Vošnjakova 1, p.p. 78, SI-1000 Ljubljana
Telefon: + 386 (0) 1 230 97 30
Faks: + 386 (0) 1 230 97 78
www.ip-rs.si

Številka: 007-57/2013/
Datum: 12.12.2013
MINISTRSTVO ZA PRAVOSODJE
Župančičeva 3, 1000 Ljubljana

ZADEVA: Predlog sprememb in dopolnitev zakona o kazenskem postopku (ZKP-M) – mnenje Informacijskega pooblaščenca
ZVEZA: Vaše zaprosilo in gradivo z dne 6.12.2013

Spoštovani,

Informacijski pooblaščenec (v nadaljevanju Pooblaščenec) na podlagi 48. člena Zakona o varstvu osebnih podatkov (Ur. l. RS, št. 86/04, 113/05, 51/07 in 67/07, v nadaljevanju ZVOP-1) daje predhodna mnenja ministrstvom, državnemu zboru, organom samoupravnih lokalnih skupnosti, drugim državnim organom ter nosilcem javnih pooblastil o usklajenosti določb predlogov zakonov ter ostalih predpisov z zakoni in drugimi predpisi, ki urejajo osebne podatke. S spodnjim mnenjem se odzivamo na Zakon o spremembah in dopolnitvah Zakona o kazenskem postopku (EVA 2013-2030-0106; v nadaljevanju predlog ZKP-M).

Pooblaščenec se opredeljuje zgolj do členov, ki zadevajo prikrite preiskovalne ukrepe.

K 7. členu predloga ZKP-M (dekoderji)

Sedmi člen novele uvaja novo 1.a točko v prvem odstavku 150. člena, in sicer možnost ti. nadzora vsebine komunikacije pri viru (nem. *Quellen-TKU oz. Quellen-Telekommunikationsüberwachung*). V skladu s prejetimi pojasnili namerava policija nabaviti posebno programsko opremo – ti. trojanskega konja, tudi »dekoder« – jo na daljavo ali s tajnim vstopom v prostore namestiti na osumljenčev računalnik, tablico, telefon oz. drugo elektronsko napravo, ter si na ta način zagotoviti možnost prestrezanja telekomunikacij, ki so sicer šifrirane in torej nedosegljive za ukrep iz 1. točke istega odstavka. Predvsem naj bi šlo za Skype in druge priljubljene VoIP/messaging programe, ki postajajo vse bolj priljubljeni, in ki šifrirajo vso komunikacijo do cilja oz. do posredniških strežnikov.

V osnovi gre za namestitev trojanskega konja na elektronsko napravo, ki naj bi jo za svojo komunikacijo uporabljala tarča ukrepa iz 1. točke istega odstavka.

Pooblaščenec pri tem opozarja na nujo po skrajni previdnosti pri izvedbi tega ukrepa. Predlog zakona ne vključuje ne primerjalnopravne analize, niti ne t.i. Privacy Impact Assesment-a, s katerim bi se podrobneje osvetlila tveganja pri uporabi ukrepa. Naj ponovno spomnimo na primer iz Nemčije, kjer »trojanca« uporabljajo že več let, in sicer na podlagi odločbe Zveznega Ustavnega sodišča[1], ki je uporabo dovolilo pod določenimi, zelo omejenimi pogoji. Vendar je kasnejša analiza nemškega združenja Chaos Computer Club (ccc) iz oktobra 2011[2] pokazala, da se ti pogoji v praksi v znatni meri ne spoštujejo. »Trojanec«, ki ga je uporabljala nemška policija, namreč ni bil omejen na nadzor določenih programskih paketov za VoIP telefonijo, ampak je omogočal kar prevzem popolne kontrole nad računalnikom ter posledično izvedbo poljubnih forenzičnih analiz, izdelavo zaslonskih slik, ter pravzaprav namestitev poljubne kode (payloada), vključno s (hipotetično) tudi ponarejenimi

