



Univerza v Mariboru

Fakulteta za varnostne vede

DIPLOMSKO DELO UNIVERZITETNEGA ŠTUDIJA
Spolne zlorabe otrok na internetu in pravne možnosti za uporabo
prikritih preiskovalnih ukrepov

Avgust, 2014

Tina Kurent

Mentorica: doc. dr. Danijela Frangež

Somentor: Anton Toni Klančnik, mag.

Zahvala

Ob uspešnem zaključku študija se iskreno zahvaljujem mentorici, doc. dr. Danijeli Frangež in somentorju Antonu Toniju Klančniku, mag., ki sta me v času pisanja diplomske naloge usmerjala ter mi bila vedno na razpolago s svojimi napotki in predlogi pri pisanju.

Posebna zahvala gre moji družini, ki mi je omogočila študij in me najbolj vzpodbujala in mi pomagala s svojimi nasveti.

Iskrena hvala tudi fantu in prijateljem, ki so mi ves čas študija stali ob strani.

Hvala!

Kazalo

1	Uvod	7
1.1	Namen in cilji	8
1.2	Hipoteze.....	8
1.3	Uporabljene raziskovalne metode.....	8
2	Opredelitev temeljnih pojmov	10
2.1	Otrok.....	10
2.2	Spolna zloraba otrok	10
2.3	Internet.....	11
2.3.1	Spletna (online) tveganja.....	12
2.3.2	Spletno nadlegovanje	12
2.3.3	Spletna pošta, spam pošta	13
2.3.4	Spletne klepetalnice	13
2.4	Tipologija storilcev spolnih zlorab	14
2.5	Statistika v Sloveniji.....	15
2.5.1	Spletno oko	15
3	Pravne podlage za pregon spletnih spolnih zlorab otrok v Sloveniji.....	17
3.1	Nacionalni dokumenti.....	17
3.1.1	Kazenski zakonik RS (KZ-1)	17
3.2	Mednarodni dokumenti.....	17
3.2.1	Konvencija o otrokovih pravicah	18
3.2.2	Izbirni protokol h Konvenciji o otrokovih pravicah glede prodaje otrok, otroške prostitucije in otroške pornografije.....	18
3.2.3	Konvencija o kibernetiski kriminaliteti.....	19
3.2.4	Konvencija Sveta Evrope o zaščiti otrok pred spolnim izkoriščanjem in spolnim zlorabljanjem	20
3.2.5	Direktiva 2011/93/EU Evropskega parlamenta in Sveta z dne 13. decembra 2011 o boju proti spolni zlorabi in spolnemu izkoriščanju otrok ter otroški pornografiji in nadomestitvi Okvirnega sklepa Sveta 2004/68/PNZ	20

4 Prikriti preiskovalni ukrepi v Sloveniji in zlorabe otrok	22
4.1 Tajno opazovanje (149.a člen ZKP)	23
4.2 Pridobivanje podatkov oziroma izpis podatkov iz elektronskega komunikacijskega omrežja (149.b člen ZKP)	26
4.3 Nadzor elektronskih komunikacij s prisluškovanjem in snemanjem ter kontrola in zavarovanje dokazov o vseh oblikah komuniciranja, ki se prenašajo v elektronskem komunikacijskem omrežju (1. točka prvega odstavka 150. člena) ...	28
4.4 Kontrola pisem in drugih pošilk (2. točka prvega odstavka 150. člena).....	28
4.5 Prisluškovanje in snemanje pogovorov s privolitvijo vsaj ene osebe, udeležene v pogovoru (4. točka prvega odstavka 150. člen ZKP).....	29
4.6 Prisluškovanje in opazovanje v tujem stanovanju ali drugih tujih prostorih, z uporabo tehničnih sredstev za dokumentiranje in po potrebi s tajnim vstopom v navedene prostore (151. člen ZKP)	30
4.7 Tajno delovanje (155.a člen ZKP)	32
4.8 Skupne značilnosti PPU	34
4.9 Primer uporabe PPU	35
5 Razprava	37
6 Zaključek.....	52
7 Uporabljeni viri.....	55

Povzetek

V diplomskem delu obravnavamo tematiko spolnih zlorab otrok na internetu in pravne možnosti za uporabo prikritih preiskovalnih ukrepov.

Spolna zloraba otrok na internetu je eno od področij kriminalitete z največjim temnim poljem, saj predstavlja glavni problem obravnavanja kaznivega dejanja, kako se dokopati do materialne resnice. Naša in tudi evropska zakonodaja ščitita otroke oziroma mladoletnike in v predpisih točno opredeljujeta, katera so kazniva dejanja zoper spolno nedotakljivost, kakšni so zakonski znaki, ki definirajo takšna dejanja, in kazni, ki so za to predpisane. Navsezadnje pa tudi zakonodaja ne pomaga, če takšna dejanja ostanejo skrita, zato utegnejo biti prikriti preiskovalni ukrepi (v nadaljevanju PPU) ključna sestavina za odkrivanje in preprečevanje kriminalitete zoper spolno nedotakljivost otrok v povezavi s kibernetiskim prostorom oziroma s pomočjo interneta.

V osrednjem delu naloge smo prikazali tipičen način storitve kaznivega dejanja s tega področja in enega od načinov in postopkov odkrivanja, s katerimi se srečujejo vladne organizacije v predkazenskem postopku. Ker gre za občutljivo področje, ki v veliki meri posega v človekove pravice in svoboščine, vsaka posamezna uporaba PPU pa vzbuja velik odziv javnosti, smo se v diplomskem delu osredotočili na pravno ureditev v Republiki Sloveniji in njeno problematiko odkrivanja, zbiranja in dokazovanja zlorab in nasilja nad otroci (zlasti v primeru spoprijateljavanja storilcev z otroki preko interneta). Pri tem poskušamo predstaviti, katere varovalke je zakonodajalec uzakonil, da bi preprečil nedovoljeno uporabo PPU, in katera pravna sredstva imamo na voljo zoper takšno dejanje, saj se organi odkrivanja in pregona vse pogosteje srečujejo s specifičnimi težavami pri odkrivanju internetnih storilcev spolnih zlorab otrok.

Ključne besede: otrok, spolna zloraba, internet, IK tehnologija, zakonodaja, prikriti preiskovalni ukrepi, analiza primera.

Summary: Online child sexual abuse and legal possibilities for the use of covert investigative measures

In the thesis, we discuss the issue of online child sexual abuse and legal possibilities for the use of covert investigative measures.

Online child sexual abuse is one of the fields of criminality with the largest dark field, since the main problem of the discussed crime investigation is how to determine the substantive truth. Our legislation as well as the European one protects children or minors and through regulations exactly defines crimes against sexual inviolability, statutory signs, which define such crimes, and penalties for them. At the end, even the legislation does not help, if such acts remain hidden, therefore covert investigative measures (in continuation CIM) could be of key-importance in identifying and preventing of crime against sexual inviolability of children in connection with the cyberspace or the internet.

In the main part of the thesis we presented a typical committing of crime from this field and one of the ways and procedures of its detection, faced by governmental organization in pre-trials. Because it is a sensitive area that heavily interferes with human rights and freedoms and every single use of CIM provokes a great public response, we focused on legal regulations in the Republic of Slovenia and the issue of identification, collection and proving of child abuse and violence against them (in particular online grooming case). By doing so we tried to present, which safety measures were legislated by the legislator in order to prevent unauthorized use of CIM and which legal means do we have against such acts, since law enforcement authorities increasingly face specific problems in identifying online child sexual offenders.

Keywords: child, sexual abuse, internet, IC technology, legislation, covert investigative measures, case study.

1 Uvod

V zadnjih nekaj desetletjih lahko v medijih, člankih, na predavanjih in drugje zasledimo številne informacije o škodljivih posledicah rabe interneta. Zaradi svoje globalne narave omogoča kriminalcem visoke možnosti prikrivanja identitete, hitrega prenosa podatkov in široke dostopnosti, torej predstavlja idealno gojišče različnih protipravnih aktivnosti, kot so: veliko število napadov na računalniške sisteme, kraj identitet, distribucije posnetkov s spolno vsebino, goljufij kot tudi uvajanja virusov in e-poštne prevare (Interpol, 2014). Tako se lahko povežejo v skoraj vse nezakonite dejavnosti po svetu, kar predstavlja resno grožnjo nacionalni in mednarodni varnosti.

Po podatkih Statističnega urada Republike Slovenije je pri nas v letu 2012 skoraj 99 odstotkov otrok, starih deset let ali več, redno uporabljalo računalnik, le malo manj internet (Razpotnik, 2012). Najraje ga uporabljajo za klepetanje, dostop do filmov in glasbe, učenje ali kot vir informacij, ki jih potrebujejo za izdelavo šolskih projektov (Stanley, 2001). Po drugi strani pa je odprl vrata tudi raznim storilcem kaznivih dejanj, ki ga uporabljajo za navezovanje stikov, komunikacijo z otroki, izmenjavo gradiva s spolnimi zlorabami otrok (angl. child sexual abuse material; v nadaljevanju CAM); le vprašanje časa pa je tudi, kdaj storilec doseže svoj cilj, ki je srečanje z otrokom v živo z namenom spolne zlorabe.

V Zakonu o spremembah in dopolnitvah Kazenskega zakonika (2011; v nadaljevanju KZ-1B) je pod kaznivimi dejanji zoper spolno nedotakljivost zapisana oblika tovrstnega spolnega nasilja, ko nagovarjanju z otrokom preko računalnika sledi srečanje, z namenom spolne zlorabe. Gre za kaznivo dejanje pridobivanja oseb, mlajših od 15 let, za spolne namene (angl. grooming), ki je opredeljeno v 173.a členu KZ-1B in mednarodnih virih, kot je Konvencija Sveta Evrope o zaščiti otrok pred spolnim izkoriščanjem in spolnim zlorabljanjem (2007).

Spolne zlorabe otrok sodijo med huda kazniva dejanja, ki jih zakonodaje različnih držav različno opredeljujejo, v vsakem primeru pa jih razumejo kot družbeno škodljive in jih sodno preganjajo. Kot učinkovit način odkrivanja storilcev tovrstnih kaznivih dejanj, ko so otroci žrtve internetne zlorabe, ima policija možnost uporabljati tudi prikrite preiskovalne ukrepe, pri njihovi uporabi pa je treba najti pravo mero med pravičnostjo in legalnostjo na eni strani ter varstvom človekovih pravic na drugi strani. V tem pogledu je pomembno vedeti, da dobra zakonodaja sama po sebi še ne zagotavlja ustreznega obravnavanja določenega ravnanja storilca

v družbi, ampak je enako pomembno kakovostno izvajanje zakonov in pravilno izvajanje kriminalističnih aktivnosti z namenom preiskati kazniva dejanja.

1.1 Namen in cilji

Namen diplomske naloge je podrobna opredelitev sklopa prikritih preiskovalnih ukrepov, ki jih je moč uporabiti pri učinkovitemu odkrivanju storilcev spolnih zlorab otrok na internetu, s poudarkom na kaznivem dejanju novačenja oziroma pridobivanja mladoletnih oseb za spolne namene. Na podlagi predstavljenega primera smo opisali pogoje, omejitve, pravno podlago ukrepov in njihovo aplikacijo v praksi, predvsem pa smo ugotavljali, ali sme slovenska policija izvajati takšne PPU pri kaznivem dejanju pridobivanja oseb, mlajših od 15 let, za spolne namene (groominga).

1.2 Hipoteze

Izhodišča oziroma delovni hipotezi, iz katerih bomo izhajali, so:

1. Slovenska zakonodaja omogoča učinkovito izvajanje prikritih preiskovalnih ukrepov za pregon kaznivega dejanja »groominga«.
2. Z uporabo prikritih preiskovalnih ukrepov za pregon kaznivih dejanj na škodo otrok se zelo kršijo pravice storilcev teh kaznivih dejanj.

Po pregledani literaturi, zakonodaji ter skozi analizo primera bo predpostavka potrjena ali ovržena z ustreznimi argumenti.

1.3 Uporabljene raziskovalne metode

V okviru deskriptivnega pristopa bomo uporabili komparativno metodo in metodo kompilacije. Komparativno metodo bomo uporabili za opis prednosti in pomanjkljivosti interneta. Z metodo kompilacije bomo povzeli stališča in sklepe številnih avtorjev s področja spolnih zlorab otrok na internetu, na podlagi česa bomo

prišli do novih, samostojnih sklepov. Pri tem bomo uporabili strokovno literaturo domačih in tujih avtorjev, članke iz revij, spletno gradivo, sodno prakso in zakonodajo.

2 Opredelitev temeljnih pojmov

Število spolnih zlorab nad otroki se v zadnjih letih povečuje, predvsem na račun interneta in sodobne informacijsko-komunikacijske tehnologije, kot so družbeni mediji in tehnologija mobilne telefonije. Gre za izredno dobičkonosen kriminalni posel, ki za sabo pušča hude posledice, saj otroke zaznamujejo za celo življenje (Otroci nas nemo ..., 2014).

V tem poglavju obravnavamo temeljne pojme, povezane s spolnimi zlorabami otrok, navajamo razloge problematičnosti uporabe interneta, sledi pregled tipologije spletnih storilcev in na koncu poglavja še statistični pregled problematike v Sloveniji.

2.1 Otrok

Beseda otrok je v 1. členu Konvencije o otrokovih pravicah (1989) opredeljena kot »vsako človeško bitje, mlajše od osemnajst let«. V Sloveniji določa Kazenski zakonik (2008; v nadaljevanju KZ-1) v 173. členu starostno mejo petnajst let, s katero mladoletna oseba lahko pristane na prostovoljni spolni odnos ali aktivnost. Bošnjak (1998) razlaga, da je mladoletna oseba pri petnajstih letih zmožna samostojno privoliti v spolne aktivnosti s pridobitvijo drugih pravic, ki jih določajo delavnopravna, družinskopravna in zdravstvena zakonodaja.

2.2 Spolna zloraba otrok

Spolna zloraba otrok je dejanje, ko se odrasli ali starejši mladostnik otroka dotika na način, da se spolno vzburi in otroka uporabi za zadovoljitev svojih seksualnih potreb. Načini in aktivnosti so pri tem početju zelo različni, vsem pa je skupno to, da odrasel zlorabi svojo moč in avtoriteto ter da otroka zavede ali celo na silo potisne v seksualno aktivnost (Bain in Sanders, 1996). Osredotočili se bomo na pregled problematike spolnih zlorab preko interneta, ki storilcem omogoča enostavnejši in hiter dostop do navezovanja stikov in pridobivanja oseb, mlajših od petnajst let, za spolne namene, ter posnetkov s spolnimi zlorabami otrok. Posnetke spolne zlorabe definiramo »kot vizualno prikazovanje in/ali uporabo mladoletnika za vzburljanje erotičnih občutij pri odrasli osebi. Mladoletna oseba je pri tem različno razgaljena.«

Osebe na posnetkih so v običajnih ali erotičnih pozah, pogosto same, v družbi z otrokom ali z odraslo osebo (Frangež in Dvoršek, 2012: 70).

2.3 Internet

Internet je računalniško omrežje, ki omogoča povezavo milijone uporabnikom, in ker je dosegljivo kjerkoli po svetu, ob predpostavki, da imamo ustrezno komunikacijsko opremo, za dostop ni individualne odgovornosti in direktnega nadzora nad njegovo vsebino (Rajšp, 2008). Zaradi svoje enostavnosti uporabe omogoča dostop do informacij, do pregleda elektronske pošte (angl. e-mail) in prenosa datotek (slik, filmov in glasbe), pisanja blogov, enostavno komuniciranje v klepetalnicah (angl. chat rooms), prenosa pogovora v živo (IRC), poslušanja glasbe, igranja iger, pregledovanje dokumentov in različne storitve (plačevanje položnic, kupovanje v spletnih trgovinah, oglaševanje). Kljub številnim prednostim ima svetovni splet tudi svojo temno stran, zaradi česar prihaja do številnih zlorab. Zaradi svoje hitrosti, anonimnosti in priročnosti se tisti, ki iščejo CAM, lažje, hitreje in prikrito povezujejo (Skrt, 2004). Stanley (2001) nadaljnje navaja, da je internet problematičen tudi zato, ker otroci prek njega najlažje pridejo do vsebine, ki je namenjena odraslim osebam. Na internetu ni določenih pravil ali avtoritet, vsakdo lahko govori ali se izdaja za drugo osebo, in tega mu nihče ne more preprečiti. Pri uporabi interneta se je treba zavedati posledic, saj lahko vodijo v čustveno, spolno in fizično zlorabo uporabnika.

Kodelja in Banovič (2012) ugotavljata, da ima internet globoke razsežnosti, ki se jih popolnoma ne zavedamo. Temno omrežje (angl. darknet) predstavlja omrežje, ki omogoča izmenjavo CAM, kjer so povezave sklenjene med zaupanja vrednimi gostitelji. Temno omrežje je dostopno preko programa, imenovanega Tor (angl. the onion router), ki omogoča visoko stopnjo anonimnosti storilcem kaznivih dejanj nagovarjanja otrok preko spleta, z namenom spolne zlorabe. Gre za enega od glavnih problemov, ki otežuje delo preiskovalcem, ki so na sledi storilcem, ki po spletu pošiljajo CAM (Kodelja in Banovič, 2012).

Pri obiskovanju spleta moramo biti izredno previdni, katere spletne strani obiskujemo, zato bomo v nadaljevanju predstavili nevarnosti, ki pretijo na radovedne, zaupljive, neizkušene in naivne otroke.

2.3.1 Spletna (online) tveganja

Spletna tveganja, ki pretijo na posameznike na internetu, lahko po pogostosti razdelimo po naslednjem vrstnem redu (Naši otroci ..., 2008):

- razkrivanje osebnih informacij,
- srečanje s spolno vsebino otrok,
- srečanje škodljivih in nasilnih vsebin,
- biti žrtev nadlegovanja, zasledovanja, žaljenja,
- sprejemanje neželenih seksualnih komentarjev,
- osebno srečevanje spletnih znancev in neznancev.

