverjamo učinke predlaganih predpisov na družbo, 1 in 2«.

[13] Točka VI. Resolucije o normativni dejavnosti namen presoje posledic opredeljuje kot izboljšanje kakovosti novih predpisov in poenostavitev zakonodajnega urejanja ter naknadno ugotavljanje doseganja zastavljenih ciljev. Sistematično presojanje posledic predpisov, zlasti ključnih okoljskih, gospodarskih in socialnih posledic predlogov, daje tako pripravljavcu kot tudi drugim akterjem v odločevalskem procesu nujno potrebne informacije in argumente za predlaganje in sprejem odločitev na normativni ali drugih ravneh odločanja.

[14] Dostopno na: http://www.rs-rs.si/rsrs/rsrs.nsf/I/K7AAECFAFA8DFD535C1257A62001C1180

spremljanje izvajanja predpisov stalna praksa, saj bi se tako lažje pravočasno odzvali na spremenjene okoliščine.

Kakšne koristi naj bi policija imela od izvajanja presoj vplivov na zasebnost?

1. Policija bo predloge za spremembe ali nova pooblastila lahko podprla z izvedenimi analizami in izkazano nujnostjo, primernostjo in učinkovitostjo ter sorazmernostjo pooblastil in tako dosegla **legitimnost** predlaganih ukrepov v smeri ciljev, ki jih zasleduje.
2. Sprejem novih pooblastil bo deležen manj **negativnih odzivov** splošne in strokovne javnosti, kot se je zgodilo v nekaj predhodnih primerih.
3. Izvedene presoje vplivov na zasebnost lahko pripomorejo k hitrejšemu, zanesljivejšemu **pridobivanju odredb** in **uporabnosti** pridobljenih dokazov v kazenskih postopkih ter posledično vplivajo na **večjo preiskanost** kaznivih dejanj.

Širše družbene koristi izvajanja predlaganih analiz pa vključujejo:

1. **Transparentnost** uvajanja policijskih pooblastil z omogočanjem javne razprave.
2. **Legitimnost** in **podlage za naknadno vrednotenje** sprejetih policijskih pooblastil.
3. Večjo **uravnoteženost** policijskih pooblastil in temeljnih človekovih pravic.

METODOLOŠKI OKVIR ZA ANALIZO NOVIH POOBLASTIL

KAJ JE PRESOJA VPLIVOV NA ZASEBNOST?

Presoja vplivov na zasebnost (v nadaljevanju PIA) 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. Tovrstne presoje so bolj uveljavljene v okoljih, kjer je normativno in institucionalno večji poudarek na varstvu zasebnosti (angl. privacy) in ne toliko na varstvu osebnih podatkov (angl. data protection). Presoje vplivov na zasebnost so tako pogosto uporabljeno (in včasih tudi obvezno) orodje pri snovalcih zakonodaje, politik in projektov v Kanadi, Avstraliji in ZDA, počasi pa si utirajo pot tudi v evropskem prostoru, kjer je večji institucionalni poudarek na varstvu osebnih podatkov. Uporabljajo se tako v javnem kot v zasebnem sektorju. Kjerkoli so bile uvedene, so se tudi uveljavile in obstale.

PIA temelji na **sistematični in pravočasni identifikaciji tveganj**, s katerimi se lahko ta tveganja lažje odpravi, zmanjša ali sprejme. Z izvedbo PIA in spoštovanjem načela vgrajene zasebnosti (angl. *privacy by design*) se lahko tudi izognemo t.i. »function creep« pojavu, ko se podatki primarno zberejo za določen namen, s časom pa se začnejo uporabljati za druge namene, s strani drugih, prej neznanih obdelovalcev in uporabnikov.

Poznamo notranjo in zunanjo[15] PIA, obe pa se na bolj neformalni ravni že uporabljata tudi pri nas. Interno PIA izvede upravljavec osebnih podatkov sam, pri zunanji pa gre bodisi za najem zunanjega

[15] Govorimo lahko tudi o kombinaciji notranjih in zunanjih PIA, kjer sodelujejo različni deležniki.

svetovanja ali pa za posvet pri pristojnem organu za varstvo osebnih podatkov – Informacijskemu pooblaščencu. Ta izdaja neobvezna pisna mnenja, prav tako pa obstaja možnost posvetovanja s strokovnjaki Informacijskega pooblaščenca pred uvedbo projekta, kjer obstajajo večja tveganja z vidika varstva osebnih podatkov. Pooblaščenec prav tako daje in objavlja predhodna mnenja državnim organom ter nosilcem javnih pooblastil o usklajenosti določb predlogov predpisov z zakoni in drugimi predpisi, ki urejajo osebne podatke, kar se čedalje bolj tudi uveljavlja in upošteva.

Pričujoče smernice so namenjene predvsem interni izvedbi PIA, katere rezultat naj bi pristojni nato posredovali v mnenje Pooblaščencu.

KATERA SO TEMELJNA NAČELA PIA?

Temeljna načela PIA gradijo na temeljnih načelih varstva osebnih podatkov:

Zakonitost

Načelo zakonitosti pomeni, da morajo biti splošna pravila obdelave osebnih podatkov vnaprej in določno predpisana z zakonom. Zakonitost obdelave osebnih podatkov konkretno pomeni, da se osebni podatki v Republiki Sloveniji (v skladu z 2. odstavkom 38. člena Ustave Republike Slovenije) lahko obdelujejo le v skladu z zakonom. ZVOP-1 za **javni sektor** še posebej strogo določa, da se osebni podatki lahko obdelujejo le, če obdelavo osebnih podatkov in osebne podatke, ki se obdelujejo, določa zakon. Izjeme glede obdelave neposredno na podlagi privolitve posameznika, ali celo brez privolitve, so ozke, in v zvezi z nalogami, ki so predmet tega dokumenta, praviloma tudi ne bodo prišle v poštev.

Področni zakon, npr. ZKP, ZNPPol, ZIN ali ZIS, mora torej javno in nedvoumno določati, da sme posamezni organ v sklopu svojih javnih pooblastil obdelovati osebne podatke, ter potem še katere, ter za kakšen namen. Pri tem mora biti zakon določen oz. jasen (*lex certa*). Predpisi namreč morajo biti jasni, določni in predvidljivi, če želimo, da jih tisti, ki se jih dotikajo, tudi razumejo. Le jasnost predpisa onemogoča različna tolmačenja. Upoštevanje načela določnosti, ki zagotavlja pravno varnost, zaupanje v pravo in enakost pred zakonom ter onemogoča različno tolmačenje oziroma uporabo predpisov v praksi, zahteva tudi Resolucija o normativni dejavnosti.

Z upoštevanjem načela določnosti se zagotavlja pravna predvidljivost za posameznike, na katere se ti podatki nanašajo, ter na posrednike, ki v vedno večji meri obdelujejo osebne podatke posameznikov in so zato pogosto tarča zahtevkov državnih organov za posredovanje osebnih podatkov. Nemogoče je npr. sprejeti razlago, da 1. odstavek 148. člena ZKP predstavlja zadostno pooblastilo za pridobivanje vsakovrstnih osebnih podatkov; navsezadnje potem kasnejši členi o zaslišanju osumljenca v predkazenskemu postopku, prikritih preiskovalnih ukrepih, ter preiskovalnih dejanjih ne bi imeli smisla. Zaskrbljujoč je tudi trend »nedoločnih« opisov oblastnih pooblastil, za rabo nespecificiranih »tehničnih sredstev« v 113. členu veljavnega Zakona o nalogah in pooblastilih policije - ZNPPol, ali podobno v nedavnem predlogu novele ZKP-M (»dekoderji«, »imsi lovilci«). Tehnična sredstva bi morala biti vsaj po vrsti opredeljena, v podzakonskih predpisih pa natančneje opisana in specificirana. Drugače si bo težko predstavljati, kako bo zanje izdana sodna odredba, oz. kako bo na kasnejšem sojenju moč preveriti zakonitost z njimi pridobljenih dokazov. »Tehničnih sredstev« namreč ni mogoče navzkrižno zaslišati.