[1] http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html
[2] http://ccc.de/en/updates/2011/staatstrojaner

dokazi. »Trojanec« za komunikacijo z nadzornikom na strani policije ni uporabljal zaščitene povezave, ampak kar nezaščiteno, ki jo je za nameček še speljal čez proxy strežnik v tuji državi (ZDA). Zavarovanje nadzorne povezave tudi ni bilo ustrezno, tako da bi računalniki preiskovanih oseb zavoljo »trojanca« v skrajnem primeru lahko utegnili bili celo žrtve vdora s strani tretjih oseb. Takšno stanje, ki očitno krši pogoje Sodišča, vzpostavlja resne dvome o zakonitosti uporabe ukrepa oz. o uporabnosti tako zbranih dokazov v kasnejšem kazenskem postopku. Težko je namreč pričakovati, kako bo sodišče lahko prepričano, da forenzična veriga tukaj ni bila pretrgana. Težko je tudi razumeti, da so bile preiskovalnemu sodniku, ki je izdal odredbo za uporabo takšne opreme, predhodno dane vse potrebne informacije za potrebe presoje upravičenosti ukrepa.

Prav tako se postavlja vprašanje, na kakšen način bo »trojanec« nameščen na ciljno napravo. Moderni operacijski sistemi vsebujejo kompleksne zaščite proti namestitvi nezaželene programske opreme, tako na oddaljen način kot z lokalnim dostopom. Za namestitev je praviloma potreben nakup informacij o ustreznih – novejših – varnostnih pomanjkljivostih (ti. *0-day exploiti*), kar ni poceni in slovenski policiji - glede na izjavo, da ta del zakona ne bo imel finančnih posledic - najbrž sploh ne bo dosegljivo. Če že, pa bo izplen omejen na računalnike s starimi, neposodobljenimi operacijskimi sistemi, na novejših sistemih oz. predvsem na mobilnih napravah, ki vse bolj služijo tudi kot Skype klienti, pa sploh ne bo mogoč.

Upoštevajoč opisane neznanke glede tehničnih, pravnih in finančnih pridržkov Pooblaščenec močno priporoča, da se omenjeni člen črta in predvidi za katero od kasnejših novel. Pred vpeljavo pa naj se izvedejo ustrezne študije, kot spodaj.

K 8., 9., 10. in 11. členu predloga ZKP-M (IMSI lovilci)

8. člen dodaja nov prikriti preiskovalni ukrep uporabe IMSI lovilca (150.a in 150.b člen), sledeči členi pa ustrezne redakcijske prilagoditve obstoječega 152. oz. 153. člena ZKP. IMSI lovilec naj bi služil za pridobitev osumljenčeve telefonske številke za potrebe izvedbe drugih obstoječih ukrepov (pridobitve prometnih podatkov po 149.b členu oz. pritajenega nadzora telekomunikacij po 150. členu), oz. za lociranje osumljenčevega komunikacijskega sredstva. Ukrep je vezan na ista kazniva dejanja (+ ugrabitev) kot 150. člen.

IMSI lovilci so v praksi slovenske policije že bili uporabljeni, domnevno na podlagi bodisi 1. odstavka 148. člena (na spornost te podlage je Pooblaščenec že večkrat opozoril), bodisi pooblastila za tajno delovanje iz 155.a člena. Gre za prenosne lažne postaje mobilne telefonije. Po vklopu se prisotnim mobilnim telefonom predstavijo kot bazna postaja enega od slovenskih operaterjev, nakar se telefon, ker gre za relativno gledano njemu najbližjo bazno postajo, seveda avtomatsko skuša priklopiti nanjo. Postaja pri tem zabeleži določene podatke o priključku (IMSI številko oz. telefonsko številko), nakar telefon odklopi. S primerjanjem tovrstnih zajemov na večih lokacijah (praviloma s sledenjem osumljencu) je mogoče izluščiti uporabljano številko osumljenca. Dodatno je po principu lova na lisico mogoče natančneje določiti lokacijo, oz. slediti določenemu telefonskemu priključku.