Skrt (2004) meni, da storilci porabijo ogromno časa, denarja in energije, da dosežejo svoj cilj, ki je srečanje z otrokom v resničnem svetu. V ta namen uporabljajo spletne klepetalnice, kjer se predstavijo pod lažnim vzdevkom in že začnejo graditi na zaupanju. Storilci spolnih zlorab med seboj tudi komunicirajo; s tem ustvarijo močne mreže po vsem svetu in jih je skoraj nemogoče ustaviti. Pri tem sodelujejo in si izmenjujejo mnenja z isto mislečimi, saj si na ta način pridobijo občutek sprejetja, da niso sami v svoji perverzности. Tako izmenjavo materiala zasledimo v novičarskih skupinah. Novičarske skupine so predstavljene kot forumi, v katerih člani razglabljajo in si med seboj lahko pošiljajo gradivo s spolno vsebino. Večina strežnikov ne dopušča dostopa do teh vsebin oziroma imajo blokiran dostop, nekateri pa omogočajo dostop na lastno odgovornost, saj pri tem tvegajo razkritje svoje identitete bodisi z IP naslovom na strežniku. Pri iskanju spletnih strani s spletno vsebino naletimo na več preprek, saj se te nezakonite strani zelo hitro selijo skozi države s spreminjanjem IP naslova.

2.3.2 Spletno nadlegovanje

Kodelja in Banovič (2010) ugotavljata, da gre pri spletnem nadlegovanju (angl. online bullying) za nadlegovanje, ki poteka s pomočjo elektronske tehnologije. Elektronska tehnologija vključuje naprave in pripomočke, kot so mobilni telefoni in računalniki, preko katerih se nalagajo (angl. upload) slike, videoposnetki, spletne strani ali lažni profili, z namenom razširjanja seksualnega gradiva, ki prikazuje mladoletne osebe, ki so pomanjkljivo oblečeni ali goli. Otroci so še posebej izpostavljeni v spletnih klepetalnicah, kjer jih kaj hitro zavedejo osebe na drugi strani računalnika, ki se lahko predstavljajo kot njihovi sovrstniki. Vsa ta igra z vidika storilca vodi k enemu

skupnemu cilju, to je srečanju v realnem svetu. Problem spletnega nadlegovanja je, da se neprimerne vsebine, objavljene slike ali video posnetke težko zbrise, prav tako je včasih težko izslediti vir.

2.3.3 Spletna pošta, spam pošta

Elektronska pošta (angl. E-mail) je način sprejemanja in pošiljanja sporočil po spletnih elektronskih sistemih. Je eden od najpomembnejših razlogov, zakaj se je večina ljudi odločila, da se povežejo z internetom, ker se pridobi ogromno na času, saj se lahko pošlje neposredno z računalnika, brez kupovanja znamk in odnašanja v poštni nabiralnik (Komuniciranje na internetu, 2013). Ima pa tudi neželene učinke. Storilci kaznivih dejanj jo lahko uporabljajo za svoje nelegalne posle, pošiljanje grozljivih sporočil, v skrajnem primeru tudi za pošiljanje gradiva s spolno vsebino otrok. Ena od slabih lastnosti spletne pošte je tudi neželena pošta oziroma spam. Gre za spletno pošto, ki jo nehote dobimo v svoj spletni poštni nabiralnik in lahko vsebuje CAM, katere namen je predvsem vsiljevanje vsebine, ki je večina uporabnikov ne bi želela prejeti (Spam: nenaročeno oglaševanje ..., 2014). Spolni nadlegovalci so prišli že tako daleč, da na raznih forumih, spletnih klepetalnicah, IRC-u najdejo naslove elektronske pošte otrok in jim tako pošiljajo gradiva s tako vsebino ali želijo priti z njimi v stik za nadaljnje izvrševanje spolnih kaznivih dejanj.

2.3.4 Spletne klepetalnice

Le malokdo od otrok ali mladostnikov ne pozna spletnega klepetanja preko Messengerjev, klepetalnic, Facebooka, IRC-a, Skypa itd. Klepetalnica je prostor na spletu, kjer se odvija odprt pogovor (angl. chat), izmenjava mnenj med dvema ali več osebami z vsega sveta. Uporabniki so ponavadi med seboj razvrščeni glede na starost, temo ali spolno usmerjenost. Klepetanje poteka hitro, z uporabo krajšav in angleških izpeljank, svoje razpoloženje pa lahko popestrimo z uporabo smeškov (angl. smilies), ki prikazujejo čustveno stanje tistega, ki piše (Komuniciranje na internetu, 2013). Stanley (2001) ugotavlja, da spletne klepetalnice uporabnikom omogočajo veliko stopnjo anonimnosti, saj je edina stvar, ki jo morajo uporabniki storiti ob registriranju izbira vzdevka. Anonimnost lahko predstavlja veliko prednost, za ljudi, ki so v resničnem svetu sramežljivi, ki se tako lahko sprostijo in se brez težav ter sramu pogovarjajo. Na drugi strani, pa to lahko izkoriščajo storilci, ki se

navdušujejo nad CAM, saj se skriti pod nedolžnimi vzdevki, lažnimi identitetami in prekrivanjem nepopolnih in zmotljivih osebnih lastnosti, kot je recimo starost, predstavljajo za sovrstnike otrok. Storilci so seznanjeni z najnovejšimi modnimi trendi, katerim sledijo otroci na vseh področjih in pri tem uporabljajo slengovsko govorico, saj s tem zakrijejo svojo dejansko starost (Carr, 2003). Za žrtev si izberejo otroka, ki je ranljiv, z nižjo stopnjo samozavesti ali pa je brez starševskega nadzora. Storilec sprva poskuša direktno nagovoriti otroka ter ga pri tem poskuša prefinjeno napeljati, da zapusti spletno klepetalnico in z njim nadaljuje pogovor v tako imenovani zasebni konferenci (Carr, 2003). Zorko (2009) opozori, da storilci pri tem uporabljajo metodo zapeljevanja otrok, ki se imenuje mehčanje (angl. groomnig), s katero vzpostavi poseben odnos. Ko storilcu uspe pridobiti zaupanje žrtve in trdno vez prijateljstva, sledi medsebojna komunikacija preko e-pošte, izmenjava SMS sporočil ali direktni pogovor preko interneta z uporabo slušalk ali spletne kamere. Ključnega pomena za storilce, da njuna zveza ostane tajna, je, da se le-ta prepriča, na katerem mestu v stanovanju oziroma hiši se nahaja računalnik, katerega uporablja žrtev za komuniciranje preko spleta. Storilec se tudi prepriča, da se o tovrstnih pogovorih ne ustvarja zgodovina, kar pomeni, da bo možnost komunikacijskega programa za shranjevanje zgodovine izključena. Kajti prej ko slej bo storilec seksualiziral vedenje oziroma pogovor in ne bo želel, da bi se pri tem ohranil kakršen koli dokaz, ki bi ga kasneje izdal ali pričal proti njemu (Carr, 2003). Med otrokom in storilcem se kasneje razvije seksualni odnos, otroka poučuje o goloti in spolnosti, kaj kmalu pa ta preide v spolne odnose. Njihovo delovanje je od samega začetka usmerjeno k enemu cilju: srečanju z otrokom v resničnem življenju z namenom spolne zlorabe.

2.4 Tipologija storilcev spolnih zlorab

Kovačič in Klančnik (2012) predstavita tipologijo Michaela Morana, ki jo je razvil na podlagi izkušenj pri spremljanju spletnih spolnih prestopnikov. Kategorije si sledijo v obliki trikotnika:

Prvo raven predstavljajo gledalci oziroma začetniki (angl. Simple Viewers), željni radovednosti, zato si na internetu ogledujejo gradivo, ki prikazuje spolne prizore z otroki. Ob tem se samozadovoljujejo in kasneje, po končanem ogledu, prekinejo s tovrstnim dejanjem. Ponavadi plačujejo za dostop do takega gradiva. Drugo raven predstavljajo ljudje iz odprtega kroga, kršitelji (angl. Open Traders), ki delujejo

odkrito – gre za uporabnike omrežij P2P (eMule, Bit Torrent ..). Njihovo delovanje je usmerjeno v skrito trgovanje z gradivom. Ker je tovrstnih odjemalcev ogromno, jih je nemogoče izslediti. S tovrstnima oblikama kaznivih dejanj naj bi se spopadali običajni policisti. Naslednji dve ravni pa predstavljata zaprto trgovanje (angl. Closed Traders) in strokovnjaki (angl. Experts). Zaprti trgovci so distributerji nezakonitih spletnih strani z CAM. Zadnjo, najvišjo raven sestavljajo strokovnjaki, ki so dolgoročno zavzeti storilci. Ti so na vrhu piramide. V svoj krog povabijo samo posameznike, ki se jim zdijo pomembni in vredni zaupanja, saj jim je visoka varnost na prvem mestu. Preden se odločijo, da osebo sprejmejo v svoj ožji krog, se jim mora ta dokazati s CAM. Na podlagi dobljenega gradiva lahko profilirajo posameznika, saj ta prikazuje njegovo osebnost. Slednji zahtevajo uporabo strokovnih enot, ki so ustrezno usposobljene na tem področju. Gre za strokovnjake, t. i. tajne policijske delavce, ki morajo biti del njihove skupnosti, poznati morajo njihovo geslo in delovati pod krinko – predvsem pa morajo imeti sposobnost, da najdejo storilce spolnih zlorab otrok na internetu.

2.5 Statistika v Sloveniji

Uradna policijska statistika kaže, da se v Sloveniji v zadnjih letih povečuje število kaznivih dejanj nasilja nad otroci; letno je prijavljenih 200 kazenskih ovadb zaradi spolnega napada na osebo, mlajšo od petnajst let. Vznemirljiv podatek je, da so številke naraščajoče, po drugi strani pa so lahko odraz povečanih aktivnosti in prizadevanj policije, prilagojene in bolj prijazne zakonodaje ter povečanja občutljivosti in ozaveščenosti ljudi (Otroci nas nemo ..., 2014). V Sloveniji je letno podanih približno 300 prijav oziroma informacij o sumih, da so otroci žrtve spolnih zlorab, v približno 20 % obravnavanih kaznivih dejanj otroci storilca spoznajo naknadno, preko spleta, kjer si le-ti prizadevajo pridobiti dostop do otroka, da lahko lažje izvršijo svoje dejanje (Problematika spolnih ..., 2008).

2.5.1 Spletno oko

Na spletni strani safe.si se nahaja prijavna točka Spletno oko, ki omogoča slovenskim uporabnikom interneta anonimno prijavo nelegalne vsebine, ki jo zasledijo s spolnimi prizori otrok ali kakršen koli sovražen govor na spletu. Namen tovrstnega projekta je predvsem pregon in umik sporne vsebine s spleta, identifikacija storilcev spolne

zlorabe ter izsleditev razpečevalcev takšnih vsebin. Prijavna točka Spletno oko tesno sodeluje z vsemi pristojnimi organi v naši državi, ki se ukvarjajo s podobno problematiko. Deluje v okviru Centra za varnejši internet, ki ga koordinira Univerza v Ljubljani, Fakulteta za družbene vede, v tem pa delujeta konzorcij in Svet Centra za varnejši internet (v nadaljevanju Svet CVI). Konzorcij se ukvarja z vsemi organizacijskimi vprašanji, v Svetu CVI pa delujejo predstavniki tistih institucij, ki aktivno delujejo na področju zagotavljanja spletne varnosti ter zaščite otrok in mladostnikov pri uporabi interneta in ostalih tehnologij oziroma se zavzemajo za zmanjšanje obsega nezakonitih vsebin na spletu (Svet Centra ..., 2014). Pri projektu kot člana Sveta CVI sodelujeta tudi Vrhovno državno tožilstvo Slovenije in Policija, ki skrbita za hitro in učinkovito obravnavo prejetih prijav, ter mediji in ostale organizacije na področju varovanja pravic otrok. V letu 2012 je Spletno oko obravnavalo 18 prijav gradiv s spolnimi zlorabami otrok, za katere je bilo ugotovljeno, da gostujejo na slovenskih strežnikih, od tega jih je bilo 10 uspešno odstranjenih po posredovanju policije in ponudnikov internetnih storitev (Kdo smo ..., 2014). K reševanju in preprečevanju konkretnih objav CAM na svetovnem spletu pripomore kakovostno sodelovanje Policije s prijavno točko Spletno oko, tudi v primeru, da bi bili na spletu objavljeni posnetki iz spolnih zlorab otrok ob t. i. metodi zapeljevanja otrok.

3 Pravne podlage za pregon spletnih spolnih zlorab otrok v Sloveniji

Spolne zlorabe otrok na internetu predstavljajo hudo kršitev človekovih pravic in temeljnih pravic otrok do ustrezne vzgoje in razvoja. V nadaljevanju se bomo osredotočili na dokumente, ki krepijo informativnost, ozaveščenost, prepoznavnost, razsežnost, predvsem pa pravice otrok pred spolnim izkoriščanjem in zlorabljanjem na internetu.

3.1 Nacionalni dokumenti

Predstavili bomo posamezne dokumente, s pomočjo katerih se Slovenija sooča s problemom razsežnosti spolnih zlorab otrok na internetu.

3.1.1 Kazenski zakonik RS (KZ-1)

KZ-1 (2008) v 19. poglavju vsebuje določbe, katerih namen je zavarovati duševno, telesno in zlasti spolno nedotakljivost otrok v naslednjih členih: posilstvo – 170. člen, spolno nasilje – 171. člen, spolna zloraba slabotne osebe – 172. člen, spolni napad na osebo, mlajšo od 15 let – 173. člen, kršitev spolne nedotakljivost z zlorabo položaja – 174. člen, zloraba prostitucije – drugi odstavek 175. člena, prikazovanje, izdelava, posest in posredovanje pornografskega gradiva – 176. člen, in kot zadnje trgovina z ljudmi – 113. člen. Z novelo KZ-1B (2011) je inkriminirano novo kaznivo dejanje v 173.a členu, ki se glasi: pridobivanje oseb, mlajših od petnajst let, za spolne namene. Opredeljena je tudi posebna kazenska evidenca, ki se nanaša na obsodbe za spolna kazniva dejanja (84. člen KZ-1), na podlagi katere se lahko preverja ustrezne zadržke oziroma prepovedi kakršnega koli dela z otroki (Klančnik, 2013a).

3.2 Mednarodni dokumenti

V nadaljevanju bodo opisani mednarodni in nekateri evropski akti, katerih osnovni namen je zagotavljanje pravic otrok ter njihova zaščita, mednarodno sodelovanje

med preiskovalnimi agencijami in ustreznost preiskovalnih orodij, nekateri izmed njih pa določajo tudi določila glede spolne nedotakljivosti otrok.

3.2.1 Konvencija o otrokovih pravicah

V Konvenciji o otrokovih pravicah (1992; v nadaljevanju KOP) morajo države pogodbenice otrokom zagotoviti ustrezne pravice in ukrepe, ki so definirani v boju proti spolnemu izkoriščanju in spolnim zlorabam. Konvencija opredeljuje štiri glavna načela, ki so: nediskriminacija, najboljša korist otroka, preživetje in zaščita, participacija ter soudeležba otrok. Pri vseh ukrepih, ki jih izvajajo organi državne bodisi zasebne ustanove za socialno varstvo, sodišča, upravni organi ali zakonodajna telesa, morajo biti otrokove koristi glavno vodilo (3. člen KOP). Države članice morajo imeti zagotovljene ustrezne ukrepe, s katerimi bodo varovale otroka pred vsemi oblikami nasilja, poškodb, zlorab, vključno s spolnimi zlorabami. Otrokom morajo nuditi zaščito pred spolnim izkoriščanjem in spolnimi zlorabami ter preprečiti prisiljenje otrok h kakršnikoli nezakoniti spolni dejavnosti, izkoriščanju otroka v prostituciji in pornografskih gradivih ali drugih nezakonitih spolnih dejavnostih (34. člen KOP). Z ustreznimi državnimi, bilateralnimi in multilateralni ukrepi morajo zaščititi otroke pred kakršnimi koli oblikami zlorabe (35. člen KOP).

3.2.2 Izbirni protokol h Konvenciji o otrokovih pravicah glede prodaje otrok, otroške prostitucije in otroške pornografije

Namen Izbirnega protokola h Konvenciji (2004) je zagotavljanje in uresničevanje pravic otrok, ki jih zagotavlja osnovna Konvencija. Poleg kaznivih dejanj, ki jih zagotavlja osnovna Konvencija, vsebuje Izbirni protokol h Konvenciji, dodatno kaznivo dejanje, ki se imenuje spolni turizem¹. Države članice morajo inkriminirati kazniva dejanja, ki so: prodaja otrok, otroška prostitucija in otroška pornografija in globalni problem spolnih zlorab otrok na internetu (1. člen Izbirnega protokola h Konvenciji, 2004). V boju proti tovrstnim kaznivim dejanjem države pogodbenice ukrenejo vse potrebno za krepitev mednarodnega sodelovanja z večstranskimi, regionalnimi in dvostranskimi dogovori za preprečevanje, odkrivanje, preiskovanje,

¹ Poudariti je treba, da gre za neustreznost rabe termina spolni turizem. V ta namen je predlagan nov izraz turistična potovanja z namenom spolne zlorabe ali izkoriščanja otroka (angl. travelling for the purpose of sexual abuse or exploitation of children (Klančnik, 2013b).

preganjanje in kaznovanje tistih, ki so odgovorni za dejanja, ki vključujejo prodajo in pospešujejo mednarodno sodelovanje in usklajevanje med svojimi organi oblasti, nevladnimi organizacijami v državi in mednarodnimi nevladnimi organizacijami ter mednarodnimi organizacijami (10. člen Izbirnega protokola h Konvenciji, 2004).