Poštenost in transparentnost

Poštenost in transparentnost se logično nanašata na to, da mora obdelava osebnih podatkov potekati na do posameznika pošten in transparenten način do posameznika. Ta mora vedeti, kateri njegovi podatki bodo obdelovani, kdo jih bo obdeloval in za kakšne namene, komu in pod kakšnimi pogoji bodo posredovani. Vsako posredovanje osebnih podatkov, zlasti državnim organom, mora biti tudi posebej zabeleženo. V javnem sektorju naj bi ti načeli zagotovili z upoštevanjem načela zakonitosti (določenost v zakonu), v zasebnem sektorju pa je bistvena ustrezna informiranost posameznika, da lahko na podlagi zadostnih informacij poda svojo privolitev kot prostovoljno izjavo volje v obdelavo določenih osebnih podatkov za določene namene.

Sorazmernost

Sorazmernost z vidika obdelave osebnih podatkov pomeni, da je dopustno zbrati in obdelovati le najmanjši obseg osebnih podatkov, ki je potreben za dosego namena obdelave osebnih podatkov (minimizacija). Sorazmernost lahko pomeni predvsem to, da če osebni podatki niso potrebni za dosego cilja, jih ni primerno zbirati (kaj šele obdelovati). Argument, da se podatke zgolj zbira, ter da šele morebitna kasnejša uporaba teh podatkov šteje za poseg v ustavno pravico, ne vzdrži. Obenem se sorazmernost nanaša tudi na uporabo manj občutljivih podatkov od tistih, katerih narava oziroma zloraba ima večjo težo (psevdonimi so boljši kot navadni podatki, govoreče šifre so slabše od naključnih nizov ipd.). Prav tako se sorazmernost nanaša tudi na časovni vidik – tako je prekomerna hramba ali obdelava osebnih podatkov nedopustna in je treba podatke po dosegu namena oziroma po preteku zakonsko ali drugače določenega roka izbrisati, uničiti ali anonimizirati.

Nekaj zelo očitnih primerov nesorazmernosti:

- zbiranje več enoličnih identifikatorjev hkrati (npr. EMŠO in davčne številke);
- ribarjenje podatkov (angl. fishing expedition);
- hramba podatkov brez utemeljenega, vnaprej opredeljenega namena, »na zalogo«;
- zbiranje podatkov zaradi napačne zasnove sistema, tehnološke rešitve, zakonodajne določbe (»sistem me ne spusti skozi«, »takšen obrazec imamo«, »to pač morate izpolniti«, »ta podatek je obvezen«);
- nevarnost, da se med preiskovanjem kaznivih dejanj *rutinirano* zbere in obdela več podatkov, kot je v danem primeru dejansko potrebno[16].

Točnost in ažurnost

Načelo točnosti in ažurnosti narekuje, da morajo biti podatki, ki se obdelujejo, točni in ažurni. Točnost pomeni, da podatki niso napačni ali nepopolni, ažurnost pa pomeni, da se uporablja zadnji, ažuren podatek. Osebni podatki so lahko točni, niso pa ažurni, kar pomeni, da se uporablja podatek, ki je sicer točen in veljaven v določenem obdobju ali trenutku, vendar pa obstaja novejši, bolj ažuren podatek. Netočni ali neažurni podatki v policijskih evidencah imajo lahko izjemno hude implikacije na pravice posameznika. Pogosto slišani argument »*saj nimam kaj skrivati*« hitro zvodeni, če ni spoštovano načelo točnosti in ažurnosti in se o posamezniku v določeni evidenci nahajajo napačni ali neažurni podatki. V mislih imamo primere oseb, ki so pomotoma uvrščene na seznam iskanih oseb,

[16] Denimo, da se fotografije, prstne odtise in brise ustnih sluznic pobira vsem osebam, ki jim je odvzeta prostost oz. so drugače vabljene na policijsko postajo, ne glede na to, ali bodo zbrane biološke sledi dejansko potrebne v konkretne primeru.

katerih avtomobili ali registrske tablice so napačno označeni kot ukradena vozila, pomotoma izdane tiralice in podobno. V takšnih primerih so lahko zoper nedolžne posameznike uvedeni zelo ostri ukrepi, posameznik pa težko dokaže, da je prišlo do pomote. Takšne in drugačne »črne liste« v povezavi z neupoštevanjem načela točnosti in ažurnosti s seboj nosijo izrazita tveganja za varovanje pravic posameznika.

Rok hrambe

Rok hrambe je v tesni povezavi z načelom sorazmernosti in določa, da se osebni podatki lahko shranjujejo le toliko časa, dokler je to potrebno za dosego namena, zaradi katerega so se zbirali ali nadalje obdelovali. Po izpolnitvi namena obdelave se osebni podatki zbrišejo, uničijo, blokirajo ali anonimizirajo, če niso na podlagi zakona, ki ureja arhivsko gradivo in arhive, opredeljeni kot arhivsko gradivo, oziroma če zakon za posamezne vrste osebnih podatkov ne določa drugače.

Eden od bistvenih elementov PIA je tudi preučitev in določitev ustreznega roka hrambe osebnih podatkov, pri čemer je bistveno izhajati iz zasledovanih namenov – kateri je tisti najkrajši rok, v katerem lahko v zadovoljivi meri dosežemo zasledovane cilje? Na primeru hrambe prometnih podatkov je raziskava Evropske komisije[17] pokazala, da se 70% zahtev za podatke nanaša na podatke mlajše od treh mesecev, 88% vseh zahtev pa na podatke, ki so stari do šest mesecev. V tej luči je sorazmernost obstoječih rokov hramba prometnih podatkov – 14 oz. 8 mesecev – lahko tudi vprašljiva.

Zavarovanje osebnih podatkov

Zavarovanje osebnih podatkov je ožji pojem od varstva osebnih podatkov in se nanaša na informacijsko varnost, t.j. zagotavljanje celovitosti zaupnosti in razpoložljivosti oziroma organizacijske in tehnične ukrepe, s katerimi s katerimi se varujejo osebni podatki, preprečuje slučajno ali namerno nepooblaščeno uničevanje podatkov, njihova sprememba ali izguba ter nepooblaščena obdelava teh podatkov. Ustrezno zavarovanje osebnih podatkov, vključno z vodenjem dnevnika uporabe in posredovanja podatkov, preprečuje oz. otežuje zlorabe, ter olajšuje naknadno odkrivanje zlorab. Vendar je treba upoštevati tudi, da četudi imamo podatke izjemno dobro zavarovane, lahko kljub temu pride do njihove zlorabe, zlasti ob neupoštevanju ostalih načel (npr. obdelavi podatkov brez prave podlage, uporabi za namene, ki so različni od namena zbiranja podatkov, predolga hramba podatkov ipd.).

Upoštevanje pravic posameznika

Eno od bistvenih načel varstva osebnih podatkov se nanaša na posameznika, čigar osebni podatki se obdelujejo. Posameznik ima namreč pravico do seznanitve z lastnimi osebnimi podatki, v primeru ugotovljenih nepravilnosti pa tudi pravico do dopolnitve, popravka, blokiranja, izbrisa in ugovora. Obveščanje posameznika lahko predstavlja pomembno varovalko za zasebnost posameznika glede izvajanja policijskih pooblastil ter smotrnost uporabe policijskih pooblastil, upoštevaje seveda ustrezne izjeme v primerih, ko bi obveščanje posameznika utemeljeno oviralo interese postopka.

[17] http://www.statewatch.org/news/2011/apr/eu-com-data-retention-report-225-11.pdf

MODELI PIA

Informacijski pooblaščenec je preučil več modelov in pristopov k izvedbi PIA in ugotavlja, da ne obstaja en model PIA za vse situacije[18]. Zaslediti je možno PIA, ki so uporabne v določenih okoljih, zelo obsežne PIA kot tudi skrajšane PIA. Ločimo lahko:

a) vse-obsežne PIA (angl. full-scale PIA),
b) PIA majhnega obsega (angl. small-scale PIA),
c) kontrolne sezname za skladnost z zakonodajo, ki ureja področje zasebnosti, in
d) kontrolne sezname za skladnost na področju varstva osebnih podatkov.