Obseg podatkov, ki jih naprava zbere, je po sami naravi podoben kot pri pridobitvi »prometnih podatkov za celotno bazno postajo«, kar je v preteklosti že bil predmet poskusa novele (sicer 149.b) člena ZKP. Policija namreč z uporabo lovilca pridobi podatke o vseh v bližini naprave prisotnih telefonih, velika večina teh pa ne bo pripadala osumljencem. Pooblaščenec je posledično tekom priprave členov predlagal več varovalk (gleda namena in pogojev za rabo ukrepa, sodne avtorizacije ukrepa, striktne izdelave zapisnikov o rabi ukrepa, ter podvzema aktivnih ukrepov za minimizacijo škode za tretje osebe). Pooblaščenčevo soglasje k členu temelji na predpostavki, da bo člen sprejet v sedanjem besedilu, ter da bodo omenjene varovalke dosledno spoštovane. Končno opozarjamo še na navedbe v utemeljitvi ukrepa, da se bo uporabljal (bolj kot ne) izključno za pregon storilcev organiziranega kriminala, ki redno in dosledno menjujejo SIM kartice in jih posledično ni mogoče drugače podrediti ukrepom iz 150. člena.

K 149.b členu predloga ZKP-M (prometni podatki)

Pooblaščenec opozarja na nadavne dogodke pred Sodiščem Evropske Unije, ki ima v odločanju dve predhodni vprašanji, ki zadevata zakonitost ukrepa obvezne hrambe prometnih podatkov iz Direktive 2006/24/ES (udejanjene v XIII. poglavju ZEKom-1). Generalni pravobranilec[3] v zadevi C-293/12 Digital Rights Ireland in C-594/12 Seitlinger in drugi, g. Cruz Villalóna, je mnenja, da je direktiva o hrambi podatkov **v celoti nezdružljiva** z Listino EU o temeljnih pravicah, v skladu s katero mora biti vsako omejevanje uresničevanja temeljnih pravic predpisano z zakonom. Pravobranilec posledično predlaga ugotovitev neveljavnosti direktive, vendar z ustreznim časovnim odlogom, da bo lahko zakonodajalec Unije sprejel ustrezne popravke. Mnenje pravobranilca seveda še ni sodba, niti ni zavezujoče za Sodišče, drži pa, da Sodišče tovrstna mnenja praviloma upošteva v večini ali celo v celoti. Posledično kaže v prihodnjem letu ali dveh pričakovati spremembo Unijine retencijske zakonodaje, minimalno v smer, da se normira tudi raba zbranih podatkov, predvsem v smislu, da se omeji na kataloški spisek hujših kaznivih dejanj. V zvezi z zapisanim naj vas ponovno opozorimo tudi na našo zahtevo za oceno ustavnosti in zakonitosti relevantnih členov ZEKom-1, vloženo iz podobnih razlogov.

Pooblaščenec posledično v zvezi z navedenim priporoča spremembo 149.b člena ZKP, in sicer v smeri omejitve ukrepa iz 1. odstavka (pridobitev prometnih podatkov) na isti kataloški spisek kaznivih dejanj, kot je sicer predpisan za ukrep iz 150. člena.

Splošna pripomba k predlogu ZKP-M (Privacy Impact Assesment)

Pooblaščenec ponovno opozarja na nujnost resnega in predhodnega ovrednotenja posledic dodajanja pooblastil represivnim organov za zasebnost državljanov (t.i. Privacy Impact Assessment ali PIA). Od predlagatelja bi si želeli več aktivnosti v to smer, ter tudi več javne razprave, po možnosti seveda pred nakupom naprav samih.

Lep pozdrav,

Informacijski pooblaščenec
Nataša Pirc Musar, univ.dipl.prav.,
pooblaščenka

[3] http://curia.europa.eu/jcms/upload/docs/application/pdf/2013-12/cp130157sl.pdf