3.2.3 Konvencija o kibernetiski kriminaliteti

Konvencija o kibernetiski kriminaliteti (2004) je prvi mednarodni pravni akt, ki določa okvir mednarodnega sodelovanja in medsebojne pomoči na področju boja proti z računalnikom povezani kriminaliteti – kibernetiski kriminaliteti. Pogodbenice sprejmejo potrebne zakonodajne in druge ukrepe v notranjem pravu, s katerimi kot kazniva opredelijo dejanja kršitve avtorskega prava, goljufije s pomočjo računalniških programov in opreme, spolne zlorabe otrok na internetu (sicer navaja besedno zvezo otroška pornografija):

- a) izdeluje otroško pornografijo ²z namenom njenega razširjanja po računalniškem sistemu;
- b) ponuja ali omogoča dostop do otroške pornografije po računalniškem sistemu;
- c) razširja ali prenaša otroško pornografijo po računalniškemu sistemu;
- d) zagotavlja otroško pornografijo po računalniškemu sistemu zase ali za drugo osebo;
- e) poseduje otroško pornografijo v računalniškemu sistemu ali na sredstvu za shranjevanje računalniških podatkov (Klančnik, 2013a).

Njen temeljni cilj izhaja iz preambule – gre za prizadevanja vseh za skupno kazensko politiko in zaščito družbe proti kibernetiski kriminaliteti s sprejemanjem ustrezne zakonodaje za odkrivanje in pregon ter tudi s kakovostnim mednarodnim sodelovanjem (Klančnik, 2013a).

² Na tem mestu je treba poudariti, da gre prav tako za neustreznost rabe termina otroška pornografija in navesti, da je predlagani termin posnetki spolne zlorabe otrok, saj spolna zloraba ni nikakršna pornografija. Beseda pornografija se uporablja zgolj za sporazumne in prostovoljne posnetke spolnih odnosov med odraslimi, ki se praviloma zakonito distribuirajo javnosti za zadovoljevanje njenih potreb. Podobe spolnih zlorab otrok to niso, saj prikazujejo otroke, ki ne morajo dati ustreznega ali potrebnega soglasja, saj so žrtve kaznivega dejanja. Da v prihodnje ne bo prihajalo do napačne interpretacije, je treba opozarjati na pomen ustreznega izrazoslovja in da povsod, kjer je možno, pojasnimo pravilno rabo terminov (Klančnik, 2013b).

3.2.4 Konvencija Sveta Evrope o zaščiti otrok pred spolnim izkoriščanjem in spolnim zlorabljanjem

Konvencija Sveta Evrope o zaščiti otrok pred spolnim izkoriščanjem in spolnim zlorabljanjem (2007) je prvi in najvišji mednarodni pravni dokument za zaščito otrok pred spolnim izkoriščanjem in spolnim zlorabljanjem. Njena naloga je spodbujanje mednarodnega sodelovanja držav podpisnic na državni in mednarodni ravni za namene preprečevanja in boja proti spolnemu izkoriščanju, zlorabljanju otrok, prostituciji in trgovanju z otroki ter pomoči žrtvam in preiskav ali postopkov, ki se nanašajo na kazniva dejanja, ki so opredeljena. Inkriminira tudi uporabo informacijskih in komunikacijskih tehnologij, ki so v zadnjih časih zaskrbljivo pojav, saj preko interneta storilci hitro navežejo stike z otroki. Vsaka pogodbenica mora izvesti zakonodajne ali druge preventivne in zaščitne postopke, s katerimi zagotovi, da se inkriminirajo vse zgoraj opisane oblike kaznivih dejanj. Vsak otrok ima pravico, da mu družina, družba in država zagotovijo ukrepe, ki mu jih narekuje njegova starost. Otroci, ki postanejo žrtve spolnega izkoriščanja in spolnega zlorabljanja, imajo zagotovljeno varstvo pravic na podlagi načela nediskriminacije, ki ne povzroča ločevanja otrok na podlagi spola, rase, barve, jezika, vere ali kakršnega koli drugega prepričanja (2. člen Konvencije Sveta Evrope). Konvencija Sveta Evrope o zaščiti otrok pred spolnim izkoriščanjem in spolnim zlorabljanjem določa tudi programe za pomoč žrtvam in na ta način spodbuja ljudi, da anonimno in zaupno prijavijo sum kaznivega dejanja spolnega izkoriščanja in spolnega zlorabljanja preko telefonske ali internetne linije za pomoč žrtvam (13. člen Konvencije Sveta Evrope).

3.2.5 Direktiva 2011/93/EU Evropskega parlamenta in Sveta z dne 13. decembra 2011 o boju proti spolni zlorabi in spolnemu izkoriščanju otrok ter otroški pornografiji in nadomestitvi Okvirnega sklepa Sveta 2004/68/PNZ

Gre za zakonodajni akt (Evropska unija, 2011), katerega namen so spremembe in razširitev področja, od kaznovanja, preprečevanja kaznivih dejanj do podpore žrtvam v Evropski uniji. Opredeljuje kazniva dejanja, ki so: spolne zlorabe otrok, spolno izkoriščanje otrok, otroška pornografija in pridobivanje otrok na spletu z namenom spolne zlorabe. Na ravni Evropske unije direktiva uvaja enotno obravnavo kaznivih dejanj spolne zlorabe otrok, spolnega izkoriščanja otrok in dejanj, povezanih z

distribucijo gradiv s spolnimi zlorabami otrok (CAM), ter za vsa relevantna kazniva dejanja zoper spolno nedotakljivost otrok določa minimalne kazni, uvaja mehanizme za boj proti turizmu, ki je usmerjen v spolno izkoriščanje oziroma zlorabljanje otrok in omejuje dostop obsojenim za tovrstna kazniva dejanja do otrok (Klančnik, 2013a).

Slovenija je ob nenehnemu spremljanju področja na vseh ravneh (globalni, regionalni, nacionalni, multilateralni in bilateralni) delovanja do sedaj izvedla že različne ukrepe in zakonodajne spremembe, ki pripomorejo k neposrednemu odkrivanju in preprečevanju kaznivih dejanj zoper spolno nedotakljivost otrok (Klančnik, 2013a).

4 Prikriti preiskovalni ukrepi v Sloveniji in zlorabe otrok

PPU so sestavni del predkazenskega postopka (opredeljeni so od 149.a člena do 156. člena Zakona o kazenskem postopku, 2012; v nadaljevanju ZKP) kot sredstvo v boju proti nevarnim oblikam kriminala. Ukrepe lahko razvrstimo po različnih kriterijih, na primer: po vrsti, obsegu in načinu izvajanja, glede na odredbodajalca in pa tudi za katera kazniva dejanja se lahko odredijo (Žaberl, 2006).

Zakonsko določeni PPU, ki policiji olajšajo odkrivanje kaznivih dejanj in storilcev so:

1. tajno opazovanje (149.a člen ZKP);
2. pridobivanje podatkov oziroma izpis podatkov iz elektronskega komunikacijskega omrežja (149.b člen ZKP);
3. nadzor elektronskih komunikacij s prisluškovanjem in snemanjem ter kontrola in zavarovanje dokazov o vseh oblikah komuniciranja, ki se prenašajo v elektronskem komunikacijskem omrežju (1. točka prvega odstavka 150. člena ZKP);
4. kontrola pisem in drugih pošilk (2. točka prvega odstavka 150. člena ZKP);
5. kontrola računalniškega sistema banke ali druge pravne osebe, ki opravlja finančno ali drugo gospodarsko dejavnost (3. točka prvega odstavka 150. člena ZKP);
6. prisluškovanje in snemanje pogovorov s privolitvijo vsaj ene osebe, udeležene v pogovoru (4. točka prvega odstavka 150. člen ZKP);
7. prisluškovanje in opazovanje v tujem stanovanju ali drugih tujih prostorih, z uporabo tehničnih sredstev za dokumentiranje in s tajnim vstopom v navedene prostore (151. člen ZKP);
8. navidezni odkup, navidezno sprejemanje oziroma dajanje daril, navidezno jemanje oziroma dajanje podkupnine (155. člen ZKP);
9. tajno delovanje (155.a člen ZKP);
10. pridobitev zaupnih podatkov in dokumentacije o vlogah, depozitih, stanju in prometu na računih ali drugih poslih oseb, udeleženih v finančnih transakcijah ali poslih od banke, hranilnice, plačilne institucije ali družbe za izdajo elektronskega denarja (156. člen ZKP).

Žaberl (2006) razdeli prikrite preiskovalne ukrepe glede na njihovo metodiko in tehniko uporabe v dve veliki skupini; v prvi skupini so tisti, ki posegajo v ustavno

zagotovljeno pravico, pravico do zasebnosti (prisluškovanje telefonskim razgovorom, prisluškovanje v prostoru, tajno opazovanje, sledenje in slikovno snemanje), v drugo skupino pa uvrsti tiste, ki neposredno ne posegajo v ustavno zagotovljeno pravico do zasebnosti, so pa problematični s tega vidika, da osebe, ki jih uporabljajo, z njimi navidezno storijo znake določenih kaznivih dejanj (to so navidezni odkup predmetov, navidezno sprejemanje oziroma dajanje podkupnine, navidezno podkupovanje in morda tajno sodelovanje).

V nadaljevanju se bomo omejili zgolj na opis temeljnih značilnosti tistih PPU, s katerimi preiskovalci lahko prispevajo k učinkovitemu odkrivanju storilcev v primerih, ko je bilo storjeno kaznivo dejanja pridobivanja oseb, mlajših od petnajst let, za spolne namene (173.a člen KZ-1B, 2011), ko jih z ustaljenimi klasičnimi metodami preiskovanja kaznivih dejanj ni mogoče odkriti.

4.1 Tajno opazovanje (149.a člen ZKP)

Gre za ukrep, ki ga Žaberl (2006) opiše kot dalj časa neprekinjeno opazovanje ali sledenje policije proti osumljeni osebi z namenom, da bi jo morda zalotili pri kaznivem dejanju ali da bi jo odkrili po storjenem kaznivem dejanju. Za dokumentiranje položaja in gibanja osebe lahko policija uporablja tehnična sredstva za avdio, foto in video dokumentiranje, s katerimi se pridobijo materialni dokazi za potrebe kazenskega postopka. Opisani ukrep torej ureja prestrezanje, nadziranje, snemanje in shranjevanje različnih vrst komunikacij, ki potekajo po tehničnih sredstvih. Za opisani ukrep je posebej predpisano, da se sme izvajati samo na javnih ter javno dostopnih odprtih in zaprtih prostorih ter krajih, ki so vidni z javno dostopnega prostora. Tajno opazovanje se sme izvajati v zaprtih prostorih izjemoma, če v to privoli imetnik prostora, kar pomeni, da se uporaba prej naštetih tehničnih sredstev brez privolitve imetnika, čeprav brez fizičnega vstopa v takšen prostor, šteje kot nezakonita.

Tajno opazovanje se sme odrediti, če obstajajo utemeljeni razlogi za sum, da je določena oseba izvršila, izvršuje ali pripravlja oziroma organizira izvršitev katerega izmed kataloško naštetih kaznivih dejanj, pri tem pa je mogoče utemeljeno sklepati, da policisti z drugimi ukrepi tega dejanja ne morejo odkriti, preprečiti ali dokazati oziroma bi bilo to povezano z nesorazmernimi težavami (prvi odstavek 149.a člena ZKP).

»Zakonodajalec predpisuje, da se tajno opazovanje izvaja z neprekinjenim ali ponavljajočim opazovanjem ali sledenjem z uporabo tehničnih naprav za ugotavljanje položaja in gibanja ter tehničnih naprav za prenos in snemanje glasu, fotografiranjem in video snemanjem in je osredotočeno na spremljanje položaja, gibanja ter aktivnosti osebe, ki se tajno opazuje (tretji odstavek 149.a člena ZKP)« (Žaberl, 2006: 321).

»Ukrep (golega) tajnega opazovanja s pisno odredbo dovoli državni tožilec na pisni predlog policije. V primeru, da se s tajnim opazovanjem huje poseže v zasebnost osumljenca ali druge osebe, pa ukrep s pisno odredbo odredi preiskovalni sodnik. Zakonodajalec določa, da to stori na pisni predlog državnega tožilca v naslednjih primerih (šesti odstavek 149.a člena ZKP):

- če se pri izvajanju ukrepa predvideva uporaba tehničnih naprav za prenos in snemanje glasu;
- če izvedba ukrepa zahteva namestitvev tehničnih naprav za ugotavljanje položaja in gibanja osumljenca s tajnim vstopom v vozilo ali drug zavarovan ali zaprt prostor ali predmet;
- za uporabo ukrepa v zasebnih prostorih, če v to privoli imetnik prostora;
- za izvajanje ukrepa zoper osebo, ki ni osumljenec« (Žaberl, 2006:322).

Odredba mora biti po navajanju Žaberla (2006) pisna, izjemoma ustna ob zakonskih pogojih nujnosti v primeru, če pisne odredbe ni mogoče pravočasno dobiti in če obstaja nevarnost odlašanja in to dovoljuje zakonodajalec. V tem primeru mora biti izdana najkasneje v roku dvanajstih ur po izdaji ustne odredbe (osmi odstavek 149.a člena ZKP).

Žaberl (2006) opiše, da zakonodajalec predvideva tudi kratkotrajno možnost izvajanja ukrepa »golega« tajnega opazovanja, brez predhodne odredbe pristojnega organa. To dovoljuje v primeru, če pride oseba, zoper katero se ukrep izvaja, v stik z drugo neidentificirano osebo, za katero obstajajo utemeljeni razlogi za sum, da je vpletena v kriminalno dejavnost v zvezi s kaznivimi dejanji, zaradi katerih se ukrep izvaja. Takrat lahko policija opisano osebo tajno opazuje tudi brez odredbe, če obstajajo razlogi za identifikacijo osebe ali pridobitev podatkov, pomembnih za kazenski postopek. O tem mora policija takoj, ko je mogoče, in najpozneje v roku šestih ur od začetka izvajanja ukrepa obvestiti državnega tožilca, ki določi, ali bo dovolil ali prepovedal nadaljnje izvajanje ukrepa. Ta ukrep sme trajati največ dvanajst ur od stika z osebo, zoper katero se ukrep izvaja. Policija pri izvajanju

ukrepa iz tega odstavka ne sme uporabljati tehničnih naprav in sredstev iz 1. in 2. točke šestega odstavka tega člena niti izvajati ukrepa v zasebnih prostorih. Policija tako po prenehanju takšnega opazovanja napravi uradni zaznamek, ki ga brez odlašanja pošlje državnemu tožilcu, ki je izdal dovoljenje iz tega odstavka, in organu, ki je izdal prvotno odredbo za tajno opazovanje. Uradni zaznamek postane del kazenskega spisa (deveti odstavek 149.a člena ZKP).

Izvajanje ukrepa tajnega opazovanja lahko traja največ dva meseca, iz tehničnih razlogov pa se lahko njegovo trajanje s pisno odredbo podaljša vsakič za dva meseca. Skupno lahko ukrep golega tajnega opazovanja traja štiriindvajset mesecev oziroma šestintrideset mesecev za nekatera kazniva dejanja, ukrep tajnega opazovanja, ki ga odredi preiskovalni sodnik, pa sme skupno trajati največ šest mesecev (deseti odstavek 149.a člena ZKP).

Policija preneha z izvajanjem ukrepa takoj, ko prenehajo razlogi, zaradi katerih je bil odrejen. O prenehanju brez odlašanja pisno obvesti organ, ki je ukrep odredil. Policija pošilja organu, ki je ukrep odredil, mesečna poročila o poteku samega izvajanja ukrepa in pridobljenih podatkov. Organ, ki je ukrep odredil, lahko v vsakem trenutku na podlagi tega poročila ali po uradni dolžnosti, če oceni, da ni več razlogov za uporabo ukrepa ali da se ta izvaja v nasprotju z njegovo odredbo, s pisno odredbo odredi, da se izvajanje ukrepa ustavi (enajsti odstavek 149.a člena ZKP).

Horvat (2004) opiše posebnost ukrepa, da ga je mogoče odrediti zoper osebo, ki ni osumljenec, če je z opazovanjem te osebe mogoče priti do osumljenca, čigar osebni podatki niso znani, je na begu ali se skriva; ob pogojih iz devetega odstavka pa je tajno opazovanje dopustno tudi zoper osebo, ki pride v stik z opazovano osebo, če so podani utemeljeni razlogi za sum, da je tudi sama vpletena v kriminalno dejavnost. Te osebe, kljub temu da niso osumljenci, morajo biti določljive – individualizirane, tudi če niso znani njihovi osebni podatki; ukrepa tajnega opazovanja ni mogoče izvajati zoper nedoločen krog oseb.

S tajnim opazovanjem osumljenca na javno dostopnih krajih se posega v njegovo zasebnost. Na javno dostopnih odprtih in zaprtih prostorih, v katerih se sme po določbah tega člena osumljenca tajno opazovati, so lahko v zasebni lasti, če so dostopni nedoločenemu krogu oseb. V primeru, če je potrebno opazovanje izvajati v določenem prostoru, v katerem njegov imetnik upravičeno pričakuje, da ima zagotovljeno zasebnost, tajnega opazovanja ni dopustno izvajati z javno dostopnega

kraja, temveč le z uporabo prikritega preiskovalnega ukrepa po določbah 151. člena ZKP (Horvat, 2004).

Na podlagi dokumentacije, ki je podlaga za podaljšanje ukrepa, ter gradiva, zbranega z izvajanjem ukrepa, zunajobravnavni senat vsakih šest mesecev presodi, ali so podani razlogi in zakonski pogoji za njegovo nadaljnje izvajanje. Namen te sodne kontrole je preprečitev, da bi se ukrepi še naprej izvajali, čeprav za to ni formalni zakonskih pogojev, oziroma če glede na rezultat dotedanjšega izvajanja ukrepa senat oceni, da nadaljnje izvajanje ukrepa ni utemeljeno, ker ni realno pričakovati, da bi lahko zbrali dokaze za utemeljen sum, da je obdolženec storil kaznivo dejanje (Horvat, 2004).