Pooblaščenec za uvajanje novih policijskih pooblastil predlaga **PIA majhnega obsega v kombinaciji s kontrolnim seznamom[19]**. Takšen pristop po našemu mnenju v zdajšnjem obdobju, ko se uporaba PIA v našem prostoru šele uveljavlja, predstavlja najboljše razmerje med formalnostjo in učinkovitostjo postopka, ter zahteva manjše administrativno breme. PIA se izvede po v nadaljevanju predstavljenem **vzorcu, ki je že prilagojen področju uvajanja novih policijskih pooblastil.**

POSTOPEK IZVEDBE PIA

Informacijski pooblaščenec predlaga konsolidacijo običajnih faz PIA (preliminarna faza, identifikacija tveganj, identifikacija ukrepov, zaključno poročilo) v zgoščeni kontrolni seznam za identifikacijo in upravljanje tveganj ter nato izvedbo testa sorazmernosti. Pri uvajanju novih pooblastil naj bi s pomočjo kontrolnega seznama:

- opravičili in upravičili uvajanje novih pooblastil, ki posegajo v temeljne človekove pravice, tako da bi izkazali nujnost, primernost in učinkovitost ter sorazmernost novih pooblastil,
- pravočasno identificirali tveganja za morebitna nezakonita ravnanja z osebnimi podatki, pojav »function creep« efekta« in druga tveganja za poseg v človekove pravice,
- identificirali ukrepe za upravljanje tveganj, kot so uporaba anonimiziranih podatkov, minimizacija nabora podatkov, ustrezni roki hrambe, elementi sprotne presoje in nadzora, obveščanje posameznika ipd,
- omogočili izvedbo naknadnih analiz učinkov predpisa in uporabo povratnih informacij za izboljšanje predpisa.

Izvedba PIA naj bi potekala po tem modelu:

1. Predlagatelj pripravi PIA po predlaganem metodološkem okviru, ter jo pošlje v mnenje IP.
2. IP pregleda PIA in poda svoje pripombe.
3. Predlagatelj se opredeli do pripomb IP, po potrebi dopolni PIA.

[18] Več informacij o PIA lahko najdete v smernicah pooblaščenca Presoje vplivov na zasebnost, ki so dostopne na: https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Presoje_vplivov_na_zasebnost.pdf.
[19] V ZDA so po določbah Section 208 E-Government Act 2002 zvezne državne agencije dolžne izvesti PIA pred uvedbo novih ali večjimi spremembami obstoječih informacijskih sistemov, v katerih se obdelujejo osebni podatki. Glej npr. smernice za izvedbo PIA, ki jih uporablja Department Of Homeland Security: https://www.dhs.gov/privacy-compliance.

4. Predlagatelj na podlagi dopolnjene PIA pripravi predlog sprememb zakonodaje, ter oboje pošlje Ministrstvu za pravosodje, skupaj z označbo, ali je predlog vsebinsko že usklajen s PIA in pripombami IP.
5. Gradivo se naprej obravnava po ustaljenih postopkih medresorskega usklajevanja.

Predlagatelj (policija oziroma MNZ) razpolaga z največ informacijami o tem, kakšna sredstva naj bi bila uporabljena, kakšne so njihove značilnosti, želeni cilji itd. in je zato najprimernejši subjekt za pripravo prve verzije PIA na podlagi ustreznega metodološkega okvira za izvedbo PIA.

Z vključitvijo Pooblaščenca v proces IPA se zagotovi **neodvisna presoja PIA** in **povratni tok informacij k predlagatelju.** Usklajenost gradiva med predlagateljem in Pooblaščencem je zelo dober signal glede ustreznosti in sprejemljivosti gradiva ter opravljenih testih sorazmernosti Ministrstvu za pravosodje in nadaljnjemu medresorskemu usklajevanju.

IZVEDBA PIA

Bistven element presoje vplivov na zasebnost pri uvajanju policijskih pooblastil je pravočasno modeliranje ukrepov. PIA bi morala na področju uvajanja novih pooblastil vključevati naslednje faze[20]:

1. **OCENA STANJA NA PODROČJU UREJANJA,**
2. **ANALIZA TVEGANJ,**
3. **UPRAVLJANJE TVEGANJ,**
4. **TEST SORAZMERNOSTI,**
   4.1 nujnost,
   4.2 primernost in učinkovitost,
   4.3 sorazmernost.

Tako opravljena PIA je nato lahko vhodna informacija in podlaga za oblikovanje konkretnih določb predpisa. V nadaljevanju podrobneje pojasnjujemo, kaj naj bi posamezno poglavje vključevalo.

1. OCENA STANJA NA PODROČJU UREJANJA

V oceni stanja na področju urejanja naj bi predlagatelj najprej utemeljil, **zakaj** naj bi se uvajala nova pooblastila oziroma spreminjala obstoječa pooblastila. **Pojasniti mora, katere probleme naj bi nova pooblastila reševala** oziroma zakaj in kako bi nova pooblastila oziroma nova tehnološka sredstva tovrstne probleme reševala **na boljši način.** Če pojasnimo na primeru – zakaj bi uporabljali brezpilotne letalnike ter katere probleme bomo z njimi reševali.

V kolikor gre za uvajanje novih tehničnih sredstev, mora predlagatelj v svojih utemeljitvah tudi dovolj natančno opredeliti, za kakšna sredstva gre[21], kaj omogočajo ter kakšne so značilnosti njihovega

[20] Pri oblikovanju faz smo poskušali v največji možni meri upoštevati obstoječe vzorce za pripravo predlogov predpisov.
[21] Ne zahteva se navajanje tipa ali modela konkretnega tehničnega sredstva, temveč splošna opredelitev tehničnega sredstva: elektrošoker, pendrek, IMSI lovilec, brezpilotni letalnik.

delovanja pri obdelavi osebnih podatkov, t.j. kateri osebni podatki katerih oseb naj bi bili zbrani, za kateri namen in koliko časa se bodo obdelovali, ipd.

IZJEMNO POMEMBNO

Tehnično sredstvo oz. delovanje tehničnih sredstev mora biti **dovolj oziroma toliko natančno opredeljeno, da bodo zlasti tisti, ki bodo odobrili njihovo uporabe (npr. preiskovalni sodniki,** pooblaščeni policisti), **jasno in natančno vedeli, za kakšno tehnično sredstvo gre in kaj omogoča.** Brez tega ni mogoče pričakovati, da bodo lahko ustrezno presojali, kdaj je uporaba sredstva upravičena in kdaj ne.

Oceni stanja morata slediti **faza identifikacije tveganj in upravljanja tveganj,** oboje pa so nato kot **vhodni parametri uporabijo v trodelnem testu sorazmernosti.**

2. ANALIZA TVEGANJ

Glede na izkušnje opažamo, da se je v dosedanji praksi vse premalo pozornosti namenjalo opredeljevanju nujnosti, argumentiranju primernosti in učinkovitosti ter sorazmernosti novih pooblastil. Obstoječi pristop je bil **kazuističen** in ne sistematičen. Pri uvajanju novih pooblastil je treba predvideti ne samo pozitivne, temveč tudi negativne učinke - treba je **pravočasno** in **celovito** identificirati tveganja za neopravičene posege v človekove pravice.

Identifikacija tveganj je bistvenega pomena – **tveganja, ki jih predlagatelj ob pripravi predloga predpisa morebiti ne bi identificiral, utegneta kasneje izpostaviti splošna in strokovna javnost. Rezultat nepravočasno ali nepopolno identificiranih in naslovljenih tveganj je lahko oster odpor strokovne in splošne javnosti – in to kljub temu, da bi bil ob ustrezni analizi tveganj ukrep sicer povsem sprejemljiv. V interesu predlagatelja je zato, da vsa tveganja pravočasno identificira in obravnava.**

V ta namen je priporočljivo uporabiti naslednjo klasifikacijo tveganj.

I. TVEGANJA POVEZANA Z NUJNOSTJO POOBLASTIL

- Ali je novo pooblastilo oz. tehnično sredstvo resnično nujno potrebno?
- Ali je mogoče z drugimi (obstoječimi oz. milejšimi sredstvi) doseči isti cilj? Če ne, s čim se to dokazuje (in ne samo domneva)?

II. TVEGANJA V POVEZAVI Z IZVAJANJEM POOBLASTIL

1. **TVEGANJA POVEZANA Z *ZBIRANJEM* PODATKOV**
   - Kakšna so tveganja, da predvidena pooblastila oz. tehnična sredstva niso primerna za dosego cilja?
   - Kakšna so tveganja, da predvidena pooblastila oz. tehnična sredstva ne bodo učinkovita za dosego cilja?