4.2 Pridobivanje podatkov oziroma izpis podatkov iz elektronskega komunikacijskega omrežja (149.b člen ZKP)

Gre za ukrep, ki za Žaberla (2006) predstavlja pomemben vir podatkov o lastništvu oziroma uporabništvu določenega komunikacijskega sredstva in za podatke o prometu v elektronskem komunikacijskem omrežju. Za policijo je to izrednega pomena, saj na tak način identificirajo uporabnika določenega telefona in podatke, s kom, kdaj in koliko časa osumljeni komunicira, ne izvejo pa same vsebine komunikacije. Sama vsebina komunikacije (elektronske pošte) se lahko pridobi le z izvajanjem prikritega preiskovalnega ukrepa nadzora elektronskim komunikacij s prisluškovanjem in snemanjem, za kar zakonodajalec zahteva strožji dokazni standard in strožje pogoje.

Zaradi različne kvalitativne vrednosti zahtevanih podatkov zakonodajalec predvideva dve vrsti zahteve in dva organa, ki ukrep odredita (Žaberl, 2006):

- Če je za odkritje kaznivega dejanja ali storilca potrebno pridobiti podatke o lastniku ali uporabniku določenega komunikacijskega sredstva za elektronski komunikacijski promet, ki niso objavljeni v naročniških imenikih, in o času, v katerem je tako sredstvo bilo oziroma je v uporabi, sme policija sama od operaterja zahtevati, da ji na njeno pisno zahtevo, tudi brez privolitve posameznika, na katerega se ti podatki nanašajo, sporoči te podatke (tretji odstavek 149.b člena). Ti podatki niso javni, vendar se z njimi po mnenju zakonodajalca ne posega v ustavno varovano tajnost občil, tako da bi bila za njihovo objavo potrebna odredba sodišča. Podatke je operater dolžan

sporočiti policiji tudi brez privolitve posameznika, na katerega se podatki nanašajo.

- Če je treba pridobiti še druge podatke o udeležencih, okoliščinah in dejstvih komunikacijskega prometa, kot so številka ali druga oblika identifikacije uporabnikov komunikacijskih storitev, vrsta, datum, čas in trajanje klica oziroma druge elektronske komunikacijske storitve, količina prenesenih podatkov in kraj, iz katerega je bila komunikacijska storitev opravljena, lahko navedene podatke s pisno odredbo zahteva le preiskovalni sodnik na obrazložen predlog državnega tožilca (prvi odstavek 149.b člena).

Predlog in odredba morata biti pisna in vsebovati podatke, ki omogočajo identifikacijo komunikacijskega sredstva za elektronski komunikacijski promet, utemeljitev razlogov, časovno obdobje, za katerega se podatki zahtevajo, ter ostale pomembne okoliščine, ki narekujejo uporabo ukrepa (drugi odstavek 149.b člena).

Zakonodajalec med drugim tudi določa, da operater omrežij svoji stranki ali tretji osebi ne sme razkriti, da je ali da bo določene podatke posredoval pristojnemu organu ali policiji (četrti odstavek 149.b člena).

Z opisanim PPU se lahko pridobijo samo podatki, ki omogočajo identificiranje uporabnika elektronske komunikacijske storitve (številka, čas klica, trajanje klica, količina prenesenih podatkov³), ne pa sama vsebina komunikacije; le-ta se lahko pridobi le z izvajanjem PPU nadzora elektronskih komunikacij s prisluškovanjem in snemanjem. Ker se tudi s pridobitvijo podatkov, navedenih v prvem odstavku 149.b člena, posega v ustavno varovano človekovo pravico do varstva tajnosti občil, jih policija oziroma državni tožilec lahko pridobita le na podlagi pisne odredbe sodišča (Horvat, 2004).

³ Sodišče Evropske unije je razglasilo Direktivo o hrambi podatkov za neveljavno, s tem je odpadla obveznost držav članic, da zahtevo po obvezni hrambi prometnih podatkov iz Direktive prenesejo v nacionalni pravni red. Kljub temu je takšna ureditev še vedno dopustna na podlagi prava EU, če je poseg v pravico do varstva osebnih podatkov sorazmeren, slovenski zakonodajalec tako zahtevi po sorazmernosti ni zadostil. Ustavno sodišče je določilo, da je del Zakona o elektronskih komunikacijah (2012; v nadaljevanju ZEKom-1) v neskladju s pravico do varstva osebnih podatkov iz 38. člena Ustave. Poseg v pravico do varstva osebnih podatkov iz podanega člena Ustave je nesorazmeren, saj je z določitvijo obvezne (preventivne) in neselektivne hrambe prometnih podatkov zakonodajalec močno posegel v zasebnost ljudi, hkrati pa ni skrbno opredelil okoliščin, na podlagi katerih bi se ta poseg omejil le na tisto, kar je nujno za dosego namena. Ustavno sodišče je hkrati »ukazalo« operaterjem, da nemudoma uničijo prometne podatke, ki so jih morali hraniti na podlagi izpodbijalne ureditve (Odločba US RS, 2014).

4.3 Nadzor elektronskih komunikacij s prisluškovanjem in snemanjem ter kontrola in zavarovanje dokazov o vseh oblikah komuniciranja, ki se prenašajo v elektronskem komunikacijskem omrežju (1. točka prvega odstavka 150. člena)

Z iznajdbo telefona se je po mnenju Žaberla (2006) pričelo tudi prisluškovanje kot metoda odkrivanja kaznivih dejanj. Ukrep se nanaša na kontrolo in zavarovanje dokazov o vseh oblikah komuniciranja, ki se prenašajo v elektronskem komunikacijskem omrežju, kar kasneje služi kot dokaz na sodišču. Če se ukrep nanaša na nadzor sporočil, ki se pošiljajo in sprejemajo po elektronski pošti (angl. E-mail), se zavarovanje dokazov za potrebe kazenskega postopka opravi tako, da se sporočila natisnejo in shranijo (Horvat, 2004).

Žaberl (2006) navaja, da navedeni ukrep posega v pravico osumljenca do tajnosti pisem in drugih občil (38. člen Ustave RS, 2013), zato ga sme odrediti le preiskovalni sodnik. Odrediti ga sme, če obstajajo utemeljeni razlogi za sum, da je določena oseba izvršila, izvršuje ali pripravlja oziroma organizira izvršitev katerega izmed kataloško naštetih kaznivih dejanj in če obstaja utemeljen sum, da se za komunikacijo v zvezi s tem kaznivim dejanje uporablja določeno komunikacijsko sredstvo oziroma računalniški sistem ali bo to sredstvo oziroma sistem uporabljeno, pri tem pa je mogoče utemeljeno sklepati, da se z drugimi ukrepi ne bi dalo zbrati dokazov oziroma bi njihovo zbiranje lahko ogrozilo življenje ali zdravje ljudi.

4.4 Kontrola pisem in drugih pošiljk (2. točka prvega odstavka 150. člena)

Posega v ustavno priznano pravico do neprekršljivosti tajnosti pisem in drugih pošiljk. Z uporabo ukrepa Žaberl (2006) opiše, da je vzpostavljena kontrola poštnih pošiljk, katerih vsebina bi imela lahko dokazni standard v kazenskem postopku. Kontrola pisem in drugih pošiljk se navezuje na tiste, ki jih pošilja osumljenec, in tiste, ki so nanj naslovljene, a je v predkazenskem postopku, ko je osumljenec na prostosti, mogoče izvajati samo kontrolo pošiljk, ki so naslovljene nanj. Pisma in druge pošiljke

se pri izvedbi samega ukrepa ne zasežejo, saj bi se s tem lahko razkrilo samo izvajanje ukrepa.

Za odreditev navedenega ukrepa veljajo enaki pogoji kot za odreditev nadzora elektronskih komunikacij s prisluškovanjem in snemanjem (Žaberl, 2006).

4.5 Prisluškovanje in snemanje pogovorov s privolitvijo vsaj ene osebe, udeležene v pogovoru (4. točka prvega odstavka 150. člen ZKP)

Bistvo podanega ukrepa je po mnenju Dežmana in Erbežnika (2003) prisluškovanje in snemanje pogovorov, z namenom odkritja kaznivega dejanja in storilca, vendar samo v primeru, ko v prisluškovanje in snemanje pisno privoli vsaj en udeleženec v pogovoru – »mali prisluškovalni napad«. Sama izvedba ukrepa ponavadi poteka tako, da policija na prikrit način ozvoči osebo, ki je dala privolitev, največkrat je to tajni policijski delavec ali sodelavec, lahko pa se prisluškuje tudi telefonu oškodovanca (npr. pri kaznivem dejanju izsiljevanja po 213. členu KZ-1) ali oseb, ki želijo s policijo sodelovati pri odkrivanju kaznivih dejanj (npr. osebe, ki jih osumljenec napeljuje k storitvi kaznivega dejanja).

Omenjeni ukrep sme preiskovalni sodnik odrediti pod enakimi pogoji kot že omenjena dva ukrepa, ki posegata v pravico do komunikacijske zasebnosti. Poseben pogoj, ki ga navaja zakonodajalec pri izvedbi danega ukrepa, je torej ta, da mora vsaj ena oseba, ki je udeležena v pogovoru, privoliti v prisluškovanje in snemanje. Privolitev mora biti pisna, zakon pa omogoča izključno avdio snemanje, na način, da se sredstva za snemanje namestijo na osebi, ki v to privoli, ali pa se z njeno pomočjo namestijo v prostoru, kjer razgovor poteka (Žaberl, 2006). Če gre za tajnega policijskega delavca, se privolitev dobi na način, ki ne razkrije njegove identitete (Horvat, 2004).

4.6 Prisluškovanje in opazovanje v tujem stanovanju ali drugih tujih prostorih, z uporabo tehničnih sredstev za dokumentiranje in po potrebi s tajnim vstopom v navedene prostore (151. člen ZKP)

Policisti pri podanem ukrepu po mnenju Žaberla (2006) uporabljajo prisluškovalne naprave, ki niso večje od ročne ure in ozvočijo celoten prostor, kjer se kriminalci sestajajo, delijo plen, načrtujejo kazniva dejanja ali se pogovarjajo o pravkar storjenem kaznivem dejanju – »veliki prisluškovalni napad«. Pri sami izvedbi ukrepa še z večjo intenziteto posegajo v nedotakljivost osumljenca, kar ponavadi zaobjema tudi poseg v zasebnost vseh tistih, ki z osumljencem prihajajo v stik v prostorih, v katerih se giblje. Zato zakonodajalec sledi načelu sorazmernosti in zahteva strožje pogoje za odobritev danega ukrepa, čas trajanja je za pol krajši kot pri »malem prisluškovalnem napadu« in krog kaznivih dejanj, pri katerih se lahko ukrep odredi, je ožji. Posebnost podanega ukrepa je, da omogoča, da se sme zaradi namestitve naprav po potrebi tajno vstopiti v navedene prostore, kjer trči ob ustavno zagotovljeno pravico do nedotakljivosti stanovanja.

Ukrep prisluškovanja in opazovanja v stanovanju ali drugih tujih prostorih z uporabo tehničnih sredstev za dokumentiranje in po potrebi s tajnim vstopom v navedene prostore s pisno odredbo odredi preiskovalni sodnik na pisni predlog državnega tožilca v primeru, če obstajajo utemeljeni razlogi za sum, da je določena oseba izvršila, izvršuje ali pripravlja oziroma organizira izvršitev katerega izmed kataloško določenih kaznivih dejanj, pri tem pa je mogoče utemeljeno sklepati, da se bo lahko v točno določenem prostoru pridobilo dokaze, katerih se z milejšimi ukrepi, vključno z ukrepi iz 149.a, 149.b in 150. člena ne bi dalo zbrati oziroma bi njihovo zbiranje lahko ogrozilo življenje ljudi (prvi odstavek 151. člena).

Z odobritvijo uporabe danega ukrepa v stanovanju oziroma v drugem zaprtem prostoru se policiji daje tudi dovoljenje, da brez vednosti imetnika stanovanja vstopi v stanovanje ali drug prostor in tajno namesti naprave za opazovanje in prisluškovanje. Vstop v prostore z vednostjo stanovalca in nato tajna namestitve tehnične naprave za dokumentiranje se šteje kot tajni vstop v stanovanje. Odredba preiskovalnega sodnika, ki dovoli tajni vstop v stanovanje zaradi namestitve takšne naprave, ne daje policiji pooblastila, da opravi po vstopu v stanovanje še hišno preiskavo (Horvat, 2004).

Ukrepe iz 150. in 151. člena ZKP odredi preiskovalni sodnik na pisni predlog državnega tožilca (1. odstavek 152. člena). Izjemoma, če pisne odredbe ni mogoče pravočasno pridobiti in če obstaja nevarnost odlašanja, sme na ustni predlog državnega tožilca preiskovalni sodnik odrediti izvrševanje ukrepov iz 150. člena ZKP z ustno odredbo. O ustnem predlogu državnega tožilca preiskovalni sodnik napravi uradni zaznamek. Pisna odredba mora biti izdana najkasneje v dvanajstih urah po izdaji ustne odredbe. Za predčasno izvrševanje mora obstajati utemeljen razlog; v nasprotnem primeru sodišče ne glede na siceršnjo upravičenost uporabe ukrepov vselej postopa po četrtem odstavku ZKP (drugi odstavek 152. člena).

Izvajanje ukrepov iz 150. in 151. člena ZKP lahko traja največ en mesec, iz tehničnih razlogov pa se sme njihovo trajanje podaljšati vsakič za en mesec, vendar za ukrepe iz 150. člena tega zakona skupno največ šest mesecev, za ukrep iz 151. člena ZKP pa skupno največ tri mesece (četrty odstavek 152. člena).

Uporaba ukrepov iz 150. in 151. člena ZKP je časovno omejena. Kot začetek izvajanja ukrepov se šteje čas, ko je bil odrejen prvi ukrep. V primeru, če je bilo podaljšanje ukrepa predlagano po preteku enega meseca, se v šestmesečni rok všteta samo čas dejanskega trajanja ukrepov po izdanih odredbah. Ko preteče maksimalni rok je zoper istega osumljenca mogoče odrediti PPU le zaradi odkrivanja kakšnega drugega kaznivega dejanja (Horvat, 2004).

Policija mora prenehati z izvajanjem odrejenega ukrepa potem, ko osumljencu odvzame prostost ali ko zoper njega poda kazensko ovadbo, saj oboje pomeni, da je ocenila, da je zbranih dovolj dokazov za začetek kazenskega postopka. Vedno pa mora policija prenehati izvajati, ko poteče čas, do katerega je bil ukrep odrejen (Horvat, 2004).

Dolžnost operaterjev elektronskih komunikacijskih omrežij je, da policiji omogočijo izvršitev odredbe preiskovalnega sodnika (Horvat, 2004).

Ukrepe iz 150. in 151. člena ZKP ni mogoče izvajati na način, ki ne bi prizadel zasebnosti tretjih oseb, ki niso osumljenci. Z določbo sedmega odstavka 152. člena ZKP se policiji nalaga dolžnost, da dane ukrepe izvaja tako, da v najmanjši mogoči meri prizadene tretje osebe. Ker se med drugim pri prisluškovanju snemajo tudi pogovori teh oseb z osumljencem, se ti pogovori ne prepisujejo, če nimajo nobene zveze s kaznivim dejanjem, zaradi katerega se je izvajal ukrep (Horvat, 2004).

4.7 Tajno delovanje (155.a člen ZKP)

Predstavlja ukrep, ki ga Žaberl (2006) opiše kot delovanje policije s pomočjo tajnega delovanja policista znotraj kriminalne združbe, ki zbira podatke o kriminalni dejavnosti osumljenih. V to kriminalno združbo se vrine policist ali druga oseba pod vodstvom policije. Pri tem mora prikriti svoj poklic in identiteto, na podlagi tega se lahko izdelajo lažne listine, kot so: osebna izkaznica, vozniško dovoljenje, potrdilo o depozitu, in podobno, z namenom preprečitve, da bi bila takšno zbiranje podatkov ali vključitev razkrita. Tajno delovanje se izvaja z vključitvijo tajnih delavcev in neprekinjenim ali ponavljajočim zbiranjem podatkom, kjer tajni delavec prihaja v neposredni stik z osumljenim. Dokaz pri izvajanju tega ukrepa je, kar je tajni delavec izvedel, videl ali slišal o osumljenem oziroma od njega prejel tekom izvajanja ukrepa.

Ukrep tajnega delovanja brez uporabe tehnične naprave za prenos in snemanje glasu, fotografiranja in videosnemanja s pisno odredbo dovoli državni tožilec na pisni predlog policije, razen v primerih iz četrtega odstavka 155.a člena, ko je potrebna odredba preiskovalnega sodnika. Odredba lahko obsega tudi dovoljenje za izdelavo, pridobitev in uporabo prirejenih podatkov in dokumentov (tretji odstavek 155.a člena ZKP).

Torej v primeru, pri katerem tajni policijski delavec uporabi tehnične naprave za prenos in snemanje glasu, fotografiranje in videosnemanje, se lahko ukrep odredi samo v zvezi s kataloško določenimi kaznivimi dejanji iz drugega odstavka 150. člena ZKP. Ukrep s pisno odredbo odredi preiskovalni sodnik na pisni predlog državnega tožilca (četrti odstavek 155.a člena ZKP). Za razliko od tajnega opazovanja, kjer ni neposrednega stika z opazovano osebo, pri ukrepu tajnega delovanja prihaja tajni delavec tudi v neposreden stik z osumljencem (Žaberl, 2006).

Izvajanje ukrepa tajnega delovanja je časovno omejeno, saj lahko traja največ dva meseca, iz tehničnih razlogov pa se lahko njegovo trajanje s pisno odredbo vsakič podaljša za dva meseca, vendar skupno največ štiriindvajset mesecev, v primeru uporabe ukrepa za točno določena kazniva dejanja pa skupno največ štiriintriideset mesecev (šesti odstavek 155.a člena ZKP).

Ukrepi iz 155.a člena se morajo izvrševati na način, na katerega se v najmanjši možni meri posega v pravice oseb, ki niso osumljenci (osmi odstavek 155.a člena ZKP). Pri

izvrševanju ukrepa tajni policijski delavec ne sme izzvati kriminalne dejavnosti (deveti odstavek 155.a člena).