- Kakšna so tveganja v zvezi z dokaznimi standardi – kateri dokazni standardi so primerni[22]?
- Kakšna so tveganja v zvezi odobritvijo uporabe pooblastil (preiskovalni sodnik, pooblaščeni policist) – ali bodo tisti, ki ukrep odobrijo, ustrezno seznanjeni s tem, za kakšno tehnično sredstvo gre, kaj omogoča in kakšne so implikacije oz. posledice uporabe tehničnega sredstva?
- Kakšno je tveganje, da tretje stranke, ki razpolagajo s podatki, ne bodo dovolj natančno seznanjene s tem, ali in katere podatke so dolžni posredovati ter v kakšnem roku?
- Kakšna so tveganja, da bi pri zbiranju podatkov prišlo do prekomernega obsega zbranih podatkov – t.j. da nepotrebni podatki ne bodo pravočasno izločeni?
- Kakšna so tveganja glede kakovosti podatkov, t.j. da bodo zbrani podatki netočni, neverodostojni[23], neažurni[24], nepopolni[25] ali nerelevantni[26]?
- Ali bomo z novimi pooblastili dejansko pridobili podatke o tistih osebah, zoper katere so usmerjena?
- Kakšen je obseg in intenzivnost posega v pravice tretjih oseb, kolateralne škode?
- Kakšna so tveganja, da bo poseg v zasebnost oseb, zoper katere je usmerjen ukrep nesorazmeren v primerjavi s pravico, ki jo želimo zavarovati z novim oziroma uporabo tehničnega sredstva?
- Na kakšen način bomo lahko naknadno izmerili in izkazali učinkovitost novih pooblastil oziroma tehničnih sredstev - s katerimi kazalniki bomo merili učinkovitost novih pooblastil oziroma tehničnih sredstev?

2. TVEGANJA POVEZANA Z ***ZAVAROVANJEM*** ZBRANIH PODATKOV

- Kakšna so tveganja v povezavi z zagotavljanjem celovitosti, zaupnosti in razpoložljivosti zbranih podatkov[27]?
  - Kakšne so možnosti, da bodo podatki dostopni nepooblaščenim osebam?
  - Kakšne so možnosti, da bodo osebe s pooblastili zlorabile svoja pooblastila? Kakšen je notranji nadzor nad procesi?
  - Kakšne so možnosti, da bodo podatki izgubljeni, spremenjeni, uničeni?
  - Kakšne so možnosti, da zlorabe ne bodo odkrite?
  - Kakšna so tveganja glede beleženja (sledljivosti) uporabe?
  - Kakšna so tveganja glede zagotavljanja celovitosti[28] dnevniških zapisov?

[22] Ali so preiskovalni sodniki dovolj seznanjeni npr. s tem, kaj je IMSI lovilec, kaj omogoča, kakšne implikacije predstavlja njegova uporaba?
[23] Glej prispevek »Zaupanje digitalnim dokazom in prometnim podatkom v mobilni telefoniji«, dosegljivo na http://pravokator.si/wp-content/uploads/2012/11/Zaupanje_digitalnim_dokazom_in_prometnim_podatkom_v_mobilni_telefoniji_Kovacic2012.pdf
[24] V Schengenskem informacijskem sistemu veliko težav povzroča nepravočasno brisanje podatkov, ko npr. določene države ne umaknejo podatkov, da določeno vozilo ni več obravnavano kot ukradeno.
[25] Npr. ukrep prikritega prisluškovanja v povezavi s šifriranjem komunikacij (npr. Skype).
[26] Npr. pridobivanje podatkov o klicih za celotne bazne postaje mobilne telefonije, kjer je velika večina pridobljenih podatkov nerelevantnih.
[27] Informacijska varnost se nanaša na zagotavljanje celovitosti, zaupnosti in razpoložljivosti podatkov. V smislu varstva osebnih podatkov se nanaša na ožji del – zavarovanje osebnih podatkov.
[28] Celovitost dnevniških zapisov se nanaša na preprečevanje možnosti potvarjanja, onemogočanja zapisa ali drugih dejanj, ki imajo vpliv na verodostojnost in dokazno vrednost dnevniških zapisov (npr. možnost izklopa beleženja, možnost naknadnega popravljanja zapisov, možnost uničenja dnevniških zapisov ipd.). Celovitost dnevniških zapisov je mogoče zagotoviti s tehničnimi (z uporabo namenskih sistemov) in/ali organizacijskimi ukrepi (npr. ustrezno ločevanje ali deljenje uporabniških pooblastil, sistem »štirih oči« ipd.)

3. TVEGANJA POVEZANA Z *UPORABO* PODATKOV

- Kakšne so tveganja, da zbrani podatki ne bodo uporabljivi v kazenskem postopku?
  - Kakšne so možnosti, da bodo zbrani podatki lahko neverodostojni, neceloviti?
  - Kakšne so možnosti, da drugi strani ne bo omogočena kontradiktornost ?
  - Kakšne so možnosti uporabe podatkov za druge namene (zlasti za pregon drugih kaznivih dejanj), ter kako zagotoviti, da bodo spoštovane zahteve ZKP v zvezi s tem?

4. TVEGANJA POVEZANA Z *UNIČENJEM* PODATKOV

- Kakšna tveganja prinašajo predvideni roki hrambe – ali so dovolj kratki?
- Kakšna so tveganja, da nepotrebni podatki ne bodo izločeni (prim. izločitvene vzorce pri odvzemu brisa ustne sluznice)?
- Katera dodatna tveganja prinašajo roki hrambe?

5. DRUGA TVEGANJA

- Katera druga, specifična tveganja obstajajo?

III. PRIMERJALNO PRAVNA ANALIZA TVEGANJ

Analiza tveganj bi morala vključevati tudi **prikaz in analizo ureditve v drugih pravnih sistemih**. Trenutno se v zakonodajnih gradivih prikaz ureditve v drugih pravnih sistemih bolj ali manj zadovoljivo izvaja, **pomanjkljivo** je po mnenju Pooblaščenca **predvsem tehtanje oziroma ocena izkušenj iz drugih pravnih sistemov**. Običajno se v tej točki zakonodajnega gradiva zgolj *opredeli pravna ureditev* v drugem pravnem sistemu (npr. ali obstaja takšno pooblastilo, kakšni so pogoji za uporabo ipd.), manjka pa analiza oziroma podatki o tem, *kakšne so dejanske izkušnje* z uporabo pooblastila, katere so bile zaznane prednosti in pomanjkljivosti – kar bi morala biti pomembna dodana vrednost tega dela analize, saj ni nobenega smisla v ponavljanju napak, ki so jih storili v drugih državah[29].

Pooblaščenec opaža, da se pri pripravi zakonodajnega besedila prepogosto zgledujemo samo pri rešitvah, ne upoštevamo pa tudi načinov izvedbe in že vzpostavljenih kavtel; prav tako se pri prenosu rešitev iz drugih pravnih sistemov ne upošteva širše normativno, institucionalno in zgodovinsko okolje[30].

Ko smo identificirali in analizirali tveganja, lahko pristopimo k upravljanju tveganj – modeliranju ukrepov, s katerimi lahko tveganja izničimo ali zmanjšamo na sprejemljive ravni.

[29] Konkreten primer predstavljajo npr. nemške izkušnje glede uporabe t.i. trojanskih konjev *(»*Bundestrojaner«), ki v pripravljalnem gradivu ZKP-M sploh niso omenjene.

[30] Upoštevati je npr. treba tudi kontekstualno okolje, npr. dejstvo, da so v našem pravnem sistemu določene pravice močneje varovane kot v drugih ureditvah (npr. varovanje komunikacijske zasebnosti v 37. členu Ustave RS). Tvegano je zgolj prenašati prakse iz drugih pravnih ureditev in pri tem zanemariti zgodovinske izkušnje, drugačne institucionalne in normativne okvire in druge kontekstualne elemente, ki so vodili do sprejema pooblastil v drugih pravnih sistemih.