Vprašanje delovanja prikritih policistov in tajnih policijskih sodelavcev, zlasti ko gre za njihovo infiltriranje v organizirano kriminalno združbo, je tesno povezano z občutljivimi vprašanji dopustnosti sodelovanja eh oseb pri storitvi kaznivih dejanja, da si pridobijo »zaupanje« kriminalne družbe. Po stališču Ustavnega sodišča RS mora biti pri zakonski ureditvi uporabe teh ukrepov začrtana meja med dovoljenim in nedovoljenim ravnanjem državnih organov, sicer so vse varovalke zoper arbitrarno uporabi zakona neučinkovite (Horvat, 2004).

Pri tajnem delovanju prikriti policist pod vodstvom in nadzorom policije načrtno in kontinuirano zbira podatke o osumljencu in njegovi kriminalni dejavnosti. V tem je podobnost s PPU tajnega opazovanja po 149.a členu, s tem da prikriti policist oziroma tajni policijski sodelavec pri tajnem delovanju prihaja tudi v neposreden stik z osumljencem, zaradi česar sme uporabljati prirejene identifikacijske listine, da se ga ne razkrije (Horvat, 2004).

Izvajalec opisanega ukrepa tajnega delovanja je lahko s prirejenimi dokumenti »udeležen v pravnem prometu«, torej sme sklepati pod prirejenim imenom tudi pravne posle, vendar samo tiste, ki so potrebni za učinkovito izvajanje PPU in so bili vnaprej navedeni v pisni odredbi preiskovalnega sodnika. Ker te posle dovoli sodišče, je izključena njihova protipravnost. Razen določbe devetega odstavka, da tajni policijski delavec pri izvrševanju ukrepa ne sme izzvati kriminalne dejavnosti - kar mora veljati tudi za tajnega policijskega sodelavca -, zakon ne določa, ali in katera kazniva dejanja bi smel storiti skozi izvajanje ukrepa, da si pridobi »zaupanje« kriminalne združbe, v katero se želi infiltrirati. To vprašanje je prepuščeno sodni praksi, ki bi morala postaviti zelo visok prag za dopustnost takšnih ravnanj (Horvat, 2004).

Dokaz pri izvajanju ukrepa je tisto, kar je tajni delavec pri izvajanju tajnega delovanja izvedel, videl ali slišal o osumljencu oziroma je od njega prejel, torej vse tisto, o čemer na sodišču pove kot anonimna priča (240. člen ZKP). O vseh teh dejstvih se tajnega delavca na sodišču zasliši kot anonimno pričo. Izvajalec ukrepa pa lahko pri tajnem delovanju uporablja tudi tehnične naprave za zvočno in slikovno snemanje (drugi odstavek 155.a člena ZKP). Ker pa se s tem že posega v zasebnost osumljenca in drugih oseb, mora imeti za to vnaprejšnje dovoljenje oziroma odredbo preiskovalnega sodnika (Žaberl, 2006).

4.8 Skupne značilnosti PPU

PPU so posebna policijska pooblastila, ki se od splošnih policijskih razlikujejo predvsem po globini posegov v posamezne človekove pravice in po dejstvu, da se izvajajo prikrito in ne javno. Čeprav so po svoji vsebini prikriti, pa imajo nekatere skupne značilnosti (Žaberl, 2006):

1. Obstajati mora višja stopnja verjetnosti, da je bilo storjeno kaznivo dejanje (zahtevajo se utemeljeni razlogi za sum) in pa dejstvo, da do podatkov ni možno priti na drug način (s klasičnimi policijskimi pooblastili, kot na primer zbiranje obvestil). Gre za t. i. subsidiarnost uporabe PPU.
2. Večina PPU se izvaja v fazi, ko je kaznivo dejanje izvršeno oziroma je že bilo izvršeno in tudi v fazi, ko se kaznivo dejanje šele pripravlja. Torej je nesporno, da bodo ti ukrepi privedli preiskovalce do rezultatov samo takrat, ko se bodo izvajali v fazi predkazenskega postopka.
3. Vsi podatki, ki jih pridobijo s PPU, imajo v nadaljnjem kazenskem postopku dokazno vrednost. V primerih, ko so ukrepi odrejeni in izvajani zakonito, sme sodba temeljiti na dokazih, ki so bili z njimi pridobljeni. Medtem ko za ostala obvestila, ki jih zbere policija v predkazenskem postopku, velja, da so zgolj informativnega značaja, pa se »obvestila« in drugi podatki, pridobljeni z zakonito uporabo PPU, uporabijo kot dokaz v nadaljnjem kazenskem postopku. Medtem lahko zakonodajalec predpiše ekskluzijo dokazov v primeru nezakonitega odrejanja ali izvajanja ukrepov.
4. Vsi PPU so časovno omejeni. Tudi to predstavljajo eno od razlik od drugih ukrepov oziroma pooblastil, ki niso časovno omejeni. Določeni PPU se smejo podaljševati, vendar je po ustreznem času potrebno prenehati z izvajanjem. Intenziteta posega v človekove pravice je med drugim odvisna tudi od časa trajanja PPU, zato zakonodajalec določa, da mora zakonitost in utemeljenost nekaterih ukrepov po poteku določenega časa preizkusiti še sodišče (zunajobravnavni senat).
5. Vsi PPU se morajo izvajati na skrivaj in tajno, na način, da oseba, zoper katero se izvajajo, tega ne sumi. Prikritost izvajanja ukrepov je temeljna značilnost ukrepov, saj v primeru, če bi osumljenec vedel za izvajanje, policija ne bi prišla do relevantnih rezultatov. Zakonodajalec to analizira tako, da so podatki, pridobljeni z uporabo PPU, sestavni del kazenskega spisa, s katerim se osumljeni seznanijo.

6. Eden od dejstev, ki PPU karakterizira, je, kdo odloča oziroma odreja njihovo uporabo. Temeljni kriterij za ureditev dovoljenja oziroma odrejanja navedenih ukrepov je intenzivnost posega v ustavno varovane človekove pravice. O izvajanju PPU tako odločajo:

- policija sama – v primerih najblažjih ukrepov (pridobitev podatkov o lastniku ali uporabniku določenega komunikacijskega sredstva);
- državni tožilec – za ukrepe, ki pomenijo nekorektno delovanje države (policija poda predlog, državni tožilec pa dovoli izvajanje);
- preiskovalni sodnik – za ukrepe, ki pomenijo hujše posege v človekove pravice (policija poda pobudo, državni tožilec poda predlog, preiskovalni sodnik odredi izvajanje).

4.9 Primer uporabe PPU

V nadaljevanju bo predstavljen primer kriminalistične preiskave omenjenega »groominga« oziroma po slovenski kazenski zakonodaji preiskave kaznivega dejanja pridobivanja oseb, mlajših od petnajst let, za spolne namene iz 173.a člena KZ-1B (2011), kot jo izvajajo policije nekaterih držav članic EU in v ZDA. Gre za sledeč primer:

Policija zaznava, da se v spletnih klepetalnicah (angl. chat-room) pogosto zadržujejo uporabniki, ki se bodisi izdajajo za mladoletne osebe (pa to niso) bodisi nadlegujejo druge spletne uporabnike z neprimernimi povabili na zmenke ali k spolnim aktivnostim z njimi. V ta namen policija izdelava načrt, s katerim opredeli prirejeno identiteto tajnega policijskega delavca (v nadaljevanju: TPD), dodeli mu delovno ime (v spletnem okolju t. i. vzdevek oziroma angl. nickname), izdelava se mu profil namišljene mlajše deklince z njenimi hobiji, željami in osebnim opisom ter drugimi karakteristikami, potrebni za nemoteno morebitno komunikacijo z neznanim osebam v omenjeni klepetalnici. Nato se TPD ustrezno prijavi v spletno klepetalnico (angl. login), stopa v komunikacijo z drugimi v klepetalnici ter zavaruje vsakršno lastno komunikacijo z drugimi uporabniki. Kot vzdevek uporablja npr. Lilly_12, pod katerim komunicira, vendar TPD uporablja zgolj in samo splošno, odprto in sprejemljivo komunikacijo, upoštevajoč tudi pravila lepega obnašanja na internetu. Ob vzpostavitvi povezave (komunikacije v klepetalnici) se predstavi z besedilom, primernim njeni starosti, in izdelanim profilom namišljene mladoletne osebe (tj.

TPD), npr.: "Čau, jst sm tud tuki. Kva dugaja?" Vzdevek TPD-ja se sprti objavlja v klepetalnici. Izkušnje policije kažejo, da se v klepetalnicah zelo hitro navezujejo stiki večjega števila oseb naenkrat. Osebe v tem primeru zelo hitro preidejo iz spodobne komunikacije na bolj neprimerno, z raznimi povabili na zmenke, v drugo sobo (angl. room) v bolj zasebno komunikacijo, pa tudi s prepričevanjem in nagovarjanjem, da se pokaže kak bolj intimni del telesa, vključi spletno kamero, se povabi k samozadovoljevanju, tudi k vzajemni masturbaciji, s povabili na spolne odnose, kako se mladoletna oseba Lilly_12 telesno razvija (rast dojk, poganjanje dlak idr.) in podobno. Mladoletni sogovornici Lilly_12 alias TPD postavljajo tudi vprašanja o kraju bivališča, hobijih, o tem, ali je sama doma, nekateri skušajo biti tudi zelo prijazni, dajejo dober vtis, češ da gre za vrstnika ali vrstnico, dajejo občutek, da so zaupanja vredni. Sprva Lilly_12 ne želi srečanja, saj je pomembno, da storilec sam prikaže izreden interes za mladoletne osebe mlajše starosti (manj kot 15 let) ter dejansko kontekst, v katerem ga zanimajo ali privlačijo ti otroci (v spolnem smislu). Naslednji dan je isti sogovornik kljub jasnemu sporočilu o starosti mladoletne deklice Lilly_12 (12 let) zelo vztrajen in sam jo nagovori za srečanje. Predhodno je bil izpolnjen pogoj, da ga zelo privlačijo otroci v spolnem smislu za realizacijo njegovega spolnega poželenja (hoče meti spolne odnose s Lilly_12). Mladoletno dekle naposled privoli v zmenek, kraj in čas srečanja določi storilec. Ob dogovorjenem času in na dogovorjenem kraju se znajde storilec, ki pa ga na podlagi opisa odkrije policija in mu odvzame prostost (A. T. Klančnik, osebni intervju, 29. 8. 2013).

5 Razprava

Kaznivo dejanje, ko se storilec z uporabo informacijskih ali komunikacijskih tehnologij z oškodovancem dogovori za srečanje, je bilo zaradi uresničitve vnaprej načrtovanega protipravnega spolnega dejanja najprej pravno opredeljeno v Konvenciji Sveta Evrope o zaščiti otrok pred spolnim izkoriščanjem in spolnim zlorabljanjem (oziroma Lanzarotski konvenciji, 2007), katere namen je zaščititi otroka pred kakršno koli obliko spolnega izkoriščanja in spolne zlorabe ter to preprečiti, hkrati pa poskrbeti za pregon storilcev. Ena od sprememb, ki je posledica sprejete Direktive o boju proti spolni zlorabi in spolnemu izkoriščanju otrok ter otroški pornografiji (2011), je, da je Vlada Republike Slovenije vložila v parlamentarno proceduro Predlog zakona o spremembi in dopolnitvi kazenskega zakonika, medtem ko je Državni zbor sprejel ta predlog zakona. S tem je bila potrjena tudi novela oziroma novo kaznivo dejanje v slovenskem Kazenskem zakoniku (KZ-1B, 2011). V primeru, da dogovoru sledi določeno konkretno dejanje, na primer prihod storilca na dogovorjeni kraj, saj za obstoj tega kaznivega dejanja ni potrebno, da je do klasičnih oblik spolne zlorabe (penetracije spolnega uda, delov telesa ali predmetov v telesne odprtine druge osebe) sploh prišlo, bi bili izpolnjeni znaki predlaganega kaznivega dejanja (Klančnik, 2013a). Gre za pripravljalno kaznivo dejanje, ki je predhodna sestavina za izvršitev drugega kaznivega dejanja iz poglavja kaznivih dejanj zoper spolno nedotakljivost (Vrhovno sodišče RS, 2013). Sprememba je bila potrebna zaradi pomanjkljivosti veljavne ureditve, težav, zaznanih v praksi, in predvsem zaradi implementacije mednarodnih in evropskih pravnih aktov v nacionalno zakonodajo (137. redna seja ..., 2011).

Preiskovanje in dokazovanje kriminalitete iz skupine spolnih zlorab otrok na internetu predstavlja za organe kazenskega postopka poseben izziv. Med dejavniki, ki prispevajo k zapletenosti preiskovanja, so predvsem vprašanje identitete, vprašanje lokacije, narava podatkov, njihova integriteta, trajnost in količina (Šugman in Gorkič, 2011). Glede na opisane probleme pri preiskovanju kaznivega dejanja, ko se storilec z uporabo informacijskih ali komunikacijskih tehnologij dogovori z oškodovancem, mlajšim od petnajst let, za srečanje zaradi uresničitve spolnih namenov, slovensko pravo omogoča preiskovalcem različne preiskovalne ukrepe pod različnimi predpostavkami. Gre za ukrepe, kot so prisluškovanje telefonskim pogovorom, tajno policijsko opazovanje, delovanje, sledenje ter slikovno snemanje, ozvočenje prostorov, kontrola pisem in drugih pošilk ter pridobivanje oziroma izpis podatkov iz

elektronskega komunikacijskega omrežja. Pred vsakim izvajanem prikritih preiskovalnih ukrepov se prepričamo, da so izpolnjene tako materialnopravne kot formalne predpostavke. Žaberl (2006) opiše, da moramo biti pri materialnih predpostavkah pozorni predvsem na izpolnjevanje zahtevanega dokaznega standarda ter upoštevanja načela sorazmernosti, saj je večina ukrepov dovoljenih le pod pogojem, da se policija do potrebnih podatkov ne more dokopati na manj invaziven način (izčrpane so klasične oblike preiskovanja). Posebno pozornost velja nameniti tudi formalnim predpostavkam. Vsekakor je bistveno, da ukrep odredi oziroma dovoli pristojni organ, še preden se ga začne izvajati. Z vidika invazivnosti predpisujejo ukrepe trije različni organi. Najbolj invazivne dovoljuje preiskovalni sodnik, kar nekaj ukrepov lahko odredi tudi državni tožilec, za določene ukrepe pa ima pristojnost odrejanja tudi policija. Odredba mora vsebovati vse podatke, ki jih zahteva zakon za posamezen PPU, saj bo le taka odredba vzdržala naknadni test pred sodiščem. V praksi je še posebej pomembno, da se ukrepi tudi dejansko izvajajo skladno z odredbo in se od nje ne odmikajo. Za vsak ukrep so v zakonu določeni roki, ki jih je treba upoštevati, ter pogoji, pod katerimi se lahko izvajanje ukrepa podaljša. PPU ni mogoče odrediti za vsako kaznivo dejanje, temveč so za posamezne ukrepe naštetá kataloška kazniva dejanja, za katera jih je mogoče odrediti, zraven pa je dodana še splošna klavzula, tako je na primer za ukrep tajnega delovanja poleg za naštetá kazniva dejanja, mogoče uporabiti za vsa kazniva dejanja, za katera je zagrožena kazen vsaj 5 let. Za najinvazivnejše PPU, ki so določeni v 150. členu ZKP, pa je poleg posebej naštetih dejanj mogoče izdati odredbo za vsa kazniva dejanja, za katera je predpisana kazen zaporá osmih ali več let. Načelo sorazmernosti ZKP udejanja tudi tako, da je za najinvazivnejše prikríte preiskovalne ukrepe dodana predpostavka, da je mogoče utemeljeno sklepanje, da se z drugimi ukrepi ne bi dalo zbrati dokazov oziroma bi njihovo zbiranje lahko ogrozilo življenje ali zdravje ljudi. Le tako bo kazenski postopek potekal zakonito in se bo lahko končal uspešno. Če se katera od teh formalnosti ne upošteva, lahko hitro pride do ekskluzije dokazov, ves trud policije pa ne rodi zelenih rezultatov (Dežman in Erbežnik, 2003).

Pri uporabi PPU je posebej pomemben pravilen izbor izmed možnosti, ki jih daje na voljo zakon. Naloga policijske taktike je, da uporabi ukrepe, ki so glede na značilnosti posameznega primera najprimernejši ter bodo lahko vodili do uspešnega konca preiskave (Šugman in Gorkič, 2011).

Ustavno sodišče uporablja tudi tako imenovan strogi test sorazmernosti, s katerim v treh korakih presojava, ali je poseg PPU nujen, ali je poseg primeren za dosego cilja

ter ali je teža posledic ocenjevanega posega v prizadeto človekovo pravico proporcionalna vrednosti zasledovanega cilja oziroma koristim, ki bodo zaradi posega nastale; gre za t. i. načelo sorazmernosti v ožjem smislu (Šturm et al., 2002). S sorazmernostjo naj ne bi imeli težav, saj je treba izhajati iz enega najbolj pomembnih načel Konvencije o otrokovih pravicah (1992), posebej zapisano v njenem 3. členu, da so pri vseh dejavnostih v zvezi z otroki, bodisi da jih vodijo državne bodisi zasebne ustanove za socialno varstvo, sodišča, upravni organi ali zakonodajna telesa, otrokove koristi glavno vodilo in da otroci po Ustavi Republike Slovenije (2013) uživajo posebno varnost in skrb (56. člen). To posebno varstvo državo zavezuje, da z ustreznimi ukrepi zagotovi uveljavitev otrokovih pravic in zagotovi pravni položaj otroka (Jenkole, 2008).

V dotičnem primeru ob predstavljenemu tipičnemu načinu storitve kaznivega dejanja in postopkov odkrivanja glede na delovanje policista bi bilo nujno uporabiti ukrep tajnega delovanja (155.a člen ZKP) v kombinaciji z ukrepom prirejene identitete (24. člen Zakona o nalogah in pooblastilih policije, 2013, v nadaljevanju ZNPPol), saj ukrepa pokrivata dejanja policista, ki so opisana v analiziranemu primeru. Ker policist pri svojem tajnem delovanju uporablja tudi tehnične pripomočke (računalnik, spletna kamera), pride v poštev tudi prisluškovanje in snemanje pogovorov s privolitvijo vsaj ene osebe, udeležene v pogovoru (4. točka prvega odstavka 150. člena ZKP). Združitev tega ukrepa s tajnim delovanjem je predvidena tudi v 4. odstavku 155.a člena ZKP.

V zapisanem primeru v prejšnjem poglavju pri uporabi PPU predstavlja zakonsko podlago za spremembo identitete policista ali izjemoma kakšne druge osebe 155.a člen ZKP, ki pa se sklicuje na 23. člen ZNPPol, uporablja pa se z ukrepom tajnega delovanja. Ukrep prirejene identitete se izvede na predlog policije s privolitvijo državnega tožilca (prvi odstavek 23. člena ZNPPol). ZNPPol sicer ne predpisuje vsebine ali oblike dovoljenja državnega tožilca, vendar zanj po analogiji veljajo smiselno enake kot za odredbo o tajnem delovanju (Šugman in Gorkeč, 2011). Predpogoj za pristop k operativnemu prodoru TPD v spletno klepetalnico je zagotovo dobro pripravljena identiteta skupaj z verjetno logično, miselno in preverljivo življenjsko zgodbo – t. i. legendo, in sicer se lahko prirejena identiteta tajnega delavca pripravi v skladu s pogoji, ki jih za to določa ZNPPol tudi pred izdajo odredbe iz 24. člena oziroma konkretno pred pisno odredbo, ki jo izda državni tožilec ali preiskovalni sodnik, s katero dovolita izvajanje PPU tajnega delovanja. Tajni delavec z ustvarjanjem legende vzpostavlja tesne stike tudi z velikim številom ostalih oseb,

ki niso subjekti predkazenskega postopka in zoper njih ni bi odrejen prikriti ukrep tajnega delovanja. Pri tem tajni delavec pogosto pride do informacij, ki se nanašajo na druga kazniva dejanja drugih oseb. V zvezi s tem se postavlja vprašanje okoli narave tako pridobljenih podatkov in informacij (Eržen, 2009).

Na internetu vidnosti delovanja policije ni, saj poleg številke IP policista, ki dostopa do določene spletne strani, sodeluje na forumu ali klepetalnici, ne utripa modra luč, ki bi dala vedeti, da imajo pred sabo uradno osebo; ravnanje policista v virtualnem svetu lahko primerjamo z njegovim delovanjem na javnem kraju – mora biti nevpadljivo in zakonito (Klemenčič, 2007).

Z vstopom v klepetalnico se odpre problematika morebitnega izzivanja kriminalne dejavnosti (tako imenovani entrapment), saj tajni policijski delavec uporablja trike, strateške pasti ali zanko, nastavljeno obdolžencu – torej se mora pretvarjati, lagati in zavajati (Maver, 2008). Gre za t. i. preslepitev kot taktiko v kriminalističnem preiskovanju, kar je vsekakor etično sporno, vendar v primerih PPU država to dopušča – ne le za pridobivanje informacij, pač pa tudi dokazov (Maver, 2008) na tak način, da policist potencialnim storilcem zgolj ponuja sredstva in priložnosti in na njih ne vpliva z dodatnimi provokacijami, ki bi lahko osumljenca izzvale k storitvi kaznivega dejanja. Kot smo že omenili v prejšnjem poglavju, je zakon za takšno presojanje predpisal objektivni test, pri katerem se izzvanost kriminalitete oceni po objektivnih lastnostih posameznika. Lahko pridemo do sklepa, da policist z vstopom v klepetalnico ne izziva kriminalne dejavnosti, saj zgolj napeljuje pogovor izključno na ključne teme in dogodke, v opisanem primeru pa je zgolj pasiven, ko z besedilom »Čau, js sm tud tuki. Kva dugaja?« samo pozdravi in potencialne storilce opozori na svojo prisotnost in jih morda dodatno spodbuja k navezovanju stika. Tukaj si zastavimo vprašanje, ali lahko pride do ekskluzije dokazov, če bi prišlo do rednega kazenskega postopka, kjer gre za sojenje storilcem kaznivih dejanj, saj ZKP (2012) v 83. členu določa, da se sodna odločba ne sme opirati na prepovedane dokaze, ki so pridobljeni s kršitvijo z ustavo določenih človekovih pravic in temeljnih svoboščin in tudi na dokaze, ki so bili pridobljeni s kršitvijo določb kazenskega postopka in je zanje v zakonu določeno, da se sodna odločba nanje ne sme opirati. Treba je izločiti vse dokaze, za katere se v fazi preiskave (lahko tudi prej) ugotovi, da je zanje nekje drugje v ZKP (2012) določeno, da se sodna odločba nanje ne sme opirati. Smisel izločitve dokazov je v tem, da se nezakoniti dokazi na sojenju ne uporabijo ter da se z njimi ne seznanijo tisti, ki vsebinsko odloča o zadevi.

Velja pa opozoriti na drug sporen vidik tovrstnega vstopanja v klepetalnico, saj morajo biti za izvajanje PPU izpolnjeni določeni dokazni standardi (v tem primeru utemeljeni razlogi za sum), oseba, proti kateri so ukrepi usmerjeni, pa vsaj določljiva. Oseba, zoper katero se vodi preiskava, mora biti individualno določena, ni pa nujno, da so znani tudi njeni pravi osebni podatki, ampak le tisti, ki so zadostni za določljivost osebe (Horvat, 2004). Kavšek in Bele (2011) dalje opozorita, da oseba, zoper katero se izvaja PPU, ni nujno, da je vedno osumljenec, saj je v nekaterih primerih rezultat, ki ga zasleduje odrejeni ukrep (pridobitev informacij oziroma podatkov), mogoče doseči le s posegom (tudi) v zasebnost drugih oseb, ki niso osumljenci. Razlog, da se PPU odredi zoper osebo, ki ni osumljenec, je po navadi ta, da je odrejen z namenom, da se osumljenca oziroma njegovo identiteto, kraj, kjer se nahaja itd., šele odkrije in zato ukrep ne more biti odrejen zoper njega. Iz tega vidika pa je tovrstno delovanje že bolj problematično, saj je usmerjeno na nedoločeno število oseb, ki tudi niso vnaprej določljive, kar logično pomeni, da zoper posameznike niso vnaprej podani utemeljeni razlogi za sum, temveč se le-ti kvečjemu pojavijo tekom pogovora, ko ukrep že poteka. Na podlagi analiziranega primera policija skozi pogovor s storilcem pridobi identifikacijske podatke, ki pomenijo določljivost osebe, kljub napačnim osebnim podatkom lahko vsebujejo vse obligatorne sestavine za določljivost osebe, zoper katero se izvaja ukrep (nadimek, pridobitev telefonske številke ob dogovoru za srečanje, naslov prebivališča).

Pri ukrepu tajnega delovanja, ki ga policist uporablja v predstavljenemu primeru, ZKP v 4. odstavku 155.a člena že predvideva tudi uporabo tehničnih naprav za prenos in snemanje glasu, fotografiranje in video snemanje. Ta sredstva se lahko uporabijo zgolj v zvezi s kaznivimi dejanji iz drugega odstavka 150. člena ZKP, kamor pa sodijo tudi kazniva dejanja, ki jih preiskuje policist, zato policist lahko tako deluje. Uporabo teh sredstev mora s pisno odredbo na predlog državnega tožilca, odobriti preiskovalni sodnik (četrti odstavek 155.a člena). V primeru tajnega delovanja v kombinaciji z uporabo tehničnih naprav mora odredba vsebovati tudi opredelitev vrste in načina uporabe tehničnih sredstev. Manjše kot je število ukrepov, ki jih izvaja policija, manjša je verjetnost, da bo prišlo do napak, saj v primeru dodatnih predlogov, podaljšanj lahko hitro pride do zatipkanja (primer: napačno zapisana številka EMŠA), kar lahko privede do izločitve dokazov.

Na splošno pa za uporabo tehničnih sredstev za dokumentiranje in snemanje velja, da se jih uporablja glede na zahteve posameznega prikritega preiskovalnega ukrepa in le ob izpolnjenih formalnih in materialnih predpostavkah. Predvsem mora biti uporaba

odobrena v odredbi, kjer je natančneje opisan tudi način izvajanja posameznega ukrepa in naprave, ki se v ta namen uporabijo (Šugman in Gorkič, 2011). Hkrati pa drži, da nam vsa ta zbrana dejstva nič ne koristijo, če kaznivega dejanja pridobivanja oseb, mlajših od petnajst let, za spolne namene ni mogoče v celoti dokazati.

Kot vidimo, je odgovor na vprašanje, ali lahko v našem primeru odredimo policijsko pridržanje, odvisen od vrste vprašanj, med drugim tudi od tega, ali sploh obstaja utemeljen razlog za sum, v kar smo v prejšnjih točkah že podvomili. Če se pretvarjamo, da je le-ta prisoten in za trenutek pozabimo na svoje pomisleke, je tukaj še vedno vprašanje, ali je izpolnjen kateri izmed pripornih razlogov ter ali je ukrep sorazmeren. Policisti smejo nekemu izjemoma odvzeti prostost in ga pridržati ob izpolnjenih naslednjih pogojih, ki so določeni v drugem odstavku 157. člena ZKP:

- če so podani utemeljeni razlogi za sum, da je storil kaznivo dejanje, za katero se storilec preganja po uradni dolžnosti,
- če je pridržanje potrebno zaradi ugotovitve istovetnosti, preverjanja alibija, zbiranja obvestil in dokaznih predmetov o tem kaznivem dejanju,
- če so za pripor podani razlogi iz 1. in 3. točke prvega odstavka 201. člena ZKP in 1. in 2. točke prvega odstavka 432. člena ZKP, v primeru iz 2. točke prvega odstavka 201. člena ZKP pa le, če je opravičena bojazen, da bo ta oseba uničila sledove kaznivega dejanja.

Če poenostavimo, mora policist najprej upoštevati:

- da obstajajo utemeljeni razlogi za sum storjenega kaznivega dejanja, če je pridržanje potrebno:
 - zaradi ugotavljanja istovetnosti,
 - preverjanja alibija,
 - zbiranja obvestil in dokaznih predmetov o tem kaznivem dejanju (npr. 173.a člen KZ-1B, 2011),
- in da je hkrati s tem podan vsaj en priporni razlog (201. člen ZKP):
 - begosumnost storilca,
 - koluzijska nevarnost,
 - ponovitvena nevarnost.

Storilec iz analiziranega primera je predhodno že dokončal kaznivo dejanje, preden je uspel storiti novo ali drugo kaznivo dejanje (npr. spolni napad na osebo, mlajšo od 15 let po 173.a členu KZ-1). Za to dejanje, če ga nismo že predhodno kdaj obravnavali, ni podan pogoj ponovitvene nevarnosti, je pa podan drug priporni

razlog: koluzijska nevarnost oziroma uničevanje dokazov, kar pomeni, da mu bo policija odvzela prostost in ga pridržala toliko časa (do največ 48 ur), da bo lahko izvedla hišno preiskavo ali osebno preiskavo ter mu zasegla vso računalniško opremo, računalnike, telefone in druge elektronske naprave, vključno z zapiski in nosilci podatkov (CD, DVD, mikro kartice, USB ključe ipd). Ko bodo opravljeni hišna preiskava in zasegi, pa bo največkrat odpadel oziroma prenehal tudi priporni razlog. Storilec bo šel na prostost, ker drugega pripornega razloga nimamo. Tako testa sorazmernosti ne bo preстал priporni razlog ponovitvena nevarnost, razen če na zaseženih elektronskih napravah najdemo posnetke s spolnimi zlorabami otrok podatke o več otrocih, s katerimi je bil storilec v stikih ali pa je celo katerega izmed njih neposredno zlorabil.

Z dejanji, ki predstavljajo inkriminirano kaznivo dejanje pridobivanja oseb, mlajših od petnajst let, za spolne namene so v večini primerov povezana tudi druga kazniva dejanja. V primeru, ko nagovarjanju prek informacijskih ali komunikacijskih tehnologij storilca z otrokom, mlajšim od 15 let, sledi dejansko srečanje in spolni napad oziroma ima z njo spolne odnose, tudi če ta sama privoli v to dejanje brez sile ali grožnje, storilcu sodijo za kaznivo dejanje spolnega napada na osebo, mlajšo od 15 let, po prvem odstavku 173. člena KZ-1 (2008). Gre za to, da je storilec z enim samim dejanjem, se pravi s storitvijo, uresničil zakonske znake dveh kaznivih dejanj, oziroma še nazorneje povedano, uresničil je dvoje ali več prepovedanih posledic, ki so določene v dveh ali več členih kazenskega zakonika ter je celotna kriminalna količina kaznivega dejanja spolne zlorabe otrok v hujšem kaznivem dejanju (Bavcon, Jakulin in Korošec, 2003). Če prikažemo na opisanem primeru, je storilec dogovorjeno kaznivo dejanje izvršil ali vsaj poskušal izvršiti (spolni napad), potem predhodna faza, dogovor izgubi samostojnost in se vključi v izvršeno ali poskušano kaznivo dejanje kot njegov naravni in pravni sestavni del – torej kvalificirana oblika hujšega kaznivega dejanja konzumira blažjo obliko – gre za t. i. navidezni idealni stek in odnos konsumpcije.

V prvem odstavku 173. člena KZ-1 (2008) so zapisani primeri spolnih dejanj z osebo drugega ali istega spola, ki še ni stara petnajst let. Vsi spolni odnosi morajo biti pri pravni opredelitvi po prvem odstavku tega člena prostovoljni, s pristankom ali vsaj brez upiranja osebe, stare manj kot petnajst let. Šele s petnajstim letom lahko otroci samostojno privolijo v spolne aktivnosti, vendar ne v vse njene oblike. Seveda gre pri tem za psihofizično zdrave otroke, za katere se upravičeno domneva, da zmorejo razumeti pomen njihove odločitve in posledice. Po petnajstem letu se

mladostnike varuje pred prisilnim spolnim odnosom, npr. posilstvom, spolnim nasiljem ali pred spolnim odnosom pod a) pretvezo, b) silo ali c) omamljanjem (2. točka 173. člena KZ-1); tak primer bi bila spolna zloraba npr. šestnajstletne duševno slabotne osebe, ki se v svojem stanju sploh ne bi mogla braniti. Kaznivo dejanje je podano tudi v primeru, ko oseba pod petnajstimi leti sama da pobudo za spolne odnose. Dejanje iz prvega odstavka tega člena ni protipravno, če je bilo storjeno z osebo primerljive starosti in če ustreza stopnji njene duševne in telesne zrelosti (peti odstavek 173. člena KZ-1, 2008).

V primeru, ko storilec v varnem zavetju svojega doma brska po internetu oziroma kjerkoli tam, kjer komunicira z otrokom in ga zelo nazorno nagovarja na spolni odnos, spolna dejanja ali spolno aktivnost, vse to na vulgaren način, ko je njegovo celotno ravnanje usmerjeno k prizadetju spolne nedotakljivosti osebe, ki še ni stara 15 let in s tem zadovoljuje svoj nagon – odgovarja za kaznivo dejanje, predvideno v četrtem odstavku 173. člena KZ-1 (2008).

Pri kaznivem dejanju, ko storilec mladoletno osebo namesto spolnega odnosa spodbudi h golemu fotografiranju, na masturbacijo ali drugačno seksualno predstavo preko spletne kamere in gradivo shrani zase, za koga drugega ali objavi na spletu, gre za t. i. izdelavo avdiovizualnih ali drugih predmetov pornografske ali drugačne seksualne vsebine s pristankom (z uporabo sile, grožnje, preslepitvijo, prekoračitvijo ali zlorabo pooblastil, novačenjem, nagovarjanjem ali zaradi izkoriščanja navede) – storilec odgovarja za naklepno kaznivo dejanje 176. člena KZ-1 (2008), ki se glasi: prikazovanje, izdelava, posest in posredovanje pornografskega gradiva. Za nadaljevano kaznivo dejanje se ne uporabijo določbe o steku, ampak se določi ena kazen v mejah kazni, predpisane za najhujše izmed kaznivih dejanj (54. člen KZ-1, 2008). Pri tem kaznivem dejanju gre za grob poseg v varnost, telesno in spolno integriteto mladoletnih oseb, ki so pogosto žrtve storilcev, tudi organiziranega kriminala, ki izkoriščajo najbolj ranljivi del človeške populacije – otroke (Višje sodišče v Ljubljani, 2012). Podatke o tovrstnem gradivu policija dobi večinoma iz tujine in na podlagi teh začnejo ugotavljati identifikacijo storilca (Moran iz Interpola ... , 2011).

Pridemo lahko tudi do domneve, da je nekdo zavestno, z naklepom izdelal klepetalnico, da si tu zaupanja vredni uporabniki preko anonimnih sistemov za gostovanje datotek lahko izmenjujejo posnetke s spolnimi zlorabami otrok. Njihova komunikacija in izmenjava poteka v skritih omrežjih (I2P, freenet, darknet ipd.) s pomočjo Tora, orodja, ki poskrbi za internetno anonimnost. V tem primeru gre za

napeljevalca, in ker odločilno prispeva k izmenjavanju CAM, mu je možno očitati sotorilstvo po tretjem odstavku 176. člena KZ-1 (2008).

Pri preučevanju pravne ureditve PPU smo izhajali iz dejstva, da do sedaj v Republiki Sloveniji za preiskovanje spolnih zlorab otrok na internetu še niso bili uporabljeni. Po uporabljenih metodah preučevanja obravnavane teme in predstavljenega primera lahko delno zavrnamo prvo hipotezo, ki se glasi, da slovenska zakonodaja omogoča učinkovito izvajanje prikritih preiskovalnih ukrepov za pregon kaznivega dejanja »groominga. V primeru, če pride do tega dejanja, nato pa še do neposredne spolne zlorabe, ne obravnavamo več dveh kaznivih dejanj, ampak zgolj le eno, hujše kaznivo dejanje iz 173. člena KZ-1. Po skoraj dveh letih od uveljavitve navedenega kaznivega dejanja policisti niso podali še nobene kazenske ovadbe, so potrdili na Generalni policijski upravi v Sloveniji, saj to kaznivo dejanje s predpisano kaznijo enega leta zapora sodi med blažje prestopke, za katere policija ne more storiti ničesar odločilnega pri uporabi PPU (Lovšin, 2014). V praksi ne bo teoretične in praktične možnosti, da bi poskušali kaznivo dejanje najprej odkriti in preprečiti s t. i. klasičnimi policijskimi ukrepi, potem pa bi predlagali še PPU.