3. VAROVALKE – UPRAVLJANJE TVEGANJ

Z vključitvijo ustreznih varovalk za upravljanje tveganj se vnaprej poskrbi za minimizacijo posegov v človekove pravice, prepreči najhujše zlorabe ter zagotovi uporabnost zbranih podatkov. Tovrstne varovalke zajemajo, primeroma:

- omejitve glede odobritve in uporabe (vključno s prepovedjo nedovoljenih rab),
- takojšnje zavrženje nepotrebnih podatkov,
- kratke, utemeljene roke hrambe,
- ukrepe za zavarovanje pridobljenih podatkov,
- ukrepe za nadzor nad rabo pridobljenih podatkov,
- vodenje statistik ter redno letno poročanje o rabi ukrepa,
- notranji in zunanji nadzor,
- obveščanje posameznika, ki je bil tarča oz. slučajna tarča ukrepa,
- možnost tretjega obdelovalca, ki na zahtevo policije le tej posreduje podatke o posamezniku, da posameznika seznani z zahtevkom,
- idr.

Z ustreznimi varovalkami je mogoče uspešno prestati test sorazmernosti – če namreč z varovalkami dosežemo minimalnost posega v zasebnost, vpliva na pravice posameznika, potem je toliko lažje upravičiti uvedbo ukrepa za dosego drugih legitimno zasledovanih ciljev.

Nabor možnih varovalk, s katerimi lahko zmanjšamo ali odstranimo identificirana tveganja, je naslednji[31]:

I. TVEGANJA POVEZANA Z NUJNOSTJO POOBLASTIL

- **podatki, argumenti, primerjalno pravne in druge analize,** ki izkazujejo nujnost pooblastila in odsotnost milejših sredstev.

II. TVEGANJA V POVEZAVI Z <u>IZVAJANJEM POOBLASTIL</u>

1. TVEGANJA POVEZANA Z *<u>ZBIRANJEM</u>* PODATKOV

- **podatki, argumenti, analize**, ki izkazujejo primernost in učinkovitost pooblastila oz. tehničnega sredstva za dosego cilja
- **utemeljitev ustreznosti dokaznega standarda;**
- **omejitve uporabe, npr.:**
  - npr. na določena kazniva dejanja,
  - določbe glede sprotnega izločanja podatkov ob zbiranju,
  - drugo_____.
- **postopek odobritve, npr.:**
  - izvedba ustreznih izobraževanj za preiskovalne sodnike, pooblaščene policiste;

[31] Seznam ni izčrpen, možne so tudi druge varovalke.

- odredba sodišča, obvezni elementi odredbe;
- drugo_____.

- **ukrepi za zagotavljanje kakovosti (celovitosti, točnosti, ažurnosti, relevantnosti) podatkov, npr:**
  - zagotovitev celovitosti dokazne sledi (angl. chain of custody),
  - kontrolni mehanizmi[32],
  - upoštevanje ugotovitev iz analize primernosti in učinkovitosti[33].
- **ukrepi za zmanjševanje tveganj v povezami s tretjimi strankami (posredniki, npr. ponudniki elektronskih komunikacij, oz. storitev), npr:**
  - določnost pravil o zbiranju in posredovanju podatkov za tretje stranke (posrednike).
- **minimizacija posega v pravice oseb, zoper katere je usmerjen ukrep**
  - konkretna in natančna opredelitev ciljev in nalog ukrepa (kaj se išče), da se preiskava neupravičeno ne razširi tudi na druga področja (t.i. ribarjenje podatkov),
  - sodna avtorizacija bolj tveganih posegov,
  - višji dokazni standard,
  - aktivni postopki za minimizacijo škode[34],
  - vnaprejšnje oz. naknadno obveščanje posameznika, na katerega se ukrep nanaša,
  - sodelovanje posameznika pri izvedbi ukrepa (prim. 223.a člen ZKP).
- **minimizacija posega v pravice tretjih oseb**
  - takojšnje (zapisniško) izločanje nerelevantnih podatkov,
  - anonimizacija,
  - obveščanje posameznika.
- **merila**, s katerimi se bo merila učinkovitost izvajanja pooblastila,
- **naknadne presoje učinkovitosti (RIA),**
  - revizija učinkovitosti izvajanja pooblastila.

2. TVEGANJA POVEZANA Z ***ZAVAROVANJEM*** ZBRANIH PODATKOV

- **postopki in ukrepi za zavarovanje pridobljenih podatkov**
  - ukrepi za zagotavljanje celovitosti, zaupnosti in razpoložljivosti zbranih podatkov,
  - posebni ukrepi.
- **sledljivost uporabe**
  - beleženje uporabe,
  - zagotavljanje celovitosti dnevniških zapisov[35],
  - označevanje izvodov nosilcev podatkov oz. dokumentov.

[32] Pri ugotavljanju osumljenčeve telefonske številke, denimo, z več kontroliranimi zajemi seznama prisotnih telefonskih številk v ustreznem časovnem zaporedju, ob istočasnem fizičnem sledenju osumljencu. Presek zajetih telefonskih številk bo pripadal osumljencu.
[33] Upoštevanje, da lahko osumljenci podvzemajo aktivne ukrepe za otežkočanje izvedbe prikritih preiskovalnih ukrepov; od menjavanja SIM kartic, uporabe VoIP rešitev, uporabe šifriranja, idr.
[34] Ponekod v tujini je, sledeč sodni praksi, izvedba nekaterih prikritih preiskovalnih ukrepov močno omejena s ciljem preiskovanja konkretnega kaznivega dejanja; npr. pri izvajanju ukrepa prikritega prisluškovanja telefonskih klicev je potrebno izklopiti snemanje, če se v določenem času ne oceni, da je klic relevanten, glej npr. http://www.justice.gov/criminal/foia/docs/elec-sur-manual.pdf
[35] Glej opombo št. 30.

3. TVEGANJA POVEZANA Z *UPORABO* PODATKOV

- **postopek uporabe**
  - ukrepi za zagotovitev kontradiktornosti.
- **(izrecne) prepovedi uporabe, npr.:**
  - prepoved uporabe za določene namene (function creep[36]).
- **poročanje o uporabi**
- **nadzor nad uporabo**
  - notranji nadzor,
  - zunanji nadzor,
- drugo_____.

4. TVEGANJA POVEZANA Z *UNIČENJEM* PODATKOV

- **uporaba minimalnih rokov, ki omogočajo izpolnitev zadanih ciljev,**
- **ukrepi za minimizacijo podatkov po uporabi, npr.:**
  - naknadno zapisniško izločanje nepotrebnih podatkov,
  - ukrepi za blokiranje, anonimizacijo nepotrebnih podatkov.

5. DRUGA TVEGANJA

- **varovalke za preprečitev preostalih tveganj.**

III. PRIMERJALNO PRAVNA ANALIZA TVEGANJ

- **ukrepi za minimizacijo tveganj, ki so bila identificirana na podlagi primerjalno pravnega prikaza analize izkušenj pri uporaba pooblastila oz. tehničnega sredstva v drugih pravnih sistemih, npr.**
  - ukrepi za zmanjšanje tveganj, ki temeljijo na izkušnjah v drugih pravnih sistemih,
  - ukrepi za zmanjšanje tveganj, ki temeljijo na kavtelah v drugih pravnih sistemih,
  - ukrepi za zmanjšanje tveganj, ki temeljijo na analiz širšega normativnega, institucionalnega in zgodovinskega okolja.

4. TEST SORAZMERNOSTI

Po oceni stanja na področju urejanja analiz tveganj in upravljanju tveganj sledi test sorazmernosti, ki temelji na rezultatih prejšnjih faz. S tem, ko je predlagatelj predstavil problematiko, analiziral tveganja in predstavil ukrepe za zmanjševanje tveganj, je sploh podana podlaga, da se lahko izvede test sorazmernosti.

Test vključuje:

4.1 test nujnosti,
4.2 test primernosti in učinkovitosti,
4.3 test sorazmernosti.

[36] Npr. prepoved uporabe dekoderjev za forenzično analizo nadzorovane naprave, glej predlog sprememb ZKP-M.

4.1 Test nujnosti

Test nujnosti se nanaša na argumente in obrazložitev, iz katerih izhaja, da je uporaba določenega tehničnega sredstva ali pooblastila **nujna za dosego ustavno dopustnega cilja**. Gre torej za **konkretne podatke, dokazila, argumente,** ki izkazujejo, da **cilja ni mogoče doseči z nobenim blažjim posegom v ustavno pravico ali celo brez njega**, pri čemer je navedeno treba dejansko utemeljiti in ne zgolj pavšalno navajati (glej primer praktične uporabe metodološkega okvira - uporaba brezpilotnih letalnikov). Pokazati je treba, da z drugimi ukrepi istega cilja ne bi mogli doseči.

4.2 Test primernosti in učinkovitosti

Test primernosti in učinkovitosti se nanaša na to, **ali bomo s preučevanim ukrepom dejansko dosegli zasledovane cilje – ali so torej predlagani ukrepi primerni in učinkoviti za dosego zaželenega, ustavno dopustnega cilja**. Tudi tu je treba navedbe ustrezno argumentirati in podkrepiti – s podatki, analizami, dokazili in podobno (glej primer praktične uporabe metodološkega okvira v nadaljevanju). Ukrepi, ki npr. podcenjujejo sposobnosti ali tehnološko opremljenost iskanih oseb (npr. uporabo spletnih kavarn, pogosto menjavanje predplačniških SIM kartic, uporabo šifriranih komunikacij, izogibanje elektronskim komunikacijam), morajo biti podkrepljeni z zelo trdnimi dokazi, da bo uporaba takšnih sredstev res dosegla cilj. Primer ukrepa, pri katerem ta test ni bil uspešno izveden, je bil predlog širitve dostopa do podatkov celotnih baz mobilne postaje, saj niso bili predstavljeni dovolj trdni argumenti, da je ukrep primeren in učinkovit.

4.3 Test sorazmernosti v ožjem smislu

Test sorazmernosti v ožjem smislu se nanaša na to, da je pri ocenjevanju nujnosti posega treba tehtati tudi pomembnost s posegom prizadete pravice v primerjavi s pravico, ki se s tem posegom želi zavarovati, in odmeriti nujnost posega sorazmerno s težo prizadetih posledic. **Ali je torej poseg v zasebnost sorazmeren v primerjavi s pravico, ki jo želim s posegom zavarovati** (do osebne varnosti, do zaščite otrok, javne varnosti ipd.). Ukrep, ki je recimo usmerjen zoper večje število predvidoma nedolžnih ljudi s ciljem, da se zberejo podatki o domnevnih storilcih kaznivih dejanj, mora zelo jasno pokazati, da je tak ukrep vendarle sorazmeren, t.j. da je pomembneje ujeti storilce kaznivih dejanj kot obseg posega v njihove pravice ali pravice tretjih oseb. Zgolj načelna določba, da je potrebno ukrep izvesti tako, da »se v najmanjši možni meri poseže v pravice tretjih oseb«, ne more zadostovati.

Predlagani ukrep mora prestati vse tri teste. Ukrep mora biti dokazano nujen in učinkovit, hkrati pa ne sme biti nesorazmeren v svojem posegu v ustavne pravice.

Odzivi na lanskoletna razkritja izjemno obsežnega zbiranja telekomunikacijskih podatkov s strani varnostno-obveščevalnih in kazenskopravnih služb nekaterih držav izpostavljajo številne dvome glede nujnosti, učinkovitosti (dejanske, izkazane koristi ukrepov preprečevanju terorizma) ter predvsem sorazmernosti izvedenih ukrepov. Še dodatni dvomi se porajajo zavoljo nedoločne in mestoma tudi tajne narava priprave in izvedbe ukrepov, ter zavoljo minimalne možnost posameznika, da se zbiranju podatkov zoperstavi oz. da zbrane podatke ovrže.

PRIMER UPORABE METODOLOŠKEGA OKVIRA

Z namenom lažjega razumevanja uporabe predstavljenega metodološkega okvira smo želeli na praktičnem primeru predstaviti njegovo uporabo v praksi. V ta namene smo izbrali primer pooblastila za dostop do podatkov celotnih baznih postaj mobilne telefonije skozi spremembo obstoječega pooblastila za pridobivanje prometnih podatkov iz 1. odstavka 149.b člena ZKP[37].

Primer je sestavljen po že opisanih korakih. Najprej smo v **oceni stanja na področju urejanja** predstavili vzroke za uvajanje novega pooblastila. Nato smo s pomočjo nabora tveganj **identificirali tveganja**, ki jih prinašajo nova pooblastila. V nadaljevanju smo s pomočjo nabora varovalk popisali ukrepe, s katerimi naslavljamo oziroma **upravljamo ugotovljena tveganja.** Na koncu smo navedene podatke uporabili v **tridelnem testu sorazmernosti**.

Opomba: upoštevati je treba, da podani teksti niso **ne izčrpni ne popolni**, temveč so namenjeni predvsem **boljšemu razumevanju uporabe** metodološkega okvira za izvajanje PIA. Gre za **primer pričakovanega prispevka s strani policije** v prvi fazi uvajanja novih pooblastil in **ne za dokončno ali širše sprejeto utemeljitev sprejema novih pooblastil.**

1. OCENA STANJA NA PODROČJU UREJANJA

POJASNILO: Ocena stanja mora na kratko pojasniti razloge za sprejem novih pooblastil – opis stanja, zaradi katerega se predlagajo nova pooblastila.

PRIMER:

V določenih primerih je bilo storjeno kaznivo dejanje ali več njih (npr. tatvine večjih količin bakra iz skladišč podjetij), policija pa na podlagi obstoječih pooblastil ni uspela zbrati dovolj obvestil in informacij, da bi lahko prišla na sled storilcem. Na podlagi ugotovitev, da storilci delujejo organizirano ter da pri organiziranju, pripravljanju ali izvrševanju teh kaznivih dejanj uporabljajo mobilne telefone, je legitimna ideja, da bi se s pridobitvijo podatkov o uporabi mobilnih telefonov za določena območja, ki jih pokrivajo bazne postaje mobilne telefonije in na katerih so bila izvršena kazniva dejanja, dalo z nadaljnjo analizo podatkov ugotoviti, katere telefonske številke se pojavljajo/ponavljajo na različnih krajih storitev kaznivih dejanj. S tem bi se dalo zožiti nabor sumljivih telefonskih številk/komunikacij in na podlagi obstoječih pooblastil izvesti nadaljnje ukrepe v smeri identifikacije storilcev.

Policija se sooča z dejstvom, da (nekateri) operaterji javno dostopnih elektronskih komunikacijskih omrežij zavračajo zahtevke za pridobitev podatkov za celotno bazno postajo z obrazložitvijo, da obstoječa pravna podlaga (149.b člen ZKP) dopušča pridobitev podatkov o klicanih številkah le za določeno komunikacijsko sredstvo, ne pa tudi za komunikacijsko opremo, kot je recimo bazna postaja mobilne telefonije.

V zadnjem letu je policija preiskovala 10 primerov, v katerih so neznani storilci odtujili večje količine bakra in s tem oškodovali 5 gospodarskih družb v skupni višini 250.000 EUR. Policija na podlagi obstoječih pooblastil ni uspela zbrati dovolj obvestil in informacij, da bi lahko prišla na sled storilcem.

[37] Glej izvorni predlog novele ZKP-K.

Preverjanje policiji znanih kriminalnih družb, preverjanje podatkov o odkupih bakra, pregled relevantnih posnetkov videonadzornih sistemov, zaslišanja dežurnih varnostnikov in splošno zbiranje obvestil se ni izkazalo kot učinkovito.

Policija ocenjuje, da obstoječi ukrepi ne zadoščajo za učinkovit pregon pisanih kaznivih dejanj.

2. ANALIZA TVEGANJ

POJASNILO: V analizi tveganj se je smiselno opreti na nabor možnih tveganj in ugotoviti, katera tveganja so prisotna. Identifikacija tveganj je lahko opisne in nestrukturirane narave.