Problematično je tudi postaviti TPD v on-line, ko naj komunicira kot npr. deklica, saj postopki navedbe vzdevka niso določeni dovolj natančno. Problematično je dodeljevati vzdevek kar tako, ne da bi kasneje sploh izvajali ustrezno dovoljene PPU (npr. tajno delovanje v povezavi z ukrepi iz 150. člena ZKP). Dejstvo je, da mora policija predlagati pristojnemu državnemu tožilcu »prirejenost identitete« z namenom, da jo bo lahko potem, po izdaji sodne odredbe za PPU, pravočasno in primerno dovoljenju uporabljal. Sama prirejena identiteta, ki se samo pripravi (legenda, profil osebe), še ne more pomeniti izvajanja PPU, če se takšna »nova« identiteta uporablja skupaj s PPU, in zopet, ker se PPU v Sloveniji uporablja za konkretno osebo oziroma zoper osebo, ki ji je mogoče čim bolj natančno opredeliti fokus (A. T. Klančnik, osebni intervju, 10. 8. 2014).

Torej, v primerih kaznivega dejanja groominga je pomembno, ali že imamo nek fokus zoper osebe ali pa ga nimamo. V praksi bi to lahko pomenilo, da če bi šlo za resnično deklico, mlajšo od 15 let, in bi z njo preko spletne klepetalnice navezalo stik kup vsiljivcev, ki bi ji sugerirali spolne aktivnosti (torej spolne zlorabe), bi si policija smela pripraviti prirejeno identiteto ob vnaprejšnjem dovoljenju pristojnega državnega tožilca, čemur pa bi sledilo tudi pridobivanje sodne odredbe za izvajanje PPU (tajno delovanje in z nekaterimi ukrepi iz 150. člena ZKP) in šele nato realno

izvajanje PPU na npr. njenem računalniku; njeno identiteto (deklince, mlajše od 15 let) bi verjetno prevzel TPD (A. T. Klančnik, osebni intervju, 10. 8. 2014).

Če pa je govora o tem, da bi si policija pridobila dovoljenje pristojnega državnega tožilca, da nekaj policistom priredi identiteto in bi kot takšni vstopali v klepetalnice, se predstavljali, da so deklince ali dečki, mlajši od 15 let, bi verjetno lahko pomenilo policijsko provokacijo (verjetnost zato, ker navajanje vzdevka »Lilly_12« bi lahko ali pa ne pomenila provokacijo, odvisno od okoliščin primera). Tu se nadalje poraja dvom, ali bi policija pridobila ustrezne sodne odredbe za izvajanje PPU po tem, ko bi bili policisti s prirejeno identiteto seznanjeni z vzdevki storilcev (vsiljivcev), ki bi spolno izkoriščali otroke. Verjetno ne, ker namen prirejene identitete ni v tem, da na osnovi nje pridobimo podatke za druge ukrepe. Mislimo, da ta varianta pri nas ni mogoča oziroma ni bila še preizkušena v praksi, ampak menimo, da bi utegnila zadeva propasti, ne glede na dober namen. In še naslednje vprašanje, ki se nam poraja: ali je bil v tem primeru že realiziran fokus na konkretnega storilca, še preden so policisti priredili identiteto in komunicirali v klepetalnici ter ali je bilo že kako sporno sodelovanje policije v komunikaciji v klepetalnici s prirejeno identiteto? Pri prvem vprašanju ni bilo fokusa, ampak ad hoc vstop v klepetalnico; drugo vprašanje pa je: kaj ni to že neke vrste izvajanje prikritega preiskovalnega ukrepa (A. T. Klančnik, osebni intervju, 10. 8. 2014)?

Ključno vprašanje, ki se nam tu poraja, je, ali si torej sme policija nadeti vzdevek in preverjati klepetalnice. Sme, vendar v kakšnem smislu; lahko se jo preprosto obišče na neki spletni strani, še posebej, če je javno dostopna, se evidentira, kaj se v klepetalnici dogaja in to ustrezno opredeli, če je v nasprotju s kazensko zakonodajo. Problematično je, da bi policisti kar komunicirali ter tako pridobivali dokaze zoper storilca, oziroma bi ga k temu spodbujali (A. T. Klančnik, osebni intervju, 10. 8. 2014).

Naslednji zaplet, ki se pojavi pri uporabi PPU v zvezi s kaznivim dejanjem pridobivanja oseb, mlajših od petnajst let, za spolne namene; da gre v tem primeru lahko kvečjemu za neprimeren poskus kaznivega dejanja, saj policist ni primeren objekt, nad katerim bi osumljenec lahko zagrešil tovrstno kaznivo dejanje, zato srečanje policista s potencialnim storilcem ni izvedljivo. V primeru, če se storilec premisli in odstopi od samega srečanja z žrtvijo zaradi nizke predpisane kazni za tovrstno kaznivo dejanje (zapor do enega leta) kazenski pregon ne bo mogoč, saj je poskus kazniv zgolj za kazniva dejanja, za katera je zagrožena zaporna kazen vsaj treh let (34. člen KZ-1).

Poleg normativne ureditve je potrebno upoštevati tudi razsežnost izvršitvenih kaznivih dejanja s področja zoper spolno nedotakljivost otrok. V kolikor so tovrstni dokazi pridobljeni v tujini, je treba upoštevati suverenost države in njeno zakonodajo v povezavi z našo pravno ureditvijo, to pomeni, da morajo biti pridobljeni v skladu z notranjo pravno ureditvijo države, kjer so se pridobivali, torej obstajati mora teritorialna pristojnost sodišča za pregon tega kaznivega dejanja na območju RS in da niso pri tem kršene človekove pravice in temeljne svoboščine, zagotovljene z našo ustavo in sprejetimi mednarodnimi pravnimi akti (Višje sodišče v Ljubljani, 2014).

Ker niso bili ukrepi nikdar uporabljeni, se porajajo pomisleki, ali so še kakšni razlogi (organizacijski, kadrovski, tehnični), saj se vsi ti nanašajo na izvedbo PPU.

Ali imamo v Sloveniji zadostno tehnično podporo za izvajanje prikritih preiskovalnih ukrepov in pooblastila za takšno izvajanje (kako vedeti, točno na katerih strežnikih iskati in na kateri točki zoper določeno osebo obstaja dokazni standard, vsaj razlogov za sum)? Kljub uspešnemu patroljiranju (identifikacija storilca, ki podatke nalaga na računalnik) je v Sloveniji vprašljivo tudi izvajanje PPU z vidika finančnih sredstev. Na splet se priključujejo uporabniki s celega sveta (vsakogar identificirati, znati jezik, ki ga govori), v ta namen ima v Sloveniji policija po navedbah Klančnika (2013a) organizirane in specializirane enote, ki se ukvarjajo s tematiko spolnih zlorab otrok preko interneta, in sicer v tem trenutku gre za 30 specializiranih kriminalistov za mladoletniško kriminaliteto, ki preiskuje spolne delikte nad otroki, hkrati pa pri svojem delu sodelujejo z notranjimi službami policije (center za računalniško preiskovanje, sektor za mednarodno policijsko sodelovanje) in zunanjimi službami (državno tožilstvo, sodišča, centri za socialno delo, vzgojno-izobraževalne institucije, inšpekcijske službe in agencije, nevladne organizacije, ponudniki internetnih storitev oziroma mobilne telefonije). Hkrati pa navaja, da policija tudi na tem področju sodeluje s tujimi policijami, Europolom in Interpolom, v skupnih preiskavah in delovnih skupinah. Da policisti pridejo na sled storilcu z uporabo PPU, porabijo ure, dneve in mesece svojega delovnega časa, da ugotovijo, kdo se je prijavil v klepet, da identificirajo osebo, ugotovijo, katere podatke/gradivo prenaša na svoj računalnik, da ne omenjamo porabe elektrike, vsega potrebnega za presnemavanje vseh pogovorov in snemanje pogovorov, v katerih je storilec napeljeval k srečanju ali k storitvi katerega izmed kaznivih dejanj zoper spolno nedotakljivost. Tudi tukaj se pojavi ena od možnosti, ki bi jo lahko uvedli v zakonodajo – vsa dejanja, ki jih stori policija in ki pomenijo visoke finančne vložke, namreč niso všteta v kazenski

postopek. Če bi storilci morali kriti vse te stroške sodnega postopka, bi bila zadeva morda malce drugačna. Kot primer naj navedem vlom, zaradi katerega policija porabi ure dela, da si kraj storitve dejanja dobro ogleda, slika in dokumentira; sledijo razgovori z lastniki in domnevnimi storilci – kar ni nič v primerjavi z zgoraj omenjenimi stroški, ki so porabljeni pri iskanju storilcev spolnih zlorab. Če v primeru storitve kaznivega dejanja žrtev na sodišču pove, da ne želi pričati (gre za t. i. institut privilegirane priče), se sodni postopek lahko konča z oprostivjo storilca vseh obtožb. To storilcev ne ustavi, nasilni so še naprej ali nasilje celo stopnjujejo do najhujše mogoče posledice, celo do umora (Pogosto zastavljena ..., 2014). Vsak posameznik bi moral nositi posledice svoje odločitve.

Pri uporabi PPU za pregon spolnih kaznivih dejanj zoper spolno nedotakljivost otrok naletimo tudi na dejstvo, ali le-ti posegajo v pravico do zasebnosti posameznika, ki je pri tem najbolj izpostavljena. Gre za vprašanje, ki bo v prihodnosti terjalo ogromno razmisleka, saj kolikor bolj internet prispeva h globalnemu pretoku informacij, toliko bolj je ranljiv za posege držav ter posameznih politikov in podobno, kolikor bolj internet postaja sredstvo za vsestransko vključitev človeka v družbo, toliko bolj so posegi v posameznikovo zasebnost pri komuniciranju lahko usodni (Klemenčič, Tičar in Makarovič, 2007). Pravica do zasebnosti uporabnikov informacijskih sistemov predstavlja pravico do informacijske in komunikacijske zasebnosti – posameznikov interes, da državi ali nepovabljenim tretjim osebam ne razkrije določenih informacij in ima nadzor nad tem, katere informacije in v kakšnem obsegu bo predstavil svetu ter da s svobodno voljo in informirano sprejema odločitve v vsakdanjem življenju. Torej ni samo pravica posameznika, da se ga pusti pri miru, gre za temeljno osebnostno pravico, ki je neločljivo povezana s svobodo, avtonomijo, notranjo rastjo in svobodno voljo posameznika (Klemenčič, Tičar in Makarovič, 2007). Gre za eno temeljnih pravic, ki je opredeljena v 35. členu Ustave Republike Slovenije (2013), na katerega se navezujeta tudi 36. in 37. člen Ustave. Pravica do zasebnosti po mnenju Kavškove in Beleta (2011) ni absolutna, ampak je omenjena z varstvom pravic in koristi drugih. Poseg v svobodo komuniciranja kot del človekove zasebnosti ni v nasprotju s 35. in 37. členom Ustave ob izpolnjenih naslednjih pogojih (Klemenčič, Kečanović in Žaberl, 2002):

- da je poseg specifično opredeljen in določen v zakonu;
- da poseg z odločbo dovoli sodišče;
- da je določno omejene čas izvajanja posega;

- da je poseg nujen za uvedbo ali potek kazenskega postopka ali za varnost države, upoštevanje pri presoji nujnosti tudi načelo sorazmernosti.

Poseg v pravico, varovano s podanim členom, se presoja s testom sorazmernosti. Po tem testu je treba tehtati dva elementa (Klemenčič, Tičar in Makarovič, 2007): pričakovanje zasebnosti in upravičenost tega pričakovanja, v nekaterih primerih pa je upravičenost pričakovanja zasebnosti abstraktno in vnaprej določena z zakonom, na primer pri prestrezanju in nadzorovanju telekomunikacij s strani državnih organov, v mnogih primerih (na primer nadzor s strani delodajalca) pa odsotnost določne zakonske regulative zahteva ocenjevanje vsakega posameznega primera posebej. Že Šturm et al. (2002), je zapisal, da bo morala slovenska ustavnosodna praksa upoštevati načelo sorazmernosti in odtehtati interes ali pravico posameznika nasproti ustavno zavarovanemu javnemu interesu in ne le eno ustavno pravico nasproti drugi, kar pomeni, da je ustavne pravice mogoče omejiti, če zakonodajalec na podlagi tehtanja javnih koristi in individualnih pravic ugotovi, da je omejitev nujno potrebna. In še dodaja, da je ukrep, s katerim zakonodajalec omeji ustavno pravico, utemeljen, če iz narave neke dejavnosti izhaja, da so za njeno izvajanje potrebna posebna znanja, sposobnosti in osebne lastnosti, brez katerih bi lahko nastale škodljive posledice ali nevarno stanje za posameznike.

V slovenskem pravnem redu na splošni ravni zaščito tajnosti in zaupnosti (posredno tudi zasebnosti) ureja Zakon o elektronskih komunikacijah (2012, v nadaljevanju ZEKom-1). Slednji v dvanajstem poglavju operaterje javnih sistemov, preko katerih se opravljajo elektronske komunikacije, zavezuje k zaščiti tajnosti in zaupnosti komunikacij in v prvem odstavku 147. člena določa, da se zaupnost komunikacij nanaša na: 1. vsebino komunikacije; 2. podatke o prometu in lokacijske podatke, povezane s komunikacijo iz prejšnje točke; 3. dejstva in okoliščine neuspešnih poskusov vzpostavljanja zvez. Zakonito prestrezanje, nadzor in shranjevanja komunikacij so dopustni zgolj, če je to nujno za samo izvedbo komunikacij (na primer SMS, faks sporočil in e-pošte); v okviru zakonite poslovne prakse z namenom, da se zagotovi dokaz o tržni transakciji ali katerikoli drugi komunikaciji, ali v okviru organizacij, ki sprejemajo klice v sili, zaradi njihove registracije, identifikacije in reševanja; v primeru zakonitega nadzora s strani državnih organov - slednje ureja isti člen (Klemenčič, Tičar, in Makarovič, 2007).

Z naslednjim bežnim orisom kazenskega postopka bi s Šugmanovo in Gorkičem (2011) lažje poudarili to, da je že upoštevanje ZKP in vestno sledenje temeljnim načelom kazenskega prava zagotovilo, da osumljencu tekom postopka ne bodo kršene pravice.

Domneva nedolžnosti je temeljno osnovno načelo vsakega modernega, demokratičnega kazenskopravnega procesnega sistema in tudi konkretno narekuje tempo kazenskega postopka; je nekakšna izhodiščna predpostavka za zgradbo celotne sheme dokazovanja in se prekriva s številnimi drugimi dokaznimi pravili. Domneva nedolžnosti varuje osumljenca skozi celoten postopek, glavni posledici tega sta dve: dokazno breme je na tožilcu, kar omogoča osumljencu popolno pasivnost in povzroči, da ima sodišče možnost izreka samo dveh vrst meritornih sodb, saj se vsak postopek, kjer krivda ni dokazana, z dokaznim standardom onkraj razumnega dvoma skladno s tem načelom konča z oprostilno sodbo. Domneva nedolžnosti pa nima učinka le na sojenju, temveč ima odločilen vpliv na vse faze kazenskega postopka. Policija skuša skozi predkazenski postopek s preiskovanjem izpodbiti ravno to domnevo nedolžnosti. Prav tu pa se pokaže poglobljen pomen dokaznih standardov, katerih glavni namen je v nasprotju z laičnim prepričanjem ravno varovanje položaja obsojenca, država bi namreč mnogo učinkoviteje posegala v pravice ljudi brez obstoja dokaznih standardov. Tako kot se skozi postopek stopnjujejo dokazni standardni, tako se torej hkrati zvišuje tudi zaščita obdolženca, preden bi država neutemeljeno posegala v njegovo integriteto. Stopnjevanje verjetnosti, da je oseba storila kaznivo dejanje, ki poteka skozi postopek, ja tako pravzaprav izraz domneve nedolžnosti in ne njeno nasprotje. Vse skupaj pomeni, da se domneva nedolžnosti razgrne v kaskado dokaznih standardov, vsak zase pa pomeni malo domnevo nedolžnosti, ki jo mora državni tožilec preseči, če želi doseči svoj delni cilj v postopku. Bistveno pravilo v zvezi s postopnim naraščanjem verjetnosti in domnevo nedolžnosti je, da mora biti najprej podana določena stopnja verjetnosti, da je posameznik prekršil pravila, šele nato lahko država vpreže svoj represivni aparat in začne dejanje raziskovati.

Na podlagi zapisanega zavrnamo drugo hipotezo, ki se glasi, da se z uporabo za pregon spolnih kaznivih dejanj na škodo otrok zelo kršijo pravice storilcev teh kaznivih dejanj. Kot že rečeno, je uporaba PPU v ZKP natančno normirana in opredeljena, prav tako so dodane formalne in materialne zahteve, ki so potrebne za odreditev posameznih ukrepov, kar naj bi preprečevalo zlorabo in morebitno arbitrarnost represivnih organov, če ne drugje bi se neupoštevanje zakona sankcioniralo vsaj na sodišču, v obliki ekskluzije nepravilno pridobljenih dokazov. Naj še dodamo, da bi morebitna ugotovitev, da PPU sami po sebi kršijo pravice storilcev tovrstnih dejanj, nujno vodila tudi v ugotovitev, da PPU kršijo pravice vseh osumljencev in so kot taki nesprejemljivi. To pa bi bilo nesmiselno, saj so PPU mednarodno in ustavno predpisan in sprejet način preiskovanja in preprečevanja

kriminalitete po vsem svetu, če se le izvajajo skladno z modernimi načeli pravne države in kazenskega prava.

6 Zaključek

Spolna zloraba je travmatična izkušnja, ki zlorabljenega otroka zaznamuje skozi celo življenje. Njegovo brezskrbno, razposajeno in varno otroštvo, polno igrivosti in odkrivanja novih stvari, se v hipu obrne na glavo, v dolgotrajne posledice, ki za vedno spremenijo kakovost njegovega zaznavanja.

O takšnih primerih smo ljudje premalo ozaveščeni in informirani, saj se ne zavedamo razsežnosti in posledic, ki jih dejanja pustijo na otroku, zato je treba ozaveščati javnost in povečati seznanjenost o spolnih zlorabah nad otroki, ki so vedno pogostejše. Otroke je treba že od malih nog poučevati o nevarnosti internetnih vsebin, kar lahko počnemo skozi redne pogovore prav v vseh dejavnostih, tako na šolski, občolski in drugih ravneh (taborih, letovanjih, izletih, učni pomoči, psihosocialni pomoči), skratka povsod. Pri vsem tem si je najlažje zatiskati oči in ne videti, kajti vse je dobro, dokler se ne dotakne nas in bližnjih. V diplomskem delu smo se osredotočili na eno izmed oblik spolnih zlorab otrok na internetu: pridobivanja oseb, mlajših od petnajst let, za spolne namene. Eden izmed razlogov, zakaj je to področje izredno problematično, je, da internet omogoča veliko stopnjo anonimnosti, kar storilci izkoriščajo za svoje početje, ki za vzpostavitev z otroki uporabljajo spletne klepetalnice, pri vsem tem pa se izdajajo za vrstnike svojih sogovornikov. Pri raziskavi tovrstnega kaznivega dejanja policija uporablja vedno več novih metod in sredstev, ki pomenijo odmik od klasičnih preiskovalnih metod. Zaradi družbenih nevarnosti je tako zakonodajalec privolil v omejevanje določenih človekovih pravic in temeljnih svoboščin s PPU, v primerih, ko je treba priti na sled storilcem hudih kaznivih dejanj, kar spolne zlorabe otrok nedvomno so. Osnovni namen PPU je zbiranje podatkov, ki se bodo kasneje uporabili kot dokazno gradivo v kazenskem postopku. Glede na njihovo raznolikost je intenziteta poseganja v ustavne pravice različna.

Težave v praksi pri izvajanju PPU zoper navedeno kaznivo dejanje zagotovo predstavljajo organizacijske, tehnične in kadrovske težave za izvedbo le-teh, saj so visoki pravni standardi v nekaterih delih pomanjkljivi in ne izhajajo iz dejstva, da so le mehanizem za zbiranje obvestil o storilcih in odkrivanju njihove prave identitete in še zdaleč ne obtožni akt.

Kaznivo dejanje pridobivanja oseb, mlajših od 15 let, za spolne namene je problematično za preiskovanje in dokazovanje, ker z zagroženo kaznijo enega leta

zapora preprečuje ključna policijska pooblastila in ne omogoča uporabe PPU, saj policist s prirejeno identiteto ni primeren objekt, nad katerim bi osumljenec lahko zagrešil tovrstno kaznivo dejanje, zato srečanje policista s potencialnim storilcem ni izvedljivo. Kljub temu pogoju kazenski pregon ne bi bil mogoč, saj je poskus kazniv zgolj za kazniva dejanja, za katera je zagrožena zaporna kazen vsaj treh let (34. člen KZ-1). Zakonodajalec je prirejeno identiteto ustrezno uredil le pri PPU tajnega delovanja. Ker pa postopki določitve vzdevka niso navedeni dovolj natančno v zakonu, ki ureja policijo, je bistvenega pomena, da žrtve same prijavijo napeljevanje z odkritimi spolnimi nameni, saj bi si v takšnih primerih policija smela pripraviti prirejeno identiteto ob vnaprejšnjem dovoljenju pristojnega državnega tožilca, čemur pa bi sledilo tudi pridobivanje sodne odredbe za izvajanje PPU in šele nato realno izvajanje PPU na računalniku, preko katerega je potekala komunikacija. Zato je pomembno, da so otroci seznanjeni s potencialnimi nevarnostmi, ki jih prinaša internet, in da žrtve nadlegovanje zaupajo svojim staršem, saj jih bodo ti lahko najlažje in najhitreje zaščitili.

Uvedba novega PPU bi bila tako nujno potrebna zaradi tehničnega vidika in razsežnosti interneta. Eden izmed takih ukrepov je navidezno patroljiranje v virtualnem svetu, s katerim kriminalist v spletni klepetalnici ne sme izzvati kriminalne dejavnosti in oseb ne napeljuje h kaznivemu dejanju, za katerega bi jih potem preganjal. Pri izvajanju tovrstnega ukrepa in ob strožji predpisani kazni za kaznivo dejanje novačenja oseb, mlajših od 15 let, za spolne namene po 173.a členu KZ-1B (2011), za katerega je domnevni storilec odgovoren, bi bila eno od značilnosti ukrepa osredotočenost na kraje, kjer bi se lahko izvajala kriminalna dejavnosti, in na nadzorovanje aktivnosti, ki bi lahko pripeljala do kriminalne dejavnosti. Torej v primeru, kjer bi nagovarjanju z otrokom preko računalnika sledilo srečanje, bi policisti storilcu pripravili zasedo na prostoru, ki je dovolj premišljen in dostopen. Ob zakonodaji, ki sledi trendom izvrševanja kaznivih dejanj, in ustreznih policijskih pooblastilih bi bilo mogoče tudi prej odkriti in preprečiti kazniva dejanja zoper spolno nedotakljivost otrok v povezavi s kibernetiskim prostorom.

Za uspešno zatiranje bomo morali v bodoče storiti narediti precej korakov naprej na različnih področjih, saj storilci pogosteje uporabljajo predrznejše metode za izvršitev kaznivih dejanj, zato bo v bodoče tovrstna tematika zahtevala od policije, tožilstva in sodišča strokovnost in izurjenost, ki jih bosta uspešno vodili v prid varnosti, pa tudi ustrezne mehanizme na področju zakonodaje in pravosodja. Obstaja bojazen, da bo to tudi eno izmed področij, ko bomo zaradi hudega posamičnega

primera prekomerno poostrovali postopke, namesto da bi že zdaj pripravili družbeni konsenz, kako naprej pri sami uporabi PPU. Če povzamemo besede Klančnika (2013a), se vprašajmo: Ali je v Sloveniji potreba po stresnem testu na področju internetnih spolnih zlorab, da bomo pripravljeni kaj storiti?

7 Uporabljeni viri

137. redna seja Vlade RS. (2. 6. 2011). *Vlada.si*. Pridobljeno na http://www.vlada.si/medijsko_sredisce/porocila_za_javnost/porocilo_za_javnost/article/137_redna_seja_vlade_rs_17865/
- Bain, Q. in Sanders, M. (1996). *Ko pride na dan. Vodič za mlade, ki so bili spolno zlorabljeni*. Ljubljana: Co Libri.
- Bavcon, L., Jakulin, V. in Korošec, D. (2003). Kaznivo dejanje in kazenska odgovornost. (2003) V L. Bavcon, A. Šelih, K. Filipič, V. Jakulin, in D. Korošec (ur.), *Kazensko pravo. Splošni del* (str. 153–376). Ljubljana: Uradni list Republike Slovenije.
- Bošnjak, M. (1998). Posegi v spolno nedotakljivost otrok. V Z. Kanduč, D. Korošec in M. Bošnjak, (ur.), *Spolnost, nasilje in pravo* (str. 225–253). Ljubljana: Inštitut za kriminologijo pri Pravni fakulteti in Urad za žensko politiko.
- Carr, J. (2003). *Child abuse, child pornography and the internet*. London: NCH.
- Dežman, Z. in Erbežnik, A. (2003). *Kazensko procesno pravo Republike Slovenije*. Ljubljana: GV Založba.
- Eržen, N. (2009). *Prikrite preiskave in zasebnost* (Diplomsko delo). Ljubljana: Fakulteta za varnostne vede.
- Evropska Unija. (2011). *Direktiva 2011/93/EU Evropskega parlamenta in Sveta o boju proti spolni zlorabi in spolnemu izkoriščanju otrok ter otroški pornografiji in nadomestitvi Okvirnega sklepa Sveta 2004/68/PNZ*. Pridobljeno na <http://register.consilium.europa.eu/pdf/sl/11/pe00/pe00051.sl11.pdf>
- Frangež, D. in Dvoršek, A. (2012). Nekatere dileme pri preiskovanju posnetkov spolne zlorabe. V A. Dvoršek in D. Frangež (ur.), *Digitalni dokazi: Kazensko pravni, kriminalistični in informacijsko-varnostni vidiki* (str. 59–73). Ljubljana: Univerza v Mariboru, Fakulteta za varnostne vede.
- Horvat, Š. (2004). *Zakon o kazenskem postopku (ZKP): s komentarjem*. Ljubljana: GV Založba.

- Interpol. (2013). *Cybercrime*. Pridobljeno na <http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime>
- Izbirni protokol h Konvenciji o otrokovih pravicah glede prodaje otrok, otroške prostitucije in otroške pornografije. (2004). *Uradni list RS*, (23/04).
- Jenkole, M. (2008). Otrokove pravice s poudarkom na koristi otroka in njegovi pravici, da je slišan, ter vloga zagovornika pravic otrok ob tem. V M. Jenkole, N. Kuzmič, S. Šemen in J. Turk (ur.), *Zagovornik - glas otroka: zbornik prispevkov za izobraževanje zagovornikov: pilotski projekt 2007–2009*, (str. 21-30). Ljubljana: Varuh človekovih pravic.
- Kavšek, N. in Bele, V. (2011). Prikriti preiskovalni ukrepi v sodni praksi. *Pravna praksa: časopis za pravna vprašanja*, 30(44), 2–8.
- Kazenski zakonik Republike Slovenije [KZ-1]. (2008). *Uradni list RS*, (55/08).
- Kdo smo? (2014). *Safe.si*. Pridobljeno na <http://safe.si/spletno-oko/kdo-smo-0>
- Klančnik, A. T. (2013a). Potreba po stresnem testu? Soočanje Slovenije z mednarodnimi razsežnostmi internetnih spolnih zlorab otrok. *Varnost*, 61(4), 36–43.
- Klančnik, A. T. (2013b). Tudi spolne zlorabe otrok preko interneta so globalni problem. *Varnost*, 61(3), 25–32.
- Klemenčič, G. (2007). Kibernetski kriminal. V M. Bogataj Jančič, G. Klemenčič, B. Makarovič, K. Tičar in J. Toplišek (ur.), *Pravni vodnik po internetu* (str. 361-395). Ljubljana: GV Založba.
- Klemenčič, G., Kečanović, B. in Žaberl, M. (2002). *Vaše pravice v policijskih postopkih*. Ljubljana: Pasadena.
- Klemenčič, G., Tičar, K. in Makarovič, B. (2007). Internet in človekove pravice. V M. Bogataj Jančič, G. Klemenčič, B. Makarovič, K. Tičar in J. Toplišek (ur.), *Pravni vodnik po internetu* (str. 361–395). Ljubljana: GV Založba.
- Kodelja, M. in Banovič, Z. (15. 5. 2010). Kdo je žrtev spletnega nadlegovanja? *Mojmikro.si*. Pridobljeno na http://www.mojmikro.si/v_srediscu/razkritje/kdo_je_zrtev_spletnega_nadlegovanja

- Kodelja, M. in Banovič, Z. (16. 7. 2012). Globoki splet in temni internet. *Mojmikro.si*. Pridobljeno na http://www.mojmikro.si/v_srediscu/razkritje/globoki_splet_in_temni_internet
- Kodelja, M. in Banovič, Z. (30. 7. 2012). Popotovanje v globino. *Mojmikro.si*. Pridobljeno na http://www.mojmikro.si/v_srediscu/razkritje/popotovanje_v_globino
- Kodelja, M. in Banovič, Z. (9. 7. 2012). Kaj je pod površino spleta? *Mojmikro.si*. Pridobljeno na http://www.mojmikro.si/v_srediscu/razkritje/kaj_je_pod_povrsino_spleta
- Komuniciranje na internetu.* (2013). Pridobljeno na <http://www2.arnes.si/~sspmkotn/edus/internet/komuniciranje.htm>
- Konvencija o kibernetiski kriminaliteti. (2004). *Uradni list RS*, (17/04).
- Konvencija o otrokovih pravicah [KOP]. (1992). *Uradni list RS*, (9/92).
- Konvencija Sveta Evrope o zaščiti otrok pred spolnim izkoriščanjem in spolnim zlorabljanjem.* (2007). Pridobljeno na <http://conventions.coe.int/Treaty/EN/Reports/Html/201.htm>
- Kovačič, A. in Klančnik, A. T. (2012). Michael Moran: »Ljudje morajo spoznati, da ne gre za pornografijo, pač pa za spolno zlorabo otrok.« *Varnost*, 60(2), 67–69.
- Lovšin, M. (3. 3. 2014). Brez ovadb za spletno novačenje otrok. *Dnevnik.si*. Pridobljeno na <http://www.dnevnik.si/kronika/brez-ovadb-za-spletno-novacenje-otrok>
- Maver, D. (2008). Preslepitev kot taktika v kriminalističnem preiskovanju. *Varstvoslovje*, 10(3), 434–449.
- Moran iz Interpola: Zloraba otrok prek spleta je globalen problem. (9. 10. 11). *Dnevnik.si*. Pridobljeno na <http://www.dnevnik.si/kronika/1042478885>
- Naši otroci so bolj ogroženi. (24. 12. 2008). *Mojmikro.si*. Pridobljeno na http://www.mojmikro.si/news/nasi_otroci_so_bolj_ogrozeni
- Otroci nas nemo opozarjajo na spolne zlorabe nad njimi. Odprimo oči! (2. 6. 2014). *Policija.si*. Pridobljeno na

<http://www.policija.si/index.php/component/content/article/35-sporocila-za-javnost/73135--otroci-nas-nemo-opozarjajo-na-spolne-zlorabe-nad-njimi-spreglejmo?tmpl=component&print=1&page=&lang=>

Pogosto zastavljena vprašanja žrtev nasilja v družini (20. 4. 2014). *Policija.si*. Pridobljeno na <http://www.policija.si/index.php/component/content/article/182-kriminaliteta/67759-pogosto-zastavljena-vpraanja>.

Problematika spolnih zlorab otrok v Sloveniji. (07. 05. 2008). *Policija.si*. Pridobljeno na <http://www.policija.si/index.php/component/content/article/35-sporocila-za-javnost/2252-sporo2255>

Rajšp, R. (2008). *Internet bančništvo za pravne osebe na primeru Abanke Vipa d.d.* (Diplomsko delo). Maribor: Ekonomsko poslovna fakulteta Maribor.

Razpotnik, B. (28. 9. 2012). Teden otroka 2012. *Stat.si*. Pridobljeno na http://www.stat.si/novica_prikazi.aspx?id=5028

Skrtn, R. (2004). Otroška pornografija na internetu. *Nasvet.com*. Pridobljeno na <http://www.nasvet.com/pedofilija/>

Spam: nenaročeno oglaševanje po elektronski pošti. (2014). *Cert.si*. Pridobljeno na <https://www.cert.si/si/varnostne-groznje/spam/>

Stanley, J. (2001). *Child Abuse and the Internet. Child abuse prevention issues*, 15. Pridobljeno na <http://www.aifs.gov.au/nch/pubs/issues/issues15/issues15.html>

Svet Centra za varnejši internet. (2014). *Safe.si*. Pridobljeno na <http://safe.si/center-za-varnejsi-internet/o-centru/svet-centra-za-varnejsi-internet>

Šturm, L. (ur.), et al. (2002). *Komentar Ustave Republike Slovenije*. Ljubljana: Fakulteta za podiplomske državne in evropske študije.

Šugman, K. in Gorkič, P. (2011). *Dokazovanje v kazenskem postopku*. Ljubljana: GV Založba.

Ustava Republike Slovenije. (2013). *Uradni list RS*, (47/13).

Višje sodišče v Ljubljani. (2012). Sklep II Kp 9220/2011. Pridobljeno na http://www.sodisce.si/znanje/sodna_praksa/visja_sodisca/2012032113052385/

Višje sodišče v Ljubljani. (2014). Sodba II Kp 2457/2010. Pridobljeno na [http://sodnapraksa.si/?q=id:2012032113064861&database\[SOVS\]=SOVS&database\[IESP\]=IESP&database\[VDSS\]=VDSS&database\[UPRS\]=UPRS&_submit=i%C5%A1%C4%8Di&page=0&id=2012032113064861](http://sodnapraksa.si/?q=id:2012032113064861&database[SOVS]=SOVS&database[IESP]=IESP&database[VDSS]=VDSS&database[UPRS]=UPRS&_submit=i%C5%A1%C4%8Di&page=0&id=2012032113064861)

Vrhovno sodišče RS. (2013). Sodba I Ips 10095/2011-62. Pridobljeno na http://www.sodisce.si/znanje/sodna_praksa/vrhovno_sodisce_rs/2012032113053502/

Zakon o elektronskih komunikacijah [ZEKom-1]. (2012). *Uradni list RS*, (109/12).

Zakon o kazenskem postopku [ZKP]. (2012). *Uradni list RS*, (32/12).

Zakon o nalogah in pooblastilih policije [ZNPPol]. (2013). *Uradni list RS*, (15/13).

Zakon o spremembah in dopolnitvah Kazenskega zakonika [KZ-1B]. (2011). *Uradni list RS*, (91/11).

Zorko, S.R. Poreden sosedov striček ... (3. 11. 09). *Mojmikro.si*. Pridobljeno na http://www.mojmikro.si/preziveti/varnost/poreden_sosedov_stricek

Žaberl, M. (2006). *Temelji policijskih pooblastil*. Ljubljana: Fakulteta za policijsko-varnostne vede.