PRIMER (*SEZNAM <u>NI NUJNO POPOLN</u>*):

Tveganja povezana z nujnostjo pooblastil *se nanašajo na to, ali ima policija že dovolj obstoječih pooblastil, da bi lahko prišla na sled storilcem, torej ali lahko z zbiranjem obvestil in drugimi metodami pridobi dovolj informacij, da zoži nabor osumljencev. V konkretnem primeru je recimo utemeljeno pričakovati, da gre za organizirano združbo (policiji že znane osebe, tipično povratnike) in da je treba ukradeni material pretvoriti v finančno korist, kar oboje že omogoča nadaljnje raziskovanje. Treba se je tudi vprašati naslednje – če je neko pooblastilo res nujno, kako smo v preteklosti reševali podobne probleme, s katerimi ukrepi smo se jih lotevali in ali so res dejansko nerešljivi?*

Pridobivanje podatkov baznih postaj vzbuja resna vprašanja in ***tveganja, povezana z učinkovitostjo in primernostjo pooblastil.*** *Zelo realno tveganje je, da storilci težjih kaznivih dejanj ne uporabljajo svojih osebnih mobilnih telefonov (na katere bi bilo preko naročniškega razmerja vezano njihovo pravo ime), oziroma da sploh ne uporabljajo mobilnih telefonov pri storitvi kaznivih dejanj. Skoraj gotovo bodo uporabljali predplačniške anonimne kartice in telefone. Hitra menjava in izmenjevanje SIM kartic in telefonskih aparatov znotraj organiziranih združb so klasične metode oviranja preiskovalnih organov. Prav tako lahko storilci uporabljajo danes že povsem običajne pametne telefone z aplikacijami, ki omogočajo komunikacijo, ki se ne hrani v retencijskih bazah operaterjev. Predlagan ukrep je v primeru aplikacij, kot so Skype, Viber, WhatsApp in številne druge, neučinkovit. Navsezadnje lahko uporabljajo tudi lasten sistem RF zvez, ki ga operater sploh ne bo zabeležil, ali se na kraj kaznivega dejanja odpravijo tudi brez komunikacijske naprave.*

Tveganja, povezana s posegom v pravice tretjih oseb *in* ***tveganje prekomernega obsega zbranih podatkov,*** *so izrazita že po naravi stvari, saj ukrep predvideva masovno, neusmerjeno pridobivanje podatkov. Glede na to, da preiskovalni sodnik ne more vedeti, katero telefonsko številko je uporabljal storilec in kateremu operaterju pripada telefonska številka iskane osebe, bo treba zahtevo za podatke nasloviti na vse ponudnike mobilne telefonije.*

Tveganja v zvezi z odobritvijo uporabe pooblastil *vključujejo več vidikov. Kako opredeliti zaprosilo za izdajo odredbe, da bo lahko preiskovalni sodnik pravilno presodil, ali so vsi zakonski kriteriji izpolnjeni? Kakšno je tveganje, da bodo nekateri preiskovalni sodniki ukrep potrjevali po privzetem, drugi pa ga zavračali? Kako bo potekalo izobraževanje preiskovalnih sodnikov? Težave lahko nastopijo tudi s formulacijo odredbe za posredovanje podatkov. Predvidoma bo preiskovalni sodnik zahteval podatke o opravljenih klicih za obdobje (verjetno) nekaj minut pred (in po?) storjenimi kaznivimi dejanji, in sicer za vse bazne postaje, na katere bi lahko bil storilec povezan (brez konkretne številke namreč ne bo mogel opredeliti, za katero bazno postajo zahteva podatke). Obseg odredbe bi moral biti zato že v samem začetku zelo širok. Število oseb, pri katerih bo prišlo do obdelave osebnih*

podatkov in posega v komunikacijsko zasebnost, bo v vsakem primeru veliko. Odgovor na vprašanje, ali bodo komunikacijski podatki nedolžnih posameznikov izpostavljeni preiskavi, bo odvisen zgolj od okoliščine, ali so se znašli v bližini storitve kaznivega dejanja, ali se je njihov mobilni aparat povezal na tisto bazno postajo, ki bo predmet zahteve po prometnih podatkih oz. ali so bili na povsem drugem koncu države, a so takrat komunicirali s takšnim posameznikom. V povezavi z navedenim obstaja tudi ***tveganje v povezavi s tretjimi strankami****, t.j. da tretje stranke, ki razpolagajo s podatki (v tem primeru operaterji), ne bodo dovolj natančno seznanjene s tem, ali in katere podatke so dolžne posredovati ter v kakšnem roku.*

Posebno ***tveganje za nesorazmernost*** *predstavljajo tudi zahteve glede hrambe podatkov. Glede na to, da gre za podatke iz t.i. data retention zbirke, bodo operaterji morali posredovane podatke glede na določbe Zakona o elektronskih komunikacijah hraniti za obdobje 10 let! 10 let hrambe podatkov o klicih za skoraj gotovo vsaj 99% nedolžnih posameznikov, katerih podatki so bili zahtevani. Podatke o tem, koga so klicali, kdaj in podatke o tem, kje so se nahajali. Še več – med temi podatki bodo podatki o lokaciji tako kličočega kot klicanega(!), ki se je lahko v času storitve kaznivega dejanja nahajal na drugem koncu države.*

Glede na nekatere raziskave o možnostih potvarjanja identitet in s tem manjše dokazne vrednosti podatkov v retencijskih zbirkah obstaja ***tveganje glede kakovosti podatkov,*** *t.j. da bodo zbrani nerelevantni podatki, ki hkrati ne bodo verodostojni.*

Neusmerjenost ukrepa prinaša po naravi stvari tudi številna druga tveganja.

Glede na veliko količino zbranih podatkov obstajajo povečana ***tveganja za zagotavljanje informacijske varnosti*** *- celovitosti, zaupnosti in razpoložljivosti zbranih podatkov. Navedeno se nanaša tako na fazo pridobivanja podatkov (kako bodo operaterji posredovali podatke, v kakšnih formatih, po katerih medijih oz. kanalih itd.), kot na fazo uporabe in uničenja podatkov. Prisotno je posebno tveganje za nezakonito posredovanje podatkov, saj se lahko iz pridobljenih podatkov razberejo komunikacijske navade posameznikov. Prisotno je tudi tveganje zlorab podatkov za druge namene – ugotavljanje komunikacijskih navad bližnjih, znanih oseb itd. Zaradi velike količine podatkov obstajajo posebna medsebojno povezana* ***tveganja v povezavi z internimi zlorabami, npr. tveganje glede beleženja dostopov do podatkov****,* ***tveganje glede nepooblaščenega spreminjanja podatkov*** *in* ***tveganja, da zlorabe ne bodo odkrite****. Prav tako zaradi velike količine podatkov, ki kažejo na komunikacijske navade posameznikov, obstajajo* ***tveganja za možnosti uporabe podatkov za druge namene*** *(zlasti za pregon drugih kaznivih dejanj) in s tem povezana vprašanja, kako zagotoviti, da bodo spoštovane zahteve ZKP v zvezi s tem. Prisotna so tudi* ***tveganja v povezavi z izločanjem in uničevanjem nepotrebnih podatkov****.*

Primerjalno pravna analiza tveganj *kaže, da je pooblastilo v rabi v naslednjih državah_____, in sicer (predstaviti pooblastila). Izkušnje pri uporabi pooblastila kažejo, da _____(navedite pozitivne in negativne izkušnje)_____.*

3. URAVLJANJE TVEGANJ

POJASNILO: S pomočjo nabora varovalk v tem delu predstavimo, s katerimi ukrepi bo dosežena minimizacija posegov v človekove pravice, preprečene najhujše zlorabe ter zagotovljena uporabnost zbranih podatkov.

PRIMER (*SEZNAM <u>NI NUJNO POPOLN</u>*):

Nujnost uporabe pooblastila lahko podkrepimo z naslednjimi podatki in argumenti_____.

Tveganja, povezana z zbiranjem podatkov, bodo minimizirana z naslednjimi ukrepi:

- *omejitve uporabe samo na določena kazniva dejanja,*
- *pridobivanje podatkov bo možno le na podlagi predhodne odredbe preiskovalnega sodnika,*
- *postopek posredovanje podatkov s strani operaterjev bo natančneje opredeljen v pravilniku,*
- *pridobljeni podatki bodo analizirani v roku___ dni, vsi nerelevantni podatki bodo v roku _____nepovratno zapisniško uničeni,*
- *izrecna prepoved uporabe podatkov izven konkretnega kazenskega postopka, v katerem je bilo uporabljeno pooblastilo*[38]*,*
- *nad izvajanjem pooblastila se bo izvajal redni interni nadzor, poročila internega nadzora bodo posredovana neodvisnemu organu (npr. Ministrstvu za pravosodje, Informacijskemu pooblaščencu),*
- *letno poročanje o učinkovitosti pooblastila na podlagi naslednjih kazalnikov:*
  - *število primerov, v katerih je bilo uporabljeno pooblastilo na letni ravni;*
  - *odstotek zbranih podatkov, ki so bili spoznani kot nerelevantni in izločeni,*
  - *delež primerov, v katerih so bili pridobljeni podatki ključni za izsledite storilcev,*
- *itd.*

4. TEST SORAZMERNOSTI

PRIMER:

<u>4.1 Test nujnosti</u>

Na podlagi naslednjih argumentov menimo, da je uporaba določenega tehničnega sredstva ali pooblastila nujna za dosego ustavno dopustnega cilja.

V zadnjem letu je policija preiskovala 10 primerov, v katerih so neznani storilci odtujili večje količine bakra in s tem oškodovali 15 gospodarskih družb v skupni višini 250.000 EUR. Policija na podlagi obstoječih pooblastil ni uspela zbrati dovolj obvestil in informacij, da bi lahko prišla na sled storilcem. Preverjanje policiji znanih kriminalnih družb, preverjanje podatkov o odkupih bakra, pregled relevantnih posnetkov videonadzornih sistemov, zaslišanja dežurnih varnostnikov in splošno zbiranje obvestil se ni izkazalo kot učinkovito. Obstaja velika verjetnost, da storilci pri organiziranju, pripravljanju ali izvrševanju kaznivih dejanj uporabljajo mobilne telefone, zato bi policija s pridobitvijo podatkov o uporabi mobilnih telefonov za določena območja, ki jih pokrivajo bazne postaje mobilne telefonije, na katerih so bila izvršena kazniva dejanja, z nadaljnjo analizo podatkov ugotovila, katere telefonske številke se pojavljajo na različnih krajih storitev kaznivih dejanj. S tem bi se dalo zožiti nabor sumljivih telefonskih številk/komunikacij in na podlagi obstoječih pooblastil izvesti nadaljnje ukrepe v smeri identifikacije storilcev. Po oceni policije z drugimi, milejšimi ukrepi ni mogoče zožiti nabora osumljencev, zato je ukrep nujen, da se izsledijo storilci opisanih kaznivih dejanj…

[38] Zavoljo neusmerjenosti ukrepa običajna doktrina plain view ne more priti v poštev.

4.2 Test primernost in učinkovitosti

PRIMER:

Policija ocenjuje, da je uporaba konkretnega pooblastila, kljub temu, da obstajajo številna tveganja v povezavi s predlaganim pooblastilom, lahko primerna in učinkovita. Gre za kazniva dejanja, ki povzročajo precejšnjo gospodarsko škodo in za katerimi stojijo dobro organizirane kriminalne družbe. Storilci kaznivih dejanj pa morajo vendarle tako kot vsi ostali komunicirati in tudi najbolj sposobne združbe se lahko spozabijo in slej ko prej uporabijo komunikacijska sredstva, ki puščajo elektronske sledi. Policija bo tako kot sedaj uporabila vsa obstoječa pooblastila in šele v primeru, da se ta ne bodo izkazala kot uspešna, bo na preiskovalnega sodnika naslovila zahtevek za izdajo odredbe za pridobitev podatkov za bazne postaje mobilne telefonije. Zahtevek za pridobitev sodne odredbe bo natančno opredelil vzroke za nujnost uporabe pooblastila. O izvedbi ukrepa, vključno z izbrisom nerelevantnih številk, bodo vodeni natančni zapisniki. S pomočjo nastale papirnate sledi bomo potem lahko izkazovali in merili učinkovitost pooblastila. S predvidenimi ukrepi za zagotovitev celovitosti zbranih podatkov bomo zagotovili upoštevanje načela kontradiktornosti ter posledično zagotovili uporabnost zbranih podatkov v konkretnem kazenskem postopku…

4.3 Test sorazmernosti v ožjem smislu

PRIMER:

Policija se zaveda, da gre za ukrep, ki je recimo usmerjen zoper večje število predvidoma nedolžnih ljudi s ciljem, da se zberejo podatki o domnevnih storilcih kaznivih dejanj. Istočasno pa se je treba zavedati tudi, da imamo na drugi strani gospodarske subjekte, ki jim opisana kazniva dejanja povzročajo precejšnjo gospodarsko škodo in s tem prihaja do posega v njihove pravice. Poudarjamo, da ne gre za manjša in nepomembna kazniva dejanja. Z izvedeno identifikacijo in analizo tveganj in sprejetimi varovalkami, bomo minimizirali poseg v pravice nedolžnih oseb ter po drugi strani preprečili nadaljnje okoriščanje kriminalnih združb, ki se lahko razširi tudi na druga področja nezakonitega delovanja. Očitki, da gre za ribarjenje podatkov, za slučajno iskanje podatkov o kaznivih dejanjih, so prav tako zavrženi z ostrimi in na konkretno preiskavo osredotočenimi pogoji za pridobitev odredbe oz. za izvedbo ukrepa. Policija sklepno ocenjuje, da bo z minimalnim dodatnim posegom v človekove pravice mogoče odkriti številne storilce kaznivih dejanj, ki so ji bili do sedaj nedosegljivi...

POMEMBNO!
Pojasnilo glede konkretnega primera uporabe metodološkega okvira

Pooblaščenec opozarja, da je namen podanega primera uporabe metodološkega okvira predvsem prispevati k boljšemu razumevanju, **kako dejansko izvesti presojo vplivov na zasebnost in katere elemente naj bi ta vsebovala.** Pooblaščenec se je pri pisanju konkretnega primera postavil predvsem na gledišče policije kot institucije, ki je glavni predlagatelj novih pooblastil in kateri je metodološki okvir zato tudi v prvi vrsti namenjen. Primer tako prikazuje predvsem, **kaj okvirno bi morala policija pripraviti v prvi fazi** uvajanja novih pooblastil. Pooblaščenec zato **ponovno opozarja, da gre šele za prvo fazo razprave in ne že za sprejem dokončne odločitve o utemeljenosti, nujnosti, primernosti in sorazmernosti novih pooblastil**. Do navedb v PIA naj bi se po predlaganem postopku opredelil **Pooblaščenec**, glede vseh podanih stališč pa bi nato lahko potekala **argumentirana razprava** v ustaljenih postopkih priprave sprememb predpisov.

ZAKLJUČEK

O sprejemljivosti novih nadzorovalnih tehnologij bi v demokratični državi morala odločati **družba**, ne pa **represivni organi** (**sami**). Če odloča policija, potem ne moremo govoriti o **pravni**, ampak o **policijski** državi. Ustrezno obravnavo novih policijskih pooblastil in uporabe novih tehničnih sredstev v času, ko tehnologija omogoča praktično neomejene posege v človekove pravice, pričakujemo državljani, Informacijski pooblaščenec, splošna in strokovna javnost. V interesu predlagatelja novih pooblastil je, da vsa tveganja pravočasno identificira in naslovi in se tako izogne odporu splošne in strokovne javnosti, izogne težavam z uporabnostjo zbranih podatkov v kazenskih postopkih in deluje v smeri večje preiskanosti kaznivih dejanj. Očitkom glede drsenja v policijsko državo, težavam z uporabnostjo zbranih podatkov v kazenskih postopkih in očitkom glede neprimernosti, neučinkovitosti in nesorazmernosti pooblastil se namreč da izogniti.

Pričujoče smernice predstavljajo košček v mozaiku uravnoteženega uvajanja novih policijskih pooblastil in tehničnih sredstev, s katerim lahko izboljšamo transparentnost uvajanja policijskih pooblastil z omogočanjem javne razprave, okrepimo legitimnost in podlage za naknadno vrednotenje sprejetih policijskih pooblastil ter pripomoremo k večji uravnoteženosti policijskih pooblastil in temeljnih človekovih pravic. **Pri Informacijskem pooblaščencu upamo, da bodo predlagatelji novih policijskih pooblastil spoznali, da je uporaba v smernicah predstavljene metodologije za izvedbo presoje vplivov na zasebnost v prvi vrsti v njihovem interesu